RECORDS MANAGEMENT AND THE ACCOUNTABILITY OF GOVERNANCE

A thesis submitted to the University of Glasgow
for the degree of Doctor of Philosophy
in the Faculty of Arts

APRIL 2009

AZMAN MAT ISA

HUMANITIES ADVANCED TECHNOLOGY AND INFORMATION INSTITUTE

ERRATUM

ABSTRACT

Governance is the process by which power and authority are exercised in a society by which government, the private sector, and citizens' groups articulate their interests, mediate their differences, and exercise their legal rights and obligations. Governance in public organisations is different from that in private organisations as they both possess different types of institutional stakeholders. Governments are directly answerable to the public. Therefore, it is essential for governments to be transparent in order to avoid any triggers in the accountability process that might adversely affect people's trust. The proper creation, capture, distribution and preservation of juridical evidence in the form of records can help avoid these problems. A trusted government is one that can demonstrate its accountability and transparency and is continually striving to improve value delivery and increase cost-effectiveness. The freedom of information demands governments to be more transparent and accountable for their actions and decisions. Whilst governments promote corporate governance to provide transparency and objectivity it can only give stakeholders better tools to do their job, it does and cannot do it for them. The need for managing risk and audit culture is imperative to balance and satisfy the expectation of citizen and stakeholders. The accountability of a government can arguably only be achieved when it demonstrates considerable transparency, which in turn can only happen when trust is supported by authentic and reliable records. The records management community claims that records have to be preserved for accountability, but they rarely explore what 'accountability' is and what role records play in the accountability processes. In addition, the contribution of records management to good governance and accountability are often not recognised by other professions and management. In an age where corporate governance and transparency is a global agenda, it is imperative for the records management community to scrutinise their present role and approach in order to change the perception by other professions about their contribution towards achieving organisational goals in a highly regulated and compliant bound environment in the public and private sectors. The contention of this thesis is that record keeping is just a tool that ensures the availability of evidence for the accountability of governance, which in turn relies on the ethical standard of those involved.

TABLE OF CONTENT

List of Figures

List of Tables

List of Abbreviations and Acronyms

AIRMIC	:	The Association of Insurance and Risk Managers, United Kingdom
ALCO	:	ALM Committee, European Investment Bank
ALP	:	Australian Labour Party
APPM	:	Archives, Personal Papers and Manuscripts
BCBS	:	Basel Committee on Banking Supervision
BCS	:	British Computer Society
CEO	:	Chief Executive Officer
CFO	:	Chief Finance Officer
CHPs	:	Community Health Partnerships
CHCPs	:	Community Healthcare Partnerships
CID	:	Communication and Information Department, European Investment Bank
CMT	:	Corporate Management Team, NHS Greater Glasgow
CRAG	:	Credit Risk Assessment Group, European Investment Bank
DERA	:	Defence Evaluation and Research Agency, United Kingdom
DFS	:	Department of Family Services, Queensland, Australia
DFSAIA	:	Department of Family Services and Aboriginal and Islander Affairs, Queensland, Australia
DIRKS	:	Designing and Implementing of RecordKeeping System
EIB	:	European Investment Bank
ERPANET	:	Electronic Resource Preservation and Access Network
EU	:	European Union
FOI	:	Freedom of Information Act 2002
FOISA	:	Freedom of Information (Scotland) Act 2002
FSA	:	Financial Services Authority
GAO	:	Government Audit Office, United States
GED	:	*Gestion Électronic de Documents*
GMC	:	General Medical Council
GP	:	General Practitioner
ICT	:	Information and Communication Technology
IRM	:	The Institute of Risk Management, United Kingdom
ISIS	:	Integrated Strategic Information System
ISO	:	International Standards Organisation
IT	:	Information Technology
JIC	:	Joint Intelligence Committee, United Kingdom
JOYC	:	John Oxley Youth Detention Centre, Queensland, Australia
LHCC	:	Local Health Care Co-operative
MAS	:	Metropolitan Ambulance Service, Victoria, Australia
MCCD	:	Medical Certificate of Cause of Death

MoD	:	Ministry of Defence, United Kingdom
MoReq	:	Model Requirements for the Management of Electronic Records
NAO	:	National Audit Office, United Kingdom
NARA	:	National Archives and Records Administration
NHSGG	:	National Health Service Greater Glasgow
NHSGGC	:	National Health Service Greater Glasgow and Clyde
NHS QIS	:	National Health Service Quality Improvement Scotland
OAIS	:	Open Archival Information Systems
PACE	:	The Police and Criminal Evidence Act 1984
QPOA	:	Queensland Professional Officers Association, Australia
QSSU	:	Queensland State Services Union, Australia
QTU	:	Queensland Teachers Union, Australia
RMD	:	Risk Management Directorate, European Investment Bank
RMSG	:	Risk Management Steering Group, NHS Greater Glasgow
RMU	:	Records and Management Unit, European Investment Bank
SDLC	:	System Development Life Cycle
SEC	:	Securities and Exchange Commission
SEHD	:	Scottish Executive Health Department
SIC	:	Statement on Internal Control
SOX	:	Sarbanes-Oxley Act (2002)
SWD	:	Social Work Department
UK	:	United Kingdom
UNSCOM	:	United Nations Special Commission
US	:	United States
XML	:	eXtensible Mark-up Language
WMD	:	Weapons of Mass Destruction

ACKNOWLEDGEMENT

This thesis would not have been possible without guidance and support from numerous people. Firstly, I am greatly indebted to my supervisors, Professor Michael Moss for the knowledge, patience and understanding that he has contributed throughout the whole duration of my research; and to Professor Seamus Ross and Lesley Richmond for their valuable support and comments throughout my research. Secondly, I would like to thank Alistair Tough and Dr James Currall for their support and constructive insight.

Sincere thanks to all interviewees for sharing their professional experience and enthusiasm in assisting me with this study. Mr Alan Murdock and his colleagues in the European Investment Bank, Luxembourg; Mrs Kate Knight in Standard Life, Edinburgh; Mr Alistair Tough, Mr John Hamilton, Dr Harry Burns, Mrs Elinor Smith, Mr Alan Lindsay, and Mr Andy Crawford in the NHS Greater Glasgow and Clyde; and Mr Mark White in PricewaterhouseCoopers, Glasgow. Many thanks also extended to all staff of HATII especially Adele Redhead, ERPANET and fellow PhD candidates for their kind assistance and support.

I am also indebted to the financial support from my sponsor, Universiti Teknologi MARA, Malaysia. My sincere thanks to these organizations especially to Associate Professor Dr Laili Hashim (Dean - Faculty of Information Management), Associate Professor Dr. Adnan Jamaludin and Associate Professor Dr. Sohaimi Zakaria, for granting me the opportunity and trust in undertaking and pursuing doctoral degree. I would also like to thank all the staff at the Faculty of Information Management for their encouragement.

To my parents whom were far away in Malaysia during my entire study. Their absence was greatly felt. Finally, to my wife, Wan Markhairulnizah Wan Ahmad, who has sacrificed so much through this journey by giving me the courage. Also to all my three boys, Megat Irfan, Megat Adib Fayadh and Megat Ahmad Thaqif and my little princess, Puteri Nuha Shasmeen, for making my life so meaningful.

DECLARATION OF AUTHOR'S COPYRIGHT

I declare, except where acknowledge, all the work has been undertaken by myself.

Signature : _____

Name of Author : AZMAN MAT ISA

Date : 30 April 2009

CHAPTER 1

INTRODUCTION

1.0 INTRODUCTION

1.1 Research Background

Records play a crucial role in most human endeavours and they are essential to many of our business and social interactions. The origin of systems of archival record keeping were developed over several millennia in Mesopotamia before spreading to Egypt, the Mycenaean world, and the Persian empire, continuing through the Hellenistic and Seleucid periods (Brosius, 2003). Record keeping was thought essential in the administration of government offices such as in the British Civil Service in the nineteen century (Moss, 2005), and in the Netherlands in the early twentieth century (Horsman, 2006). Indeed, record keeping practices have evolved from the ancient world to modern times. The introduction of computers in the middle of the twentieth century affected the role of record keeping in underpinning effective administration and businesses operations as organisations were beguiled by the impressive characteristics of digital technology, particularly in the creation, storage and retrieval of information along with apparently reliable security features. It is essential for organisations to have reliable record keeping systems for their sustainability, particularly for censorship and retention policies, intelligence, security and intellectual property purposes (Cox, 2006).

In addition, the implementation of electronic government (e-government) systems in many countries across the world has resulted in the exponential growth of use of electronic records. Dominated as the digital environment is by information and communication technology (ICT) professionals, the records management community often finds it extremely difficult to push for the adoption of an organisational-wide effective records management system within the context of an ICT strategy. It also unfortunate that the records management community has simultaneously been overtaken by a relatively new risk management approach to corporate governance. The starting point of this thesis is to question why records management is not considered high priority in many organisations?

A government, particularly in a truly democratic country, is accountable to its people for its administration and governance. Public records, which are the bye-products of public organisations, provide evidence of the governance of the country. Meijer (2001) argues that the records management community claims that records have to be preserved for

accountability purposes, but they rarely explore what accountability is and what role records play. In addition, the contribution of records management to good governance and accountability is not recognised by other professions and management.

It is, therefore, essential to tease out the nature or ontology of records and records management in order to fully understand their role in ensuring accountability of an organisation. The accountability of a government can arguably only be achieved when it demonstrates considerable transparency, which in turn can only happen when trust is supported by authentic and reliable records. In an age where corporate governance and transparency are key goals in a global agenda, it is imperative for the records management community to investigate the way in which records management practice can fulfil this role.

1.2 Problem Identification

Ironically, despite the claims of the advantages of digital technology and corporate governance, high profile cases of poor governance and maladministration are often identified by, and were widely reported in the press. For example, corruption and mismanagement in the Australian government in the 1980s, the collapse of Enron, WorldCom and Tyco in the United States and Parmalat in Italy, the issues surrounding and leading to the death of the British civil servant, Dr David Kelly, and the killings by Dr Harold Shipman all raise questions about the accountability, transparency, and trust placed in those working in specific roles working in both the public or private sectors. Such failures in accountability, transparency, and trust can happen as a consequence of an individual act, or more worryingly, a group of people who deliberately and systemically breached the trust placed in them. These cases all individually raised concern in the public mind about the process of documenting a business or administrative transaction. In addition, it was doubted that appropriate documentation procedures existed, and were followed by all employees.

The contention of this thesis is that record keeping is just a tool that ensures the availability of evidence for the accountability of governance, which in turn relies on the ethical standard of those involved. I set out to investigate and identify the underlying problems of such failures in order that lessons can be learned from in the future. Meijer's (2001) assertion that records management is not regarded as essential in underpinning

good governance triggered my interest in exploring the reality by conducting case studies in the chosen organisations which might be expected to have good records management systems, and where risk management could be expected to influence policies and procedures.

Risk management, a relatively new area compared to records management, covers almost every aspect of an organisation's activity. It might be assumed that risk assessment can only be conducted effectively when authentic and reliable records are available. It is the purpose of this research to identify a potential relationship between records management and risk management in order to facilitate organisations to strike a balance between costs and benefits. Arguably the records management community itself needs to better understand its role in underpinning the accountability of governance. If this is the case it is therefore vital for the records management community to scrutinise their present role and approach in order to change the perception by other professions about their contribution towards achieving organisational goals in a highly regulated and compliant bound environment in both the public and private sectors.

1.3 Research Questions

Three research questions were identified to explore the relationship between records management and the accountability of governance, namely:

i. Why records management is not regarded as essential for good governance? Despite an increasing demand for transparency and accountability, least attention is given by organisations to improve their records management. Yet they managed to survive. It is important to investigate the underlying reasons for this scenario in order to facilitate improving good governance.
ii. What role do records play in the accountability of governance? Accountability of governance is an evidence based process that occurs after activities have been executed or decisions have been taken. Hence, it is important to investigate the role of records and the evidence that they contain in demonstrating accountability of governance.
iii. What is the relationship between risk management and records management? Records management ensures the availability of records for risk assessment and systematically captured the records of risk management processes. Risk management is a dynamic process. Effective records management ensures the

availability of records for future assessment in order to determine whether the recommended risk mitigation has been followed by relevant business process owners. It is essential to explore the relationship between these two areas in order for organisations to benefit the synergy of their integration.

1.4 Research Objectives

The objectives of this research are:

i. To identify the underlying cause of records management not being regarded as essential for good governance.
   The ability to identify the underlying cause enables records management community to enhance their contribution to good governance by ensuring the availability of trustworthy records.

ii. To identify the role of records in the accountability of governance.
   The ability to identify and understand the role of records within an organisation facilitates the process of implementing organisational-wide effective record keeping system. This in turn, ensures the availability of trustworthy records which is a pre-requisite in promoting a climate of trust and overall commitment to good governance.

iii. To identify the relationship between risk management and records management.
   It is essential to be able to identify the relationship between these two areas as it helps organisations to balance their cost and benefits, which ensures their sustainability. The ability to identify all risks and their mitigation ensures whenever a risk occurs, all necessary resources to mitigate the risk are readily available.

1.5 Research Methodology

This is descriptive research that uses case study methodology. In order to gather information, firstly document analyses were undertaken, and secondly officials from various departments were interviewed. Three case studies were conducted in different organisations, namely:

- Standard Life plc, Edinburgh
  Standard Life plc is a holding company, owned by its shareholders. Its business areas include life assurance, pension business, banking, healthcare, and

investment. It also has joint ventures with companies in several countries across the globe.

- European Investment Bank, Luxembourg
  The European Investment Bank (EIB) is a unique institution with two statuses: it is simultaneously an institution of the European Union, and a bank. It works in close collaboration with the banking community, both when borrowing on the capital markets and when financing capital projects.
- NHS Greater Glasgow and Clyde Health Board, Glasgow
  NHS Greater Glasgow Health Board (NHSGG) is a public organisation. It is responsible for local health planning and improvement and for the delivery of hospital, community and primary care services to the community of Greater Glasgow and Clyde.

The objective in selecting these organisations was to identify best practice in records management which could easily and effectively be adopted elsewhere, particularly in the public sector.

1.6 Research Scope

The scope of the research is limited to the management of records in the chosen organisations. Access was not sought or given to the confidential records of the named organisations. Internal staff across various divisions within each organisation and related parties such as external auditors were interviewed in the process of gathering information.

CHAPTER 2

LITERATURE REVIEW

2.0 LITERATURE REVIEW

2.1 Introduction

This chapter explores the theoretical and real relationships between records management and the accountability of corporate and organisational governance. A comprehensive literature study shows that records management used to be the backbone of efficient business and government administration in the United Kingdom (UK) and the Netherlands, though record keeping practice is not limited to these two countries, before ICT came to dominate work places. The implementation of electronic government presents new challenges to the information and records management professions. Although ICT changes the nature of office environments and business transactions, the ethical elements remain the same. Theoretically, a holistic approach to records management involving risk management, legal and compliance requirements as well as business requirements, may prove the significance of records management in underpinning accountability of governance.

2.2 Governance

Governance can be viewed as the collective policies and oversight mechanisms in place to establish and maintain sustainable and accountable organisations that achieve their missions while demonstrating stewardship over resources. Today, corporate governance is of central importance as members of the public are more concerned about issues of transparency and accountability following the high profile corporate failures in the third quarter of the 20th century. Organisations, both public and private, must comply with domestic and international regulations in order to remain sustainable.

2.2.1 Definition of Governance

Governance is derived from a Latin term ‘gubernare’ which means to steer (OECD, 1999). The United Nations Development Programme (UNDP, 1997) defines governance as the exercise of economic, political and administrative authority to manage a country’s affairs at all level. Governance can also be viewed as the collective policies and oversight mechanisms in place to establish and maintain sustainable and accountable organisations that achieve their missions while demonstrating stewardship over resources (Government Accountability Office, 2005). There is a fundamental tension between freedom and governance, which has existed ever since individuals found the

need to relate to others, and recognized that workable relationships require ground rules to be successful (Davies, 1999). The primitive rules which evolved to shape early tribal relationships seem to have moved with the passage of time into two main categories – customs (which are means of working together effectively), and moral codes (which are ends in themselves). Therefore, governance is seen as a process for reconciling the ambitions of the individual with the need to preserve and develop a 'common weal' which binds through shared interests. Davies (1999) agrees with Muller (1981) who defines governance as constrained in the intrinsic nature, purpose, integrity and identity of an institution with a primary focus on an entity's relevance, continuity, and fiduciary aspects.

Governance involves monitoring and overseeing strategic direction, social economic and cultural context, other externalities and constituencies of the institution. Governance is about processes, not about ends. It is about the process by which power and authority is exercised in a society by which government, the private sector and citizens' groups articulate their interests, mediate their differences, and exercise their legal rights and obligations (Fukuda-Parr and Ponzio, 2002). In other words, governance is a series of administrative activities and actions use to steer an organisation and other actors in its circle towards its organisational objectives and goals. The administrative activities and actions must comply with rules and regulations imposed by government (directly or indirectly) or the organisation itself. Pierre and Peters (2000) state that governance has two perspectives namely, governance as structure and governance as process. Governance as structure is about governance arrangements that have existed historically, as well as presently: hierarchies, markets, networks and communities. Meanwhile, governance as process is more important because governance is not so much about structures, but more about interactions between structures. These interactions are vital to ensure organisational goals are achievable. Governance has to be dynamic to suit the fast changing work environment and societal expectation.

2.2.2 Styles and Elements of Governance

Styles of governance vary depending on the nature and size of the organisation. Be it a public or private organisation, conformity with regulations is often considered more important than performance, because a failure to comply can have important downside consequences for shareholder value. In the not too distant past society tended to accept that governance of non-profit making organisations relied more on trust than on rules, but

Kearns (1996) has demonstrated misappropriation of resources by charities and non profit organisations has led to a change in attitude to governance in the not-for profit sector as well[1]. The nature of different organisations, require different approaches to be able to fulfil the needs and expectations of shareholders and stakeholders and to ensure institutional sustainability. Davies (1999) asserts trust can only work with open governance; in bodies which are opaque in their governance rules become an essential sheet anchor. Amalgamation of trust and rules has been adopted in most organisations to provide flexibility within regulatory boundaries. Under these circumstances, an appropriate documentation is vital to ensure the availability of records of actions and decisions taken.

Davies further explains several criteria that organisations need to establish their governance, such as:

i. The identity of the body;

ii. Definition of its purpose;

iii. How the purpose is to be achieved;

iv. Membership criteria (both explicit, such as shared interests, and implicit, for example shared values);

v. How the body is to be administrated;

vi. How the body relates externally

vii. How success is measured; and

viii. Termination arrangements.

All organisations must establish these criteria (either explicitly or implicitly) to guide and facilitate their governance in achieving organisational goals.

The United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP) identified eight major characteristics of good governance. They are participatory, consensus oriented, accountable, transparent, responsive, effective and

[1] Kearns (1996) states that the American Society for the Prevention of Cruelty to Animals (ASPCA) has strayed from its mission and is not getting maximum benefit from its $20 million in annual revenues. Specific concerns focused on the self-elected board, overtime pay for staff, and construction and design flaws in the ASPCA's new headquarters building.

efficient, equitable and inclusive, and follow the rule of law. It assures that corruption is minimised, the views of minorities are taken into account, and that the voices of the most vulnerable in society are heard in decision-making. These characteristics must also be responsive to present and future needs of society. Governance can be defined in different contexts such as corporate governance, international governance, national governance and local governance. Governing public organisations is different to governing private organisations as governments are directly answerable to the public. It is essential therefore for governments to be transparent to avoid any triggers in the accountability process that might affect people's trust. Avoiding this possibility can be assured through proper creation, capture, distribution and preservation of juridical evidence in the form of records.

2.2.3 CORPORATE GOVERNANCE

Corporate governance is one of the key elements in improving economic efficiency and growth as well as confidence among investors and stakeholders. Corporate governance does not guarantee success and sustainability of organisation. However, it does provide a better approach for organisations to demonstrate transparent and accountable governance.

2.2.3.1 History of Corporate Governance

According to Davies (1999), corporate governance emerged after the Second World War (WW II). He asserts:

> *The growth of trades unions in the first half of the century began to offset the power of companies which had been able to force down wages to maintain profit even as trading became more competitive. This phenomenon made governance more complex, adding a new dimension to the shareholder/board of directors axis. This situation was consolidated by the need to work together through the war and the unions entered the second half of the century with enhanced and growing power. The war also strengthened the impact of government on businesses, bringing in a mass of new regulations many of which survive their usefulness. (Davies, 1999:33).*

He then further describes how in the third quarter of the 20th century negotiations between protagonist employees and company directors eventually resulted in the avoidance of strikes by employees rather than enhancing stakeholder value. A series of corruption scandals and the collapse of major public and private organisations worldwide, especially during the economic recession in the late 1980s, reawakened awareness of the importance of good governance. A view emerged that traditional governance was not capable of coping with a rapidly changing work environment which produced new challenges and threats to accountability in the early 1990s. Davies (1999) further argues that fraud was a key element in corporate collapse such as Rolls Royce, Maxwell Communication, Polly Peck and Rolls Razor. These failures only increased the sense of betrayal not only of stakeholders, but of employees, suppliers and, in the case Robert Maxwell, pensioners. In addition, these failures drew attention to the need for better governance, which eventually contributed to setting of new standards.

2.2.3.2 Definition of Corporate Governance

There are many definitions of corporate governance depending on the context. For the purpose of this research, the most relevant definitions are by Organisation for Economic Co-operation and Development (OECD) and the Cadbury Committee in the UK and, also a recommendation made by the President of the World Bank. Both OECD (2004) and Cadbury Committee (1992) defined corporate governance as the system by which business corporations are directed and controlled. The corporate governance structure specifies the distribution of rights and responsibilities among different participants in the corporation, such as the board, managers, shareholders and other stakeholders, and spells out the rules and procedures for making decisions on corporate affairs. By doing so, it also provides the structure through which the company objectives are set, and the means of attaining those objectives and monitoring performance.

Meanwhile, Wolfensohn (1999) defines corporate governance as about promoting corporate fairness, transparency and accountability[2]. Although the second definition is short, it is pertinent to this research which focuses on accountability and responsibility of governance. Establishing corporate governance means promoting accountability and responsibility to all stakeholder groups, participants, actors and agents. Good corporate

[2] John Wolfensohn, the President of the World Bank as quoted by *Financial Times*, 21 June 1999.

governance should be able to monitor corporate affairs and avoid sudden disaster as all actors are accountable for their actions. Sternberg (1998) argues that the key concept of corporate governance is accountability, which means that individuals and institutions are answerable for what they do; they must account to others for their conduct and for their use of resources. She further explains that there are two types of accountability that are critical for corporate governance: the accountability of directors to shareholders, and the accountability of corporate employees and other corporate agents to the organisation.

There are other definitions, such as that which views the critical relationship among various participants in determining the direction and performance. It is essential to determine who are the participants, actors or agents of corporate governance as this makes it easier to specify their responsibility in directing an organisation towards achieving its goals. The primary participants are the shareholders; the management (led by the chief executive officer); and the board of directors (Monks and Minow, 2001). Although stakeholders do not possess as much power as shareholders, they should not be sidelined as they have an impact on the long-term return of an organisation and its reputation. Sternberg (1998) argues that whether the purpose of an organisation is business, charity or education, the aim of corporate governance is to make sure that it is shareholders' stipulated objective that governs the corporation and all its actions and agents. It is therefore vitally important to establish criteria of governance as proposed by Davies (1999) to avoid diversion from organisational goals.

Compliance with corporate governance does not mean that a company is being run properly or that there is no danger of shareholder value being lost. Shareholders have to keep a close eye on the performance of their investments. OECD (2004) asserts that corporate governance provides transparency and objectivity – while it gives shareholders better tools to do their job, it does not do it for them. This has to be clearly understood if corporate governance is to maintain its credibility[3]. Apart from rules and regulations underpinning corporate governance, another essential element is the attitude of employees towards their job responsibilities. Although employees are accountable for their acts, sometimes people might cheat, simply because they need to maintain their credibility. As O'Neill (2003) suggests, demands for universal transparency are likely to

[3] It is a professional discussion as a respond to the Higgs report on how to improve corporate governance in the UK. Further information can be found in *Higgs Might Fly! The New Combined Code*. Available at: http://www.wragge.com/files/HiggsMightJustFly_Jul2003.pdf. (21 June 2007).

encourage evasions, hypocrisies and half-truths that we usually refer to as 'political-correctness', but which might more forthrightly be called either self-censorship or deception.

2.2.4 GOVERNANCE AND GOVERNMENT

Relationship between governance and government is complex and confusing. Sternberg (1998) shows how corporate governance contrasts with government by stating that governments are backed by the use of its state's coercive power, and public policy objectives are legitimately chosen and implemented only by those who are publicly accountable to the electorate. Ironically, with less power as compared to government, private organisations are properly accountable only to their shareholders, but they are, also, subject to the law of the land which means that they are obliged to comply with rules and regulations imposed by government. However, there may well be differences with organisations that provide public utilities across a nation.

Government, be it democratic or autocratic, is responsible to the people that demand good governance. Government is directly accountable for the performance of public organisations and indirectly accountable for the performance of private organisations through laws and regulations that it imposes. Public utilities and services, such as electricity, water, gas and public transportation, are under constant public pressure to deliver reliable and satisfactory services. Incidents such as train accidents and strikes by unions badly affect commuters and cost millions of pounds[4]. To this end, governance involves dynamic human activities, not just a structure on paper. It involves discussion and dialogue, including disagreement and confrontation but it is based on rules and procedures. It is also open to change, adaptation, and improvement (Wyatt[5], 2005).

In the case of transport systems, unions and employers should be able to reach a win-win decision instead of dragging on their dispute until a strike is unavoidable. Thus, government within its capacity and authority can intervene to prevent any serious

[4] The Rail, Maritime and Transport (RMT) Union strike in 2002 left millions of commuters struggling to get to and from work. Accounting firms estimated the cost of the strike was £60 to £100 million. Further information available at: http://news.bbc.co.uk/1/hi/england/2135146.stm (21 June 2007).

[5] Marilyn Wyatt, PhD, is a consultant and governance expert based Prague, Czech Republic. Further information available at http://www.euconsult.org/241/ *and* http://www.spock.com/Marilyn-Wyatt-RjA5c1oV

consequences for its biggest stakeholders, members of the public. Sternberg (1998) further argues that corporate governance is not about the 'relationship of corporation to the society', nor about the regulation of corporations in the interests of society, as regulation is backed by the force of law which is subject to civil government, not corporate governance. The relationship between governance and government has been made more complex by the rise in corporate failures either in the private sector or more especially in public organisations. Government is seen to be directly responsible for ensuring good governance and may well over-react.

A trusted government is one that can demonstrate its accountability and transparency and is continually striving to improve value delivery and increase cost-effectiveness. Freedom of Information (FOI) legislation demands governments to be more transparent and accountable for their actions and decisions. O'Neill (2002) argues that openness and transparency are set to replace traditions of secrecy and deference, at least in public life. In a democratic nation, it is essential for the government to deliver corporate governance as it promotes values which are important in gaining and retaining the people's trust. Records, and the evidence they contain, are the instruments by which governments can promote a climate of trust and demonstrate an overall commitment to good government. Hence, accountability and transparency can only be demonstrated if records, which are the foundation of accountability, are well-managed. Ironically, good record keeping is not only for demonstrating good governance but also for hiding mismanagement such as in the case of the collapse Enron[6].

Physical records have proved their significant contributions to the efficiency and effectiveness of public administration. However, their contributions have become less easy to identify since conventional administration tasks, manually performed by humans, have been automated by the use Information and Communication Technology (ICT). As opposed to the benefits of ICT in terms of easy storage and speedy retrieval of information, there are drawbacks in the form of new and critical challenges in the management of the creation and preservation of information to ensure its authenticity. The authenticity and reliability of electronic records are best ensured by embedding procedural rules in an agency-wide records system and by integrating business and documentary procedures; instituting procedures that tighten the archival bond; integrating

[6] Further discussion is available in Section 3.2.2 The Collapse of Enron.

management of non-electronic and electronic records systems (Duranti, 2001; InterPARES, 2001). This means that governments with coercive power should be able to establish and implement procedures to ensure records are well-captured and preserved to retain their authenticity. This issue will be further discussed in *Section 2.8.4 Authenticity and Integrity of Records*.

2.2.5 Electronic Government

The last decade of the 20th century has seen the introduction of electronic government (e-Government) by many countries around the world such as the United States (US) and the UK[7]. The OECD (2001b) states that e-Government focuses on the use of new information and communication technologies by governments as applied to the full range of governmental functions. In particular, the networking potential offered by the internet and related technologies has the potential to transform the structures and operation of government. A more recent literature by Curtin *et al.* (2004) define e-Government as the use of any and all forms of ICT by governments and their agents to enhance operations, the delivery of public information and services, citizen engagement and public participation, and the very process of governance. e-Government is believed to have the capacity to provide more responsive, transparent and cost-effective administration by exploiting the potential of ICT.

The idea behind e-Government is to provide high performance electronic services to the public through the use of internet-based technology. For e-Government to work effectively and efficiently, it is essential that public have access to accurate and authentic information. As electronic records by their very nature are intangible, a comprehensive and holistic approach to item creation and management is required to ensure electronic evidence is accurate and authentic. To this end, government must establish a comprehensive policy for e-Government which embraces administrative, legal and technical issues. Principles and approaches used in managing conventional records can be used for managing electronic records, though it may require minor adaptation to suit different electronic environments. Fisher (2004) asserts that in establishing standards, it

[7] Accenture research on the implementation of e-Government covers 22 developed and developing countries around the world. Apart from the US and the UK, other countries involved are Canada, Australia, Singapore Denmark, Finland, Sweden, France, the Netherlands, Belgium, Ireland, Japan, Germany, Norway, Spain, Malaysia, Italy, Mexico, Portugal, Brazil and South Africa. Further information available at http://www.accenture.com/NR/rdonlyres/D7206199-C3D4-4CB4-A7D8-846C94287890/0/gove_egov_value.pdf (20 June 2007).

is important to specify the policies, procedures, practices, and documentation required for establishing the integrity and authenticity of recorded information held as an electronic record in an electronic information system. Policy is vital to protect employees from any legal challenges whilst executing their responsibility in accordance with standards required for delivering services to public.

Accenture (2004) reports that many countries implementing e-Government are at a crossroad with their online programs as many factors affect the implementation[8]. Davison *et al.* (2005) assert that there are many barriers to the implementation of e-Government namely, issues of citizen privacy and security, inadequately skilled citizens and government employees, the tendency for e-Government to replicate traditional government and digital divide amongst citizens. Meijer (2001) states that the technological characteristics of ICT do not determine how the technologies are used, but create opportunities and risks. In certain contexts opportunities may or may not be used, and risks may or may not be avoided. Hence, knowledge of the opportunities and risks associated with ICT applications is crucial to ensure the technology deployed is of value for money. It is the responsibility of government through its procedures and regulations to ensure that the appropriate technology has been deployed. Knowledge of technology employed would be useful in facilitating the preservation of electronic records to avoid any doubt about authenticity and reliability. Duranti (1998) refers to the failure to preserve electronic records produced during the early days of the introduction of computers by the Federal Government of the US. Today's governments should learn from this lack of foresight to avoid e-Government initiatives meeting a similar fate. She expresses her concerns about the threat to electronic records by saying:

> *While no one can deny the importance of records, we have rushed into the computer age without considering the implications. The greatest threat we face is the nonchalance with which people treat electronic records. There is far too much accidental destruction and manipulation. We've already lost the last five generations of electronic records. The few we have cannot be proven reliable or authentic. It's a tragedy. (Duranti, 1998a).*

[8] Since 2000, Accenture has been studying and reporting on trends of the e-Government landscape. Their findings are certainly important for implementing better e-Government applications.

Improving cost-effectiveness is a driving value for implementing e-Government (Accenture, 2004). This could be achieved by having a comprehensive information system framework with effective capture and distribution of accurate and up-to-date information and records over the network to allow effective decision making. This is to say that the development of e-Government applications must consider record keeping requirements to enhance the integrity and authenticity of records over time to facilitate decision making. However, these requirements must be made seamless to users and should not dampen the performance of public services. But, more importantly it must be of value for money to the public though the benefit may not surface immediately. MacNeil (1996) states the trustworthiness of records has two qualitative dimensions, reliability and authenticity.

Duranti (2001) and InterPARES (2001), argue that reliability and authenticity of electronic records are mainly assured through procedural means. Official assignments of authority and delegation of responsibility ensure procedures are properly followed in performing record keeping activities. O'Neill (2002b) is cynical suggesting that new legislation, regulations and controls are nothing more than fine rhetoric. They require conformity to procedures and protocols, detailed record-keeping, provision of information in specified formats and success in reaching targets. Records of access to a system, either manual or electronic, must also be captured consistently to safeguard the reliability of records.

The government of Canada learnt a useful lesson following the Commission of Inquiry into the Deployment of Canadian Forces to Somalia at the National Defence Operations Centre (NDOC) which revealed a number of serious problems with logs resulting from lack of standard operating procedures, an ineffective database security system, and inefficient system audits. Hence, NDOC logs were not reliable records of transactions and could not be used as evidence in a court of law (MacNeill, 1996). Electronic information systems, therefore, must be equipped with methods for ensuring the authenticity and reliability of records when captured and stored. It is essential that evidence of transactional security is built into all aspects of systems and environments (Allinson, 2001). Such information security systems must have controls for access and privilege, logging and audit, accountability, and monitoring and reporting in accordance with the level of sensitivity of the electronically or digitally stored, transmitted and processed information.

Although information systems are still exposed to unauthorised access by irresponsible parties, audit trail should be able to track offenders. Audit and certification are discussed in depth in *Section 2.8.3 Audit and Internal Control*. Authenticity of records can be attested through diplomatic and digital forensics. Jenkinson (1954) argued that no description of an administrative department can be completed without a description of the forms of document it produced and the way in which they were written. Diplomatic may affect evaluation of documents by identifying their place within underlying administrative organisations. Duranti (1998b) asserts that the three kinds of authenticity are diplomatic, historical and legal. Documents are authentic if they meet certain diplomatic, historical and legal criteria. Meanwhile, digital forensic is the adaptation of diplomatic concepts to an electronic environment and involves a comprehensive scrutiny of digital records[9] (Harrison, 2004). Arguably, diplomatic is essential in ensuring the authenticity and integrity of records.

In order to improve the operations and security of e-Government applications, the government of the UK has introduced an e-Government Policy Framework[10]. Meanwhile, the government of the US has produced Design Criteria Standard for Electronic Records Management Software Applications which is also known as DoD 5015.2-STD[11]. The UK's e-Government Policy Framework consists of several policies including the e-Government Interoperability Framework (e-GIF) which contains the e-Government Metadata Standard (e-GMS) framework that is essential for managing electronic records. These metadata standards improve audit trails by providing sufficient content, context and structural metadata that are essential for detecting irregularities of business

[9] According to Harrison (2004) digital forensic plays a crucial role in the conviction of a British physician for killing hundreds of his elderly ill-patients. Further scrutiny of digital records eventually discovered vital evidence of his crime and led to the conviction.

[10] The United Kingdom e-Government Policy Framework consists of several policies including e-Government Interoperability Framework (e-GIF) which contains e-Government Metadata Standard (e-GMS) framework that is essential for managing electronic records. The e-GMS has been reviewed three times, the first version was introduced in May 2001, the second version in May 2003 and the latest version in April 2004 (version 3.0). e-GIF is available at http://www.govtalk.gov.uk/documents/eGIF%20v6_1(1).pdf (21 June 2007).

[11] The United States' DoD 5015.2-STD was first introduced in November 1997 and later has been replaced by the second version in June 2002. Like e-GIF, DoD 5015.2-STD emphasizes the importance of metadata and categorised metadata into mandatory and non-mandatory groups to facilitate the management of electronic records. This standard can be found at http://jitc.fhu.disa.mil/recmgt/p50152stdapr07.pdf_ (21 June 2007).

transactions. Procedures must be put in place to ensure that necessary metadata are recorded for the integrity and authenticity of records.

The essence of capturing adequate metadata is also explicitly demonstrated by Sarbanes Oxley Act (2002) (SOX) legislation in the US in an effort to avoid another Enron-like corporate catastrophe. This act emphasizes the importance of audit as a tool to detect any wrong doings such as corruption and mismanagement through the scrutiny of both, paper and electronic records. The SOX legislation demands a number of new roles for audit committees and auditors, such as: auditors will report to and be overseen by a company's independent audit committee; An audit committee must approve all services provided by its auditor; The auditor must report new information to audit committee; Offering specified non-audit services by external auditors is prohibited; The audit partner must be rotated every five years. The act also creates tough penalties for those who destroy records, commit security fraud and fail to report fraud. In terms of financial reporting and the auditing process, the SOX legislation requires a second partner's review and approval of every audit report; management assessment of internal controls. Audit reports must contain a description of internal control testing to determine any significant defects or material found to be non-compliance. Undoubtedly, the SOX legislation requires a comprehensive and transparent business audit to approve the integrity and accountability of an organisation.

2.2.6 Evidence and Accountability

Understanding the notions of evidence from the legal perspective is crucial to prevent and avoid any legal consequences. Uglow (1997) defines evidence as those items of information which are presented to the court by the parties as a means of persuading the court that their argument is correct – in other words, information advanced to prove their case. He further explains that,

> *The court does not permit all information to be placed before it – it must be relevant, have probative weight, be non-prejudicial and not subject to any rule of exclusion. If the information possesses these characteristics, it is admissible evidence, often known as judicial evidence. The information placed before the court can be of different types: oral testimony by witnesses, normally their perceptions, especially what they have seen or heard, but perhaps also the opinions of expert witnesses;*

> *documents, often written but now frequently containing visual or sound recording or electronic data; real evidence, namely material objects such as fingerprints, automatic recording or a witness's demeanour. (Uglow, 1997:14-15).*

Although the number of electronic documents submitted as evidence is increasing, approval by experts is still required for admissibility in a court of law. This situation cannot last forever as more people are becoming familiar with ICT, and, getting approval from experts is time consuming and expensive, which delays proceedings. The judge in Regina v. Shepherd (1993), Lord Griffiths suggests that it will be very rarely necessary to call an expert and that in the vast majority of cases it will be possible to discharge the burden by calling a witness who is familiar with the operation of the computer. In this sense, the witness knows what the computer is required to do and that he can say that it is doing it properly (Uglow, 1997). There is further discussion on the admissibility of electronic records as evidence in courts of law in *Section 2.3.3 Electronic Records Management.*

Evidence is proof. Records provide evidence. This, however, has to be testified in a court of law by assessing record keeping metadata in order to ascertain the authenticity and integrity of evidential value in representing an event (Government of Canada, 2001). Further discussion is available in *Section 2.8.4 Authenticity and Integrity of Records*. Duranti (1998) asserts that records play a crucial role in most human endeavours and they are essential to all of our business and social interactions. Government functions and accountability, medical treatment and scientific research all depend on them. The International Council on Archives (ICA) Committee on Current Records in an Electronic Environment (2004) defines a record as 'recorded information produced or received in the initiation, conduct or completion of an institutional or individual activity and that comprises content, context and structure sufficient to provide evidence of the activity'. The National Archives of Canada defines a record as a document made or received in the course of the conduct of affairs and preserved (*Document d'archives*)[12]. The International Records Management Trust (IRMT) defines a record as a document regardless of form or medium created, received, maintained and used by an organisation (public or private) or an individual in pursuance of legal obligations or in the transaction of

[12] Glossary by the Canadian Committee on Archival Description can be found at http://www.cdncouncilarchives.ca/RAD_Glossary_revised_Aug2003.pdf (5 January 2005).

business, of which it forms a part or provides evidence. Meanwhile Currall *et al* (2002) define a record as a piece of recorded evidence or information, created or received by an organisation or person for use in the course of and subsequently kept as evidence of such transactions.

Although these definitions are slightly different, these commentators agree that records provide evidence by capturing sufficient content, context and structure accurately to represent a transaction. Context and content are vitally important to underpin the authenticity of a record. However, in order to be called a record there are certain criteria or standards required, which will be discussed in *Section 2.6 Phases of Records*. Organisations that take record keeping requirements for granted or neglect them might face serious consequences if their credibility is questioned by stakeholders. Records cannot simply be created to cover up inefficiency or wrong doings, as audit process is able to scrutinise every single metadata element relating to the records particularly, when a transaction is of highly suspicious. Eventually, evidence will be discovered.

Regular audits, however, should not scrutinise every single metadata as the cost would stack up against the benefit. Upward (2000) argues that electronic information systems used for conducting business are not necessarily designed to function effectively as recordkeeping systems. He further elaborates that if such systems are to support accountability requirements, recordkeeping systems must be designed to ensure the creation of adequate records and their capture, maintenance and accessibility over time. Similarly, to support accountability, Shepherd and Yeo (2003) suggest that records managers must assess the needs of the creator, the business unit and the organisation for records to provide evidence that the organisation has acted correctly and in accordance with its rights and obligations. This encompasses:

i. Compliance with the law and internal and external regulations
ii. Auditing requirements (financial audits, quality audits and other internal and external audits)
iii. Response to challenge (legal defence and handling of internal and external grievances or complaints).

In other words, more often than not the larger the organisation, the more difficult it is to sustain accountability as they are more exposed to greater public scrutiny.

Accountability is intimately linked to responsibility (Giri, 2000). He argues that it is not only about being accountable for what one is expected to do or perform, but to one's responsibility beyond the legal minimal, to the growth of oneself and the other and thus contributing to society. It is important for an organisation to demonstrate accountability not only to its shareholders and stakeholders, but also to the public as a part evident of social responsibility. Day and Klein (1987) elaborate six (6) general elements of accountability processes that can be distinguished are:

i. Trigger – there is an event that triggers the accountability process. For legal accountability the trigger may be that a citizen sues a government organisation for an inadequate decision, or alternatively, a process of political accountability may be triggered by press coverage or a disaster.
ii. Accountable person – someone is accountable or is held accountable for what has happened. In some cases, a minister may be held accountable by Parliament, in other cases the director of a government organisation may have to account for a decision to a court of law.
iii. Situation – there is an action or situation for which the person or organisation is accountable. A minister may have to explain why a certain decision was taken and why a disaster was not prevented.
iv. Forum – there is an accountability forum to which a person or an organisation is accountable. This forum may be the Parliament, a court of law, the media, the citizens, peers or scientists.
v. Criteria – accountability processes require that criteria are applied to judge an action or situation. These criteria may derive from the law but also from political standards.
vi. Sanctions – in some cases sanctions may be imposed on the person or organisation. A minister may be sacked, a government organisation may be forced to take another decision, or fines may be imposed.

Looking at all the six (6) elements, it is vital to avoid the first element that triggers the accountability processes. Triggers for accountability can range from failure to deliver a promise to dissatisfaction of one party against the other. Records management has a

pivotal role in responding to such triggers by capturing all evidence of a decision or action that has been taken. Good governance explicitly delegates responsibility to officials as the best way to hold individuals accountable.

Accountability processes occur self-evidentially after activities have been executed or decisions have been taken. Records must possess adequate content, contextual and structural metadata to be self-evident and to facilitate understanding of a particular transaction. Organisations are able to anticipate the information that may be required. Understanding business processes is certainly essential in helping to identify key records. In comparison to private organisations, public organisations are more exposed to the risks of being held to account, as they are answerable directly to the members of the public. Bearman (1993) argues that government organisations should not focus on structures but on business processes. From the accountability perspectives, government organisations have to provide 'evidence of business transactions'. They will put more efforts into creating, capturing and preserving documents concerning their decisions and activities.

It is essential to note that records management is not only about keeping but also destroying records. Anticipation plays a role in identifying whether or not to keep records, but too much anticipation might expose organisations to higher risks, if records required to sustain accountability are not in place. The task of identifying and preserving records to be used as evidence in the accountability process would be much more efficient if records management is a component of the management of risk. Indeed, records management underpins risk management by ensuring the availability of relevant records. Merging of records management and risk management will redeem the records management profession and functions in organisations with more explicit outcomes. There is further discussion on the relationships between records management and risks management in *Section 2.7 Risk Management and Managing Records.*

2.3 Records Management

Records management is the systematic control of all records from their creation or receipt, through their process, distribution, organisation, storage, and retrieval, to their ultimate disposition. Records management is fundamentally underpinned by record keeping activities to ensure records are properly captured and retrievable in a reasonable

response time. Records management has existed from ancient times in parallel with the proliferation of writing and recording technology. Records in whatever medium, the ancient clay tablets, vellum, papyrus, animal skin, paper, video, audio tape and film or today's electronic records, remained significantly important as evidence of business and administrative operations. Enormous production of electronic records triggers concerns among records management professionals that researching and establishing an appropriate approach for managing electronic records is imperative.

2.3.1 Document and Record

'Document' and 'record' are terms that are frequently used interchangeably. An understanding of these terms is essential to facilitate the capture of records that are judicial evidence of organisations. Foucault brought a new dimension to the notion of documents. He argued that in the past, the document was always treated as the language of a voice since reduced to silence, its fragile, but possibly decipherable, trace. Hynes (1996), quoting Foucault, states:

> *Document is not the fortunate tool of a history that is primarily and fundamentally memory... In our time, history is that which transforms documents into monuments. In that area where, in the past, history deciphered the traces left by men, it now deploys a mass of elements that have to be grouped, made relevant, placed in relation to one another to form totalities; it might be said, to play on words a little, that in our time history aspires to the condition of archaeology, to the intrinsic description of the monument. (Foucault, The Archaeology of Knowledge, 1972:7 cited in Hynes (1996))*.

Ability to allocate documents accurately within totalities helps historians to understand the documents and the contexts that contributed to their existence. These surroundings embrace the law, society, culture and civilization which influence human actions and reactions. In other words the understanding of documents or records leads to the understanding of systems, culture and civilization of the society that produced them. This concept is certainly useful in identifying accountability of any entity within the totalities.

Jenkinson (1949) describes documents as anything written or annexed to a writing, by whatever means that writing is made or reproduced. Modern inventions are extending

this definition inevitably to substitute for writing technologies such as sound recording. A more comprehensive elaboration by Buckland (1991) states the meaning of 'document' was addressed by bibliographers and documentalists in the documentation movement concerned with information storage and retrieval problems in the early twentieth century. One solution was to use 'document ' as a generic term to denote any physical information resource rather than to limit it to text-bearing in specific physical media such as paper, papyrus, vellum, or microform. Buckland claims that Otlet, Briet and other documentalists affirmed that:

i. Documentation (information storage and retrieval) should be concerned with any potentially informative objects;
ii. Not all potentially informative objects were documents in traditional sense of texts on paper; and
iii. Other informative objects, such as people, products, events, and museum objects generally should not be excluded.

Levy (2001) provides a much simpler elaboration by stating that documents are quite simply, talking things. They are bits of the material world - clay, stone, animal skin, plant fiber, sand - that we've imbued with the ability to 'speak'. Shepherd and Yeo (2003) also state their views, the term 'document' can be used in many ways and even some managers have used 'document' and 'record' synonymously. On the other hand, Barry (1996) claims that documents in preparation or at some early draft stage are not normally regarded as records, until such time as they are communicated into the business or corporate (institutional) domain for comment or action. He further states that a large majority of documents are also records. This statement means that there will be no document once a process has been completed. Instead, only records will be available. This definition seems unhelpful because people still use the term 'document' to refer to records.

Utilitarian definitions are perhaps more helpful for managing records. Robek, Brown and Stephens (1995) define a 'document' as the smallest unit of filing. The International Records Management Trust (IRMT) defines a 'document' as a unit of recorded information, while for the International Standard Organisation (ISO) (2001) it is recorded information or object which can be treated as a unit. The similarity of these definitions

that embrace documents and records supports smooth administrative and business operations.[13] Roberts (1994) provides two definitions of 'document'. First, a 'document' as recorded information, regardless of medium or form, a meaning that can be applied to both paper and electronic documents. The second definition is a 'document' as a physical record item or unit, perhaps in terms of a specific physical format. There is similarity between the definitions by Robek, Brown and Stephens (1995) and Roberts (1994), in that all the authors agreed a 'document' is a unit of filing. This definition covers the usage of the term 'document', when referring to a component in filing.

Above all, the notion of document from a legal perspective is essential. In the UK, the Civil Evidence Act 1995 section 13, states:

> … *'document' means anything in which information of any description is recorded and 'copy', in relation to a document, means anything onto which information recorded in the document has been copied, by whatever means and whether directly or indirectly.*

Apart from paper and its predecessors (parchment, vellum, stone, marble, clay and metal); film, photographs, video tape, audio tape, computer disks, fax, are all capable of being documents within the meaning of the Civil Evidence Act (Uglow, 1997). Records managers with the assistance from other professionals are expected to identify records of judicial evidence, in any format, to be kept for any subsequent possible legal requirements.

In records management, it is essential to understand the difference between a document and a record in order to facilitate record keeping activities. The National Archives of Scotland[14] provides an easy to understand description distinguishing a document and a record.

> *A document is any piece of written information in any form, produced or received by an organisation or person. It can include databases, websites,*

[13] Meeting ISO 15489 records management requirements is compulsory for an organisation in order to get ISO certification.
[14] http://www.nas.gov.uk/

> *email messages, word and excel files, letters and memos. Some of these documents will be ephemeral or of short-term value and should never end up in a records management system (such as invitations to lunch). Some documents will need to be kept as evidence of business transactions, routine activities or as a result of legal obligations, such as policy documents. This should be placed into an official filing system and at this point, they become official records. In other words, all records start off as documents, but not all documents will ultimately become record. (The National Archives of Scotland, 2006).*

Organisations are still at risk, though minimally, as only relevant records are kept and others will be destroyed. This suggests that collaboration between records management and risks management is vital for identifying records to be kept or disposed, because organisations are exposed to external scrutiny with relentless advance of audit society in both the private and of greater concern the public sector (Moss, 2005).

2.3.2.1 Digital Document

The phenomenon of ICT has resulted in the production of various types of digital documents as well as conventional paper documents. Buckland (1998) argues that attempts to define digital documents are likely to remain elusive, if more than an *ad hoc* pragmatic definition is wanted. A more comprehensive notion of document developed by Foucault is certainly useful for understanding their total complexity. A document is not only a single entity as it is seen, but its interpretation extends far beyond. Its relationships with other entities to form totalities are essential for a greater understanding of their content. In the electronic environment which cannot be seen by naked eyes, digital documents present a far more challenging and complicated situation. Due to the very nature of digital documents that are intangible and the instability of binary code, digital objects are prone to changes, both physically and electronically. Defining an object based on form, format and medium appear to be less satisfactory than a functional approach, following the path of reasoning underlying the largely forgotten discussions of Otlet's objects[15] and Briet's antelope[16]. Otlet (as cited in Buckland, 1998) stressed the

[15] Buckland refers to Otlet, P. (1937, 217) T*raité de documentation. Editiones Mundaneum, Brussels. Repr. (1989) Centre de Lecture Publique de la Communaute Francaise, Liege.*
[16] Buckland refers to Briet, S (1951, 8) *Qu'est-ce que la documentation? Editions Documentaires Industrielles et Techniques, Paris*.

need for the definition of document and documentation to include natural objects, artefacts, objects bearing traces of human activities, object such as models designed to represent ideas, and works of arts, as well as text. Briet (as cited in Buckland, 1998), a French documentalist, claimed that the catalogued antelope is a primary document and other documents are secondary and derived. Buckland comments that objects are ordinarily documents but become so if they are preserved for informational purposes. To this end, a digital object would only be meaningful when supported by adequate contextual information.

This claim is based on the understanding that in digital form, what appears on screen is not everything. The result must be supported with processes (algorithm or function) hence producing a digital document. Therefore, each and every algorithm or function has to be approved by a responsible entity to produce results that represent the intended business operations. Irresponsible parties can manipulate electronic data to generate the same result, which does not represent the actual operation. This situation can only be traced if a reliable audit trail exists. Audit trails are usually reviewed at regular time intervals or in response to accountability triggers[17]. Because the document is a part of a record series, its authenticity underpins the authenticity of all the records in the series. In a more complicated situation, such as in database environments, preserving authenticity of digital documents often requires records managers or archivists to draw statistically sound samples from the datasets to determine which of the actual files are to be preserved in the long term, while at the same time preserving the dataset to provide the overall context. As a consequence, the archivist's task will be complicated rather than simplified by the existence of large datasets of personal records (Moss, 1997).

The terms ‘digital’ and ‘electronic’ document are also used interchangeably. Most document management software uses the term Electronic Document Management System instead of Digital Document Management System. Even though both terms refer to the same conditions binary digits of 0s and 1s, the term ‘electronic’ is more widely used. The term ‘digital’ is frequently used to refer to digitisation, where documents are converted into digital form, with obviously the same electronic form. This might be the result of a conversion process which is known as digitisation, converting analogue into digital form. ‘Digitally born’ refers to objects electronically created rather than converted

[17] Further discussion is available in *Section 2.8.3.2 Audit Trail.*

into digital format. In other words, there is no absolute term. Either 'digital' or 'electronic' terms can be used to refer to the same situation or object. Even though both terms refer to the same processes, the term 'electronic' is more widely used.

The use of digital documents rather than their analogue equivalent in legal proceedings is far more complicated and challenging because of the very nature of digital objects. Police and Criminal Evidence Act 1984 section 69 (PACE S69) states that in any proceedings, a statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein unless it is shown –

i. there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer;
ii. that at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents; and;
iii. that any relevant conditions specified in rules of court under subsection (2) below are satisfied[18].

This section (69) can be satisfied by a certificate from 'a person in a responsible position in relation to the operation of the computer' that the computer was properly used and in proper working order and the original supplier of the information must not be available to give evidence[19]. Evidence of the proper working of the computer can also be given orally by a wider range of witnesses. Leroux (2004) asserts that to be admissible, digital records must possess all attributes of conventional evidence. They must: conform to legal rules; be authentic; be complete; be reliable (there must be nothing about how the evidence was collected and subsequently handled that casts doubt about its authenticity and veracity); and believable (understandable by the court).

This, however, is easier said than done. The British Computer Society (BCS) (2001), a leading professional and learned society in the field of computers and information systems, explains from its experience that the PACE S69 admissibility hurdle is so high

[18] Further information is available at http://www.swarb.co.uk/acts/1984PoliceandCriminalEvidenceAct.shtml (26 April 2007)
[19] Police and Criminal Evidence Act 1984, Schedule 3, Paragraph 8.

(showing that the computer was operating properly and was not being used improperly) that a competent challenge by the defence on technical grounds will often succeed in having the evidence ruled inadmissible. These conditions proved to be burdensome and the Law Commission (1997) proposed that the section be abolished[20] (Zander, 2003).

The BCS (2000), however, believes that it would be dangerous to repeal PACE S69, without first implementing a protocol for the handling of computer evidence in the criminal courts. This suggestion is similar to views by Walden (1993), MacNeil (1996), Duranti (2000) and InterPARES (2001) that to present electronic records of adequate weight for legal admissibility, organisations must ensure that adequate procedures and regulations are in place to enable maintenance, including the retention of computer programs, manuals and instructions in use when the records were originally created and stored. Indeed, the conformity to procedures and protocols, detailed record-keeping, provision of information in specified formats and access are essential if the reliability of records is to be safeguarded (O'Neill, 2002b). Whether fortunate or not, the PACE S69 eventually was repealed by the Youth Justice and Criminal Evidence Act 1999, section 60 and schedule 6[21].

2.3.2 Modern Records Management

Modern records management embraces the management of records in any form. As we have seen, the emergence of modern records management stemmed in part from the need of archivists to help organisations identify records of archival value (Norton, 1956). The definition of archives advanced by Posner (1972) that 'archives' are non-current records because of their permanent value, and have been transferred to an *ad hoc* agency, called archives, which have been internationally adopted. However, the use of *ad hoc* qualification is no longer relevant as the existence of archives, particularly national archives, at least in modern times are deliberately planned by governments for the custody of national archive collections. Posner's definition draws a line between records and archives that subsequently led to different approaches to meet different requirements and demands for managing records and archives. According to Schellenberg (1956), there are several reasons for an archival establishment:

[20] Law Commission. (1997). *Final Report: Evidence in Criminal Proceedings: Hearsay and Related Topics*, No. 245, Cm. (3670), cited in Zander (2003).
[21] Police and Criminal Evidence Act 1984 [amended – as at February 2003].

i. For the practical need of improving governmental efficiency – centralised custody of archives.
ii. Cultural purpose e.g. the records of the *ancien régime* in France were considered as public property, were kept primarily for cultural purposes.
iii. Personal interest - public records obviously define the relations of the government and the governed. They are the ultimate proof for all permanent civic rights and privileges; and the immediate proof for all temporary property and financial rights that are derived from or are connected with the citizen's relation to the government.
iv. Official – records are needed by a government for its work. Records provide evidence of financial and legal commitments that must be preserved to protect the government[22].

Schellenberg (1956) further elaborates that records are efficiently managed if they can be found quickly and without fuss or bother when they are needed, if they are kept at a minimum charge for space and maintenance while they are needed for current business, and none are kept longer than they are needed for such business unless they have a continuing value for research or for other purposes such as evidence of accountability of governments or organisations. Records management is thus concerned with the whole life span of most records. The only thing not mentioned by Schellenberg (1956) is where to keep records of continuing value, that is, archival records, for future access. The emergence of the national, departmental and local archives, stimulated by Posner's definition of archives, fulfils the role of providing access to archival records in the public sector.

A standard for selecting archival collections is essential to ensure that records which provide evidence of governmental operations are consistently retained for posterity. Demonstrating consistency of processes of government and organisational administration is essential in guaranteeing equity for the governed. Such transparency can be achieved, sustained and demonstrated if records are consistently managed. Both top level administrators, who are concerned with major programs, and the lowly clerks, who are concerned with routine transactions, need reliable records for their work.

[22] Although Schellenberg's *Modern Archives: Principles and Techniques (1956)* was published sixteen years before Posner's *Archives in the Ancient World (1972)*, his discussion of records management is very similar to today's approach for managing records and archives.

Evidence of all transactions, high or low level, must be kept not only for current business activities, but also for future needs, especially possible legal proceeding.

Records are needed to provide evidence of the implementation of policies and procedures established by strategic and tactical management levels. Records from operational level are required for reports of accomplishments and performance, and to record all phases of the government's dealings with the particular parties involved in its transactions. Records on policy and procedural matters – on general as distinct from specific matters – are difficult to assemble, to reorganise into recognisable file units, and to identify in such a way that their significance will be apparent. Records of routine operations, on the other hand, are easily classified. A sound classification and filing system ensures that records stored can be retrieved. Schellenberg (1956) explains that the earliest American filing systems were quite simple and corresponded somewhat to the registry systems used in Europe during the same period.

However, Schellenberg (1956) further explains that gradually the simple alphabetical and numerical systems were replaced by more complicated systems – the Dewey-decimal, the subject-numeric, duplex-numeric and others[23]. There was no uniformity of system as organisations adopted different systems to suit various requirements. Today, there are several standards, either internationally or nationally, for managing records, such as ISO 14589; national standards such as BS ISO 14589, AS ISO 14589. Even, the US Department of Defence (2002) established its own standard for managing records in electronic environment, known as DoD 5015.2-STD[24].

Records management activities are of a highly specialised type, requiring specialised competencies and a specialised experience. In every large and complicated government organisation, therefore, a special staff should exist somewhere in its administrative hierarchy concerning itself exclusively with providing leadership for all agencies in their handling of records and information. This recommendation, if implemented, would

[23] Dewey-decimal classification system is widely adopted for managing library information resources; subject numeric system is used for managing records, where documents are arranged by related subjects in the encyclopaedic fashion and assigned numbers to maintain their sequence; and duplex-numeric is also employed for managing records, and it uses encyclopaedic arrangement with subdivisions for each major category. Dewey-decimal was used for filing in the whole UK Foreign Office until the introduction of personal computers (Moss, 2009).

[24] See no. 10.

contribute to economical and efficient administration by ensuring availability of records whenever required. Unfortunately, it does not seem imperative to many governments as the benefits are less than explicit. Today's advanced ICT products with easy storage and speedy retrieval simply overshadows the long-established conventional records management practices. It is evident that information systems are managed by ICT professionals and not records management professionals. Thus, it is not surprising that records management is not acknowledged by many.

The purpose of records management staff are to make records serve the needs of accountability and to dispose of them after those needs have been served. Having a qualified records management staff in government organisations would be beneficial, as recommended by Jenkinson (1949) as appraisal of records of archival value should be conducted by individual departments rather than overwhelming archival institutions with the task[25]. Records of archival value are less likely to be accidentally destroyed. This is mainly due to the ability of the records management staff and support from other professionals within the individual departments who are conversant with the nature of their business.

Arguably this might lead to inconsistencies across departments as appraisal are conducted by various officials, but, if centralised appraisal is to take place, there are not enough officials to perform the task, and they might not get adequate support from other professionals within the organisation. Although the roles and importance of records in providing evidence for both public and private organisations is crucial and well proven, the numbers of professionals employed are less than satisfactory. Managing records should be a shared responsibility, not because records management professionals have limited knowledge, but more important is achieving effective and economic administrative at minimal cost. Support from other professionals, especially ICT professionals, is needed to help identify pertinent records for organisations to sustain themselves and remain competitive.

[25] This, however, requires a huge financial resources and it is doubtful if it can be implemented without commitment from the government.

2.3.3 Electronic Records Management

Today, application of computers in workplaces is almost inevitable, even in a small organisation, for at least word processing tasks. Medium and large scale organisations normally implement their own networking systems. In these situations, besides paper records, various types of electronic records are produced everyday in the conduct of daily business. In public organisations, the implementation of e-government in many countries has contributed to the production of a mass of electronic records[26]. Ross (2006) calls attention to trust in the accountability of e-government and its success depends upon transparent, secure and workable digital curation[27] mechanisms within public sector environment. The need for a sound management of electronic records is imperative.

As electronic records by their very nature are intangible, a comprehensive and holistic approach to item creation and management is essential to ensure electronic evidence is accurate, authentic and sustainable like their paper counterparts. Principles and approaches used in managing conventional records can be used for managing electronic records, though it may require adaptation to suit different electronic environments. To remain competitive, organisations cannot afford to lose their records, and electronic records are particularly at risk due to their unstable (volatile) binary nature. Managing electronic records, just like their paper equivalent, requires support and cooperation from senior management and other professionals. Procedures and guidelines alone are not enough to achieve organisational goals, if responsible officials do not consistently follow them.

---

[26] e-Government and electronic records are synonyms due to mass production of electronic records by various electronic applications across government departments. Electronic records simply overwhelmed paper records in a hybrid environment. Unfortunately, managing electronic information shadows the importance of managing electronic records in today electronic information world. The reason behind it is, electronic information is mainly, or perhaps solely, managed by IT professionals, with the main focus on information storage and retrieval. On a higher level, there is no regulation imposed to mandate records management, especially in government departments. Records management professionals are given less rooms to contribute to the efficiency of administrative in organisations.

[27] Ross (2006) describes digital curation encapsulating the many activities involved in caring for digital entities such as selection, documentation, management, storage, conversion, security, preservation, and provision of access. Curation focuses not just on preserving digital entities but on keeping them functional, supporting their continuous annotation and maintaining their fitness for purpose. Preservation is a lot narrower in focus.

Electronic records present a complex and never ending task for records management professionals due to their intangible nature and the fast changing technology that supports the creation and future use. The emergence of various types of electronic documents demands efficient management to retain their accuracy and authenticity as evidence of transactions and the accountability of officials or organisations. Metadata is the in-thing or core to ensure the authenticity and durability of electronic records. The ability to capture and retain adequate metadata is certainly crucial for the preservation of electronic records over time[28]. Preservation is comprehensively discussed in *Section 2.8.4.2 Preservation of Records.*

2.4 The Records Life Cycle

The process of capturing evidence of functionality and accountability traditionally begins with the creation or capture stage of records. Over time, records accumulate more additional information about the document, such as who has had access and its relationships to other documents, especially contextual metadata, as they pass through later stages of maintenance and disposition. Comprehensiveness and consistency in capturing such metadata information is essential to ensure the long term authenticity, integrity and reliability of records. Furthermore, records of archival value may eventually be sent to archives for research and posterity. There are two models of records management: the first is the 'life span' of records that was advocated by Schellenberg (1956) half a century ago; the second is the record continuum concept which emerged in the 1980s and 1990s (Upward, 1997). The life cycle model portrays the record as going through various stages or periods, much like a living organism (Figure 2.4a)[29].

[28] Preserving electronic records means preserving their availability, accessibility and understandability. Availability of storage media, on which records are stored does not guarantee accessibility of records, as appropriate hardware is required for accessing them e.g. 5 ½ inch floppy disks need appropriate drives to access records stored. Accessibility does not guarantee understandability as appropriate software is required to present stored records in an understandable fashion. This has led to different approaches by various parties, e.g. InterPARES, in efforts to ensure the survival of electronic records over time.

[29] The figure of the records life cycle by the IRMT is confusing as it did not explicitly explain the sequence of recordkeeping activities. The archives phase is not even developed.

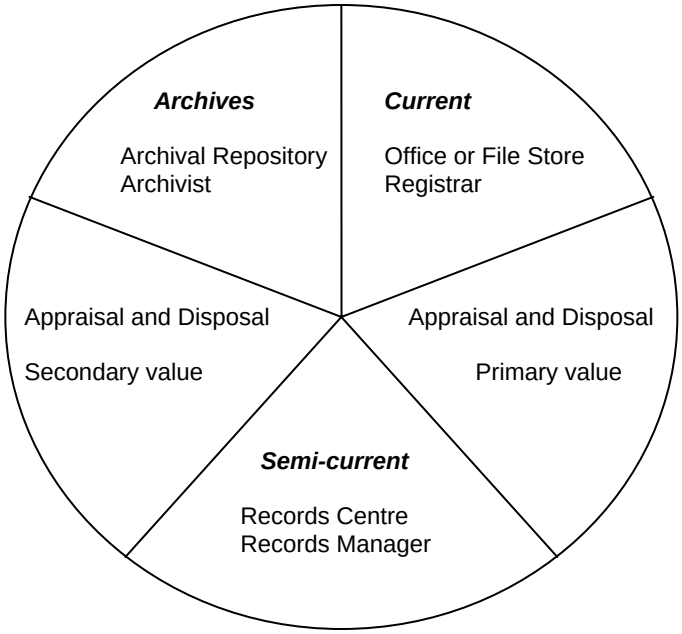

Figure 2.4a: The life cycle concept of records (© IRMT, 1999).

In brief, there are three phases of the life cycle of records: current; semi-current; and non-current (IRMT, 1999). The first phase is also known as active records, which comprise records that are regularly used for the conduct of the current business of an organisation or individual. The creation of records is presumably for a legitimate reason and according to certain standards or protocols. These records will normally be maintained in or near their place of origin, or in a registry, or records office. Appraisal and disposal process, which take place during and at the end of the current phase, determine records of continuing value and records of no further value. Records of continuing value will then be relegated to the next phase, semi-current.

On the other hand, records of no further value will be destroyed. The second phase is also known as semi-current records, as the name implies, are records that are infrequently referred to in the conduct of current business, and they will normally be maintained in a records centre or other offsite intermediate storage pending their ultimate disposal. Finally, another appraisal and disposal process will take place in order to identify records to be transferred into the third phase, that is non-current or also known as in-active phase. This is another determining point, when a decision has to be taken

as whether to destroy or send the record to archives, which is reserved for inactive records with long-term indefinite value. This small percentage of records (normally estimated at approximately five per cent of the total documentation) is sent to an archival repository, where specific activities are undertaken to preserve and describe the records (IRMT, 1997).

Another model of the records life cycle is from North America, by Read-Smith, Ginn and Kallaus (2002) (Figure 2.4b). The model consists of five phases; they are creation, distribution, use, maintenance and disposition. According to the model, the first stage is the creation stage, which includes records that are internally produced or received from external parties. The second stage is distribution, where records are then distributed to the persons responsible for their use. The third stage is use, where records are commonly used for decision making, documentation or reference, in answering inquiries, or in satisfying legal requirements. When a decision is made to keep a record for use at a later date, it must be stored, retrieved and protected – three key steps in the maintenance stage, that is the fourth stage. Records must be stored (filed), which involves preparing and placing records into their proper storage. Whenever a request is made for a record, it must be retrieved from storage for use. When the retrieved record is no longer needed for active use, it may be re-stored and protected, using appropriate equipment and environmental and human controls to ensure record security

The maintenance stage also involves updating stored information and purging or throwing away obsolete records that are no longer useful or which have been replaced by more current ones. The last stage of this model is disposition. After a predetermined time has elapsed, records to be kept are transferred to less expensive storage sites within the firm or to an external records storage facility. At the end of the number of years indicated in the retention schedule, the records are disposed of, either by destruction or by transfer to permanent storage. The facilities, where records of an organisation are preserved because of their continuing or historical value, are called the archives.

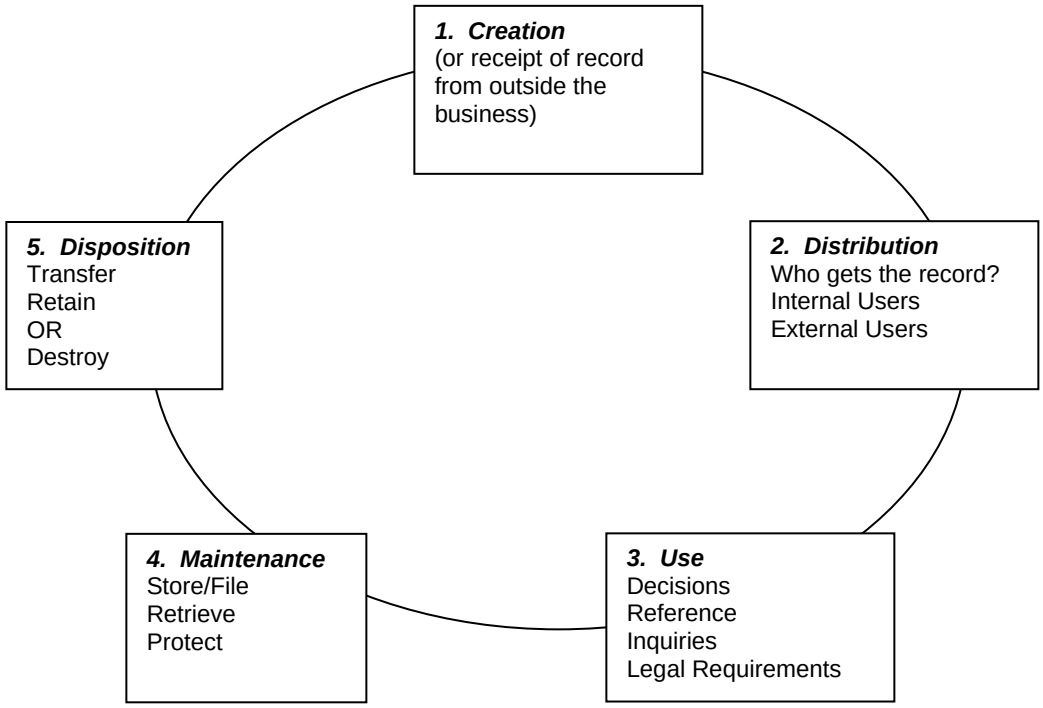

Figure 2.4b: The record life cycle (© Read-Smith, Ginn and Kallaus, 2002).

Although the underlying concept of both models is the same, their difference is mainly a matter of approach. The variants between these two models can be seen in Figure 2.4c. The first model (IRMT) is used in the UK and many Commonwealth countries, excluding Australia. It is based on the principle of pre-action aggregation and routing of records, which is widely implemented through the registry system (Reed, 2004; Tough, 2005). Meanwhile, the second model which is used in North America, is based on individual action followed by post-hoc filing (Tough, 2005). Figure 2.4c attempts to converge the two models: the former model comprises three phases and the latter model comprises five. However, scrutinising the phases and the nature of activities involved, reveals the following:

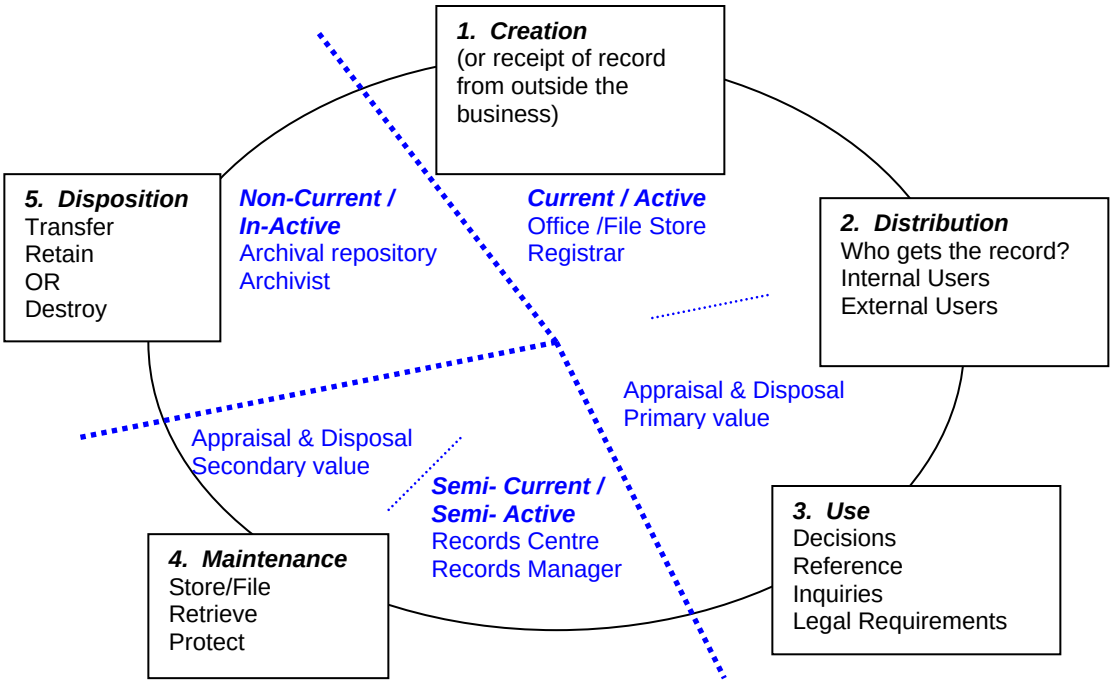

Figure 2.4c: Combination of the life cycle models: The life cycle concept of records (© IRMT, 1999) and the record life cycle (Read-Smith, Ginn and Kallaus, 2002).

i. Current / Active Phase

Based on the nature of activities involved, the current / active phase embraces the first phase of the North American's model, these are the creation phase, the distribution phase and the use phase. Current / Active records are frequently accessed and used for various purposes as stated earlier. In the light of providing efficient administration at the most economical cost, records which have served purposes for which they were purported to be created, will then be appraised to determine records to be transferred to a record centre for further storage. Appraisal and disposal[30] must be undertaken with an awareness of the functions the records served and their context in relation to

[30] Disposal is not synonymous with destruction, though that may be an option. It is also known as disposition in North America.

other records; and must also be based on their primary value[31]. This in turn enables organisations to dispose of records of non-continuing value in accordance with disposal schedules and practices. Appraisal and disposal activities are clearly stated in the IRMT model, but not the North American's model.

ii. Semi-current / Semi-active Phase

Records of continuing value are then transferred to a record centre for further storage, hence leaving more room for new records in the operational departments. During this stage, records will be held until they have fulfilled their disposal schedule. In the records centre, records are organised and stored in such a way as to facilitate retrieval. However, at this stage records are still not available for public access. As records from various departments are gathered together, it is therefore crucial to retain their contextual information in order to maintain their integrity as evidence. Records are stored according to *respect des fonds* principles, which maintain their contextual and transactional information. Another appraisal and disposal processes take place at the end of the semi-current / semi-active phase. Different from the previous appraisal process in the current / active phase, the focus of appraisal process in this phase is to identify records of secondary value[32]. The North American's model, again, does not state this necessity instead, only features storing or filing, retrieving and protecting activities in a phase named maintenance. This might give the misleading impression that

[31] Primary value is the continuing utility of records or archives, by virtue of their contents, for the transaction of the business that gave rise to their creation. It can be further sub-divided into three categories: (1) Operational (Administrative) value – for the continuance of the administration or operations of the creating agency or a successor in function or as evidence thereof; (2) Fiscal (Financial) value - for the continuance of the financial or fiscal business of the creating agency or a successor in function, or as evidence thereof (such as for audit), and; (3) Legal value - for the continuance of the legal business of the creating organisation or a successor in function or the protection of its legal rights or those of its employees or third parties (IRMT, 1999).

[32] *Ibid*. Secondary value is the enduring value that records or archives possess, by virtue of their contents, for purposes other than the transaction of the business for which they were created. Secondary value also can be further subdivided into three categories: (1) Evidential value – value of records or archives in providing information on the origins, structure, functions, procedures and significant transactions of the organisation that created them; (2) Informational value – value of records or archives for reference and research deriving from the information contained in them and often incidental to their original purposes; (3) Intrinsic value – value of records or archives by reason of their age, historical associations, physical form and features, aesthetic or artistic quality or monetary value.

all records are kept from the creation to disposition (the only time disposition appeared in the model!).

iii. Non-current / In-Active Phase

The North American's model of life cycle final phase is disposition, which involves transferring, retaining or destroying records accordingly based on an appraisal process (which is not even stated in the model). Records of secondary value, also known as archival records, will then be transferred to an archival repository for permanent retention. These records are known as archives and may be accessible to members of the public, but not necessary as not all archives are open by right to public access. However, managing archives is a separate activity though it is closely related to records management. It is not the purpose of this dissertation to address it in-depth.

Comparing the models reveals that the North American's model, arguably, is not as comprehensive and is less descriptive than the IRMT model. The absence of appraisal and disposal processes in the model might lead to confusion as people might think that records are simply transferred into next stages without having passed any scrutiny. Understandably, these absences reflect the characteristics of records management in the US that does not have appraisal in their record life cycle[33]. On the other hand, the IRMT model is more comprehensive and descriptive as all entities in the three stages are clearly stated, including the appraisal and disposal processes at the end of the current /active and semi-current / semi-active phases. Nevertheless, the differences between the two models are less profound when the life cycle concept is compared with the more recent records continuum thinking.

2.6 Phases of Records

The life span of records varies depending on the types of records and the purpose of the organisation. However, all records undergo similar phases in their life span before they will be either permanently destroyed or transferred to archives. The phases are as follows:

[33] The OAIS model by Consultative Committee for Space Data Systems, provides explicit features of an archival system that contains several packages for various purposes, such as Submission Information Package (SIP), Dissemination Information Package (DIP) and Archival Information Package (AIP). For further information, please explore *Reference Model for an Open Archival Information System (OAIS)*. Available at: http://public.ccsds.org/publications/archive/650x0b1.pdf (21 June 2007).

2.6.1 Creation or Capture

Records provide evidence of accountability and ensure the smooth operations of an organisation by providing efficient access to information that meets legal and regulatory requirements. Records must be complete, accurate and reliable over time to become evidence of organisational transactions. The traditional registry system has proved its significant contribution in ensuring the authenticity and integrity of records, whilst the electronic records management system is struggling to replicate or produce such a sound and stable system. Fisher (2004) states in the electronic environment, if the integrity of the filing cabinet can be demonstrated, then anything stored or recorded in the filing cabinet inherits the integrity of the filing cabinet. This, in turn, could be demonstrated by following a standard that identifies how electronic records are to be recorded or stored and the nature and purpose of the electronic records.

The backbones of the registry system is a comprehensive file plan structure, which together with record keeping procedures enable the capture of adequate metadata, particularly contextual metadata that underpins the meaning of records. Craig (2002) notes that re-creating the original web of contexts for records is clearly difficult because many ties, firmly rooted in practice but not in text, are first hidden and then lost as time passes by[34]. A record must be captured during or immediately after a transaction occurs to avoid any details being lost, which may affect subsequent retrieval. At this point, in the electronic environment, metadata needs to be added to identify and define documents, providing its context, its purpose, where it is located and the (automatic) management of its retention and disposal[35] (Currall *et al*., 2002). The Effective Records Management Project team at the University of Glasgow concluded that creation is the best place to assign metadata to documents. The cost of capturing adequate metadata retrospectively is simply too high and it is unlikely that resources can ever be found to do so. If there are tools, such as automated systems for producing adequate metadata, then long-term management might be cost-effective and straight-forward.

[34] Craig (2002) states a fabric of relationship, some recorded and some not, combined everyday to hold people in an understandable relationship with their world. To understand the meaning of a record, contemporary users, regardless of the interest which they use archives, need to have clear views of the intricate web of contexts in which records were made and kept as extensions of people as they acted and communicated.

[35] The Effective Records Management Project team at the University of Glasgow implemented an electronic records management system that emphasizes the use of metadata to underpin the authenticity and integrity of electronic records.

Record keeping metadata is structured or semi-structured information which enables the creation, management, and use of records through time and within and across domains. Furthermore, record keeping metadata can also be used to identify, authenticate, and contextualize records; and the people, processes and systems that create, manage, and maintain and use them (Wallace, 2000). Similarly, McKemmish, Cunningham and Parrer (1998) state that recordkeeping metadata includes all standardised information that identifies, authenticates, describes, manages and makes accessible documents created in the context of social and business activity. Metadata is continuously generated as records pass through time reflecting every action that has occurred affecting an individual record. Electronic records in particular, are not self-explanatory and do not possess the look and feel of their physical counterparts. This makes the process of capture more crucial and it must be done consistently and systematically. Record keeping processes demand both intellectual and clerical efforts. In regard to the traditional registry system, Craig (2002) reflects:

> *Registry clerks generally handled all physical jobs related to the control and movement of files, while a registrar, sometimes called the librarian, classified records, controlled the vocabulary used for titles and references, and ensured documents and information were ordered within the files upon receipt and before putting them away in storage areas.*

Similarly, in the electronic environment, the task of classifying records and assigning semantic metadata which demands intellectual knowledge must be done by a qualified or professional records official. Some metadata, particularly technical metadata, may automatically be captured as record keeping system which can be customised to meet local situations.

Managing records is not all about managing record keeping activities *per se*, but it also requires managerial effort, such as establishing policies and regulations for records management, at the corporate level both organisationally or nationally. A prerequisite for the implementation of any of the proposed strategies for managing electronic records should be based on policies which address issues of concern such as the assignment of accountability for record keeping, the definition of roles and responsibilities, the

expression of rules for record keeping (an enormous challenge in an electronic work environment where it is difficult to define the latent work processes upon which such record keeping rules can be defined), the incorporation of archival considerations, the development of functional requirements, not to mention the standards, practices and systems for facilitating the implementation of the requirements, and finally education and training strategies (McDonald, 1999). Policies and regulations at both national and organisational levels would certainly strengthen records management's role in managing evidence of organisations.

Critical business functions are usually exposed to higher risk. Such business processes require detail documentation to ensure the accuracy, authenticity and integrity of records. Understandably, ensuring the accuracy, integrity and authenticity of paper records is less problematic than their electronic counterpart, mainly due to the very nature of electronic records. Unfortunately, in the present digital world, most records are created electronically, and they are easily created by anyone with access to a computer. It is more difficult to control the creation of records in a distributed computing environment[36] than a networked computing environment[37], even when rules and regulations are in place[38]. An ethics philosopher, O'Neill (2002b) asserts conformity to procedures and protocols, detailed record-keeping, provision of information in specified formats and access are essential to safeguard the reliability of records. Her concern was noted by Schellenberg (1956) half-a-decade ago when he insisted that:

> *The efficacy of a records management program is dependant on the earnestness and competency of its staff. The more sincere and able the*

[36] In a distributed computing environment, only minimal verification procedures take place such as user password and identification. There is little control or interventions by system administrators as all computers operate individually. Although rules and regulations are in place, the actual creation of records process is hugely exposed to human errors. In a large organisation, it is extremely difficult to control individual machines without a central hub of system administration. Consistency of the creation process must be assured if records are to be made identifiable and retrievable.

[37] In a networked computing environment, activities of all users are recorded by the system used. Procedures can be made compulsory to ensure the consistency of the creation and use of records. Audit trail is available to allow an investigation whenever required. A networked computing is much safer than distributed computing as it facilitates centralised control and monitoring, though its initial cost is much higher.

[38] MacNeil (1996), Duranti (2001), InterPARES (2001) and O'Neill (2002b) assert that authenticity and integrity of electronic records are mainly assured through conformity to procedures and regulations.

> *staff, the more effectively will records be classified and filed for current use; and the better they are classified, the more easily they can be disposed of after they have served current needs. The better the staff, the sounder will be its judgements on the disposition to make of records. The extent to which sound judgements are made depends on the professional competency and thoroughness with which records are analysed. (Schellenberg, 1956:47).*

Therefore, it is important to ensure every individual involved acts responsibly to ensure the accountability of an organisation. Ironically, Schellenberg (1956) further states that it is a curious anomaly that the more important a matter, the less likely is a complete documentation of it to be found. While modern technology has aided the making and keeping of records in many ways, it has also made unnecessary the production of many documents that once would have become part of the record of an action. Much that influences the development of policies and programs never makes its way into formal records. Important matters may be handled orally in conferences or by telephone, an instrument that has been referred to by Paul Hasluck, Australian Ministers for Territories, as the 'great robber of history'[39]. This analogy is more likely applied to any form of electronic communication, was proved in the report of the inquiry into the circumstances surrounding the death of Dr David Kelly in regard to Britain's declaration of the war on Iraq. The report reveals poor record keeping practices in the Ministry of Defence, particularly the Defence Science and Technology Laboratory (DSTL) by stating:

> *Paragraph 8.4.1*
> *It is important to dispel any impression, however unfounded, that there is a conflict of interest between a particular activity and the responsibilities of an employee. There is no exhaustive list of activities that fall into this category, but it is in everyone (sic) interest for individuals to seek approval before indulging in any such activity and to ensure that records are kept. (Hutton Report, 2004:8).*

[39] Schellenberg (1956) quotes Paul Hasluck on 'Problems of research on contemporary official records' *Historical Studies: Australia and New Zealand*, V, No. 17 (November, 1951), p.5.

The report also disclosed anxiety of an official, Dr. Brian Jones, who in a letter to the Deputy Chief of Defence Intelligence stated that:

> *The Foreign Affairs Committee appears to consider it important that the Foreign Secretary told them, "… that there had been no formal complaint from members of the security and intelligence services about the content of the [September 2002] dossier." I believe his evidence was, in fact, that he was not aware of any such complaint, and there is no reason to suppose he should have become aware of mine. Nonetheless, it is now a matter of record, and I feel very uneasy that my minute could be uncovered at some future date, and that I might be judged culpable for not having drawn attention to it*[40]*. (Hutton Report, 2004:316).*

There are two issues related to this situation. First, whether or not records have been accurately captured according to established procedures. Second, responsibility can be delegated to individual officials, but not accountability, as it resides squares on the shoulder of the employer. Individual officials can only be blamed if they failed to comply with procedures and guidelines, but in the eyes of the public it is the employer that has the greater responsibility.

Records management concern is that records must precisely represent the event, and in the name of democracy, the people of a nation must be able to trust such records. Initially records are produced as an integral part of an organisation's operations and eventually those with archival value will be kept in archive for reference in the future. Inaccurate record keeping has repercussions for the role of records centres and archives in providing evidence for users in the future. Records centres and archives have no power to attest to the veracity of records, particularly the content and context in which they were created, as that responsibility lies with the operational divisions. Conformity to procedures and regulations is essential to ensure the production of complete and reliable

[40] The issue of accuracy of records, responsibility and accountability of officials and organisations is closely inter-related. The anxiety of Dr David Kelly that people might judge him as the culprit of the case reflects the status of the establishment of the dossier (September, 2002). Dr Kelly knew exactly what went on, that there is not enough underpinning evidence. The conclusion by Lord Hutton of poor recordkeeping practices in the Ministry of Defence bears out everything as what was suggested by Schellenberg (1956) that it is a curious anomaly that the more important a matter, the less likely is a complete documentation of it to be found.

records. In a distributed computing environment, users are not electronically monitored and they are free to use any machine to create records if no password authentication is required. This makes conformity to record keeping procedures uncertain. Wallace (1990) asserts that without early identification and intervention an electronic record may not survive. Equally it may survive, but may not contain all relevant information that was inherently contained in a paper-based record system. Failure to control the creation of records usually means failure to retain accurate records that subsequently affects the retrieval process. Hence, frequent monitoring is essential to ensure record keeping activities accord to procedures and guidelines being practised across an organisation.

To support accountability, record keeping systems must be designed to ensure the creation of adequate records and their capture, maintenance and accessibility over time (Upward, 2000b). The only really effective manner to achieve this is to build the archival and record keeping requirements into the system before the records are even created and in a fashion that will not obstruct the functioning of the organisation (Cox, 2001). Record keeping is a natural outcome of a series of related tasks (many of which are increasingly automated) that themselves are supporting the business functions and activities of the organisation (McDonald, 1999). Apart from meeting the specific record keeping requirements, the system must also comply with internal and external regulations. The process of creation and capturing of records would be more effective with the participation of records management professionals together with other parties such as operation managers, in the development of record keeping and information systems, as system developers are rarely aware of specific records management requirements, and it is usually necessary to specify additional functionality beyond the standard configuration of the system (Bantin, 2001).

Like developing a library system and other customised software, input from practitioners in the fields, particularly regarding the functional requirements, is essential if the final system is to be fully effective and efficient. McDonald (1999) argues that the establishment of policies, business rules, and functional requirements coupled with a sound understanding of the culture of the organisation and its record keeping requirements (from both the operational and accountability perspectives) are prerequisites in the processes used to identify and acquire the relevant technology solutions. Records management professionals know exactly what system is needed to

keep records intact over time. Based on their input, the record keeping system will be designed and developed by the software developer either using the traditional system development life cycle or prototyping a new approach. Apart from the functional requirements, adequate controls must be put in place to ensure the records in the system remain intact and secure.

Comparing the traditional records life cycle and the records continuum it may be concluded that the latter is more suitable and practical to deal with records in electronic environment. The reason is, the records continuum advocates that the requirements for a record keeping system must be identified ahead of the system designing stage. This is to allow these requirements to be embedded into the system, which subsequently facilitate later record keeping activities such as assigning retention periods, control of access and appraisal before disposal. Upward (2000a) supports this claim by stating that records continuum encompasses the concept of managing a record from the point of design of a recordkeeping system, that is, before records are even created, through to disposal and the continuing use of records as archives.

Theoretical discussion about metadata is not as complex as implementing or testing their practicality in the real world. Theoretically, it may be as easy as providing a template and control vocabulary, and describing which metadata fields will then be completed by relevant employees at various stages. Practically, it is about more than completing those metadata fields as the consistency of records and high level of commitment from both operational staff and the management are important factors for the system to be sustainable. Based on first hand experience, McDonald (1999) asserts that consistency of metadata captured can be assured through the use of icons or wizards or templates. Similarly Currall *et al*. (2001), based on the experience of ERM project, explore the use of wizards, templates and macros in Microsoft Word to aid the document creator to produce a well structured and consistent record with adequate metadata at the creation stage.

The types and number of metadata fields required may vary depending on the nature of transactions and organisations. Bantin (2001) argues that it cannot be assumed that all such systems are capable of collecting a full range of metadata as their developers (software engineers) are rarely aware of records management requirements, and it is usually necessary to specify additional functionality beyond the standard configuration of

the system. Systems, particularly in an electronic environment, therefore, must be customised to meet different record keeping and legal requirements.

2.6.2 Distribution

Once a record is created, it is then distributed to a party or parties responsible for its use. These parties could be both internal and external parties as activities might involve entities from outside the organisations. It is essential to record the parties involved in a particular transaction because contextual information, apart from content and structure, is critical to support understanding of the records. Securing adequate contextual information within which records are created is critical to the understanding their purpose and nature of their existence. More importantly, when the information is of a highly confidential category, the name and details of each recipient must be recorded appropriately. Such contextual information of electronic records is less visible, electronic records must be further scrutinised to disclose contextual information. Some contextual information of electronic records, such as hyperlinks, may not be permanently available depending on the availability of the contextual source.

2.6.3 Use

Records play an important role in ensuring consistency and smooth administration of an organisation. Schellenberg (1956) emphasises that records are needed for the transmission of policies and procedures to be followed, reports of accomplishment and performance of staff from below, and to record all phases of an organisation dealing with particular parties involved in transactions. Records are used for decision making, for reference and documentation, answering inquiries and in satisfying legal requirements. Records may be used repeatedly over time, especially during their active or current phase. Active records are stored in the operational office as they are frequently accessed by relevant officials. Electronic records are stored in folders that replicate directory structures in the paper world. However, not all records can be accessed by all employees. Therefore, access control must be in place to ensure that records are accessible to authorised officials only. In a traditional paper environment, controlling access means a record officer must verify individual user, to check whether he or she is allowed or not access to a particular record. It is a repetitious process that requires careful checking on users' profiles to ensure they cannot gain access to records beyond their capacity. It relies mostly on human factors to maintain consistent security.

As records are stored in various operational departments, it is therefore, crucial to ensure officials who control access to records are aware of their responsibility to provide access only to those who are authorised. Meanwhile, in an electronic environment, the process of controlling access is much easier as electronic systems can be configured to verify users' profiles every time they try to gain access to a particular record. In the light of audit requirements, electronic systems capture every log and are able to track down all activities that have taken place within the system. Depending on the level of confidentiality of information, various user identification and password authentication methods, from common alpha numeric to sophisticated biometrics verification, are being used to ensure only authorised officials can gain access to information. Audit trail provides vital information for an investigation to identify illegal activities and misbehaviour by users. Further discussion on audit trail is available in *Section 2.8.3 Audit and Internal Control.*

2.6.4 Maintenance

Maintenance of records has a great impact on the smooth administration and operation of an organisation as it involves the storage, retrieval and protection or preservation of records. Records that have to be kept for subsequent use must be systematically stored to facilitate later retrieval. These processes would be easier to accomplish if records were appropriately classified at both macro level and item level at an earlier stage, especially at the time of creation. Organisation could suffer from difficulties in retrieving records that are not systematically stored. When the number of records accumulates, the problem would gradually emerge. The retrieval process, in turn, consumes longer time and thus affects the smoothness of the administration and decision making process. Large organisations suffer from poor record keeping very quickly as huge numbers of records are produced daily. No organisations can remain competitive if retrieving records for decision making frequently encounters difficulties and worse if they are not retrievable at all. It is, therefore, crucial to have systematic record keeping procedures and guidelines in place before an organisation begins operations. The fact is organisations pay less attention to managing records until they are hit by a crisis or are in a complete mess, where evidence required cannot be found on demand. The reason is in most cases organisations can still survive without having a proper records management program. In other words, they are not aware of the benefits of a records management

program. A strategic and holistic approach is required if record keeping processes are to succeed.

Generally, it is always easier to store than to retrieve information, regardless of its form. In a paper environment, records exist physically, meaning that they can be seen by the naked eye. On the other hand, due to the very nature of electronic records that are intangible, only systematic design and comprehensive record keeping procedures can ensure that their existence can be identified and verified over time. In an electronic environment, although various information or database systems provide retrieval utilities, they are not the same as having a comprehensive record keeping and file plan structure that enables a better classification and storage of records. Understanding the file plan structure means understanding the business processes, and understanding the business processes means understanding the business of an organisation[41]. This is certainly helpful in appropriately classifying and storing records.

2.6.5 Disposition

Disposition or disposal refers to the actions that are associated with implementing decisions about the retention or destruction of records. Shepherd and Yeo (2003) suggest it may also include migration and transfers of records to new storage locations, custodians or owners (ISO 15489-1:2001, clause 3.9; AS 4390.1-1996, clause 4.9). Disposition of records greatly relies on records retention schedule that allocates the length of time they should be kept. After completing their retention periods, records of secondary value will be transferred to archives for permanent storage. Although it is so-called permanent storage, these records still can be re-assessed depending on current and future circumstances. Traditionally, disposition process does not encounter problems as physical records can be dealt with both at item and group level. Electronic records, on the other hand, due to unavailability of retention schedule in most information system, are vulnerable to non systematic disposition.

Destruction of records must be undertaken according to procedures and guidelines to ensure records that are supposed to be permanently destroyed, are permanently destroyed. Authorisation and verification of the destruction process must be recorded as

[41] McDonald (2002) states that understanding records begins with understanding business processes, and understanding business processes begins with understanding the business of an organisation.

evidence that the process conforms to procedures and regulations required, and also to ensure the status of records is traceable. The destruction method of paper records could be done by shredding, pulping or incineration. However, destroying electronic records, due to their very nature, requires more attention. Deleting files from electronic directories does not permanently delete them as such files can be resurrected.

Even emptying 'recycle bin' for 'permanently destruction' still does not permanently destroy the files. Currall (2005) argues that deleting an electronic record does not delete it permanently, but what actually happens is only the removal of the pointer to the electronic records, thus, making the record irretrievable, and giving the impression that the records have been deleted. Indeed, a record can only be permanently deleted by overwriting the record with another record, or by destroying its physical storage media[42]. Shepherd and Yeo (2003) suggest that electronic records can be erased by reformatting, degaussing or physically destroying their physical storage media. Understandably, as technology changes and new inventions continuously pour into the market, the techniques and methods for destroying electronic records will change over time.

2.6.6 Post-custodial

Traditionally, records of archival value that have served their current and semi-current needs will then be physically transferred to archives for permanent custody. These records are then identified as archives and they are managed by archivists, who are at the receiving end. However, the emergence of the continuum concept has spurred debates on the appropriate approach to the management of archival records. Tough (2004) states that the continuum regime insists the transfer of records from their creators into the custody of archival institutions is no longer necessary, nor even desirable, in the context of electronic record keeping. The continuum regime insists that if archival records in an electronic environment are to be safely secured as archives, archival institutions can no longer wait for electronic records to become non-current before considering them for permanent preservation as they might find there were no longer any records left[43]. Understandably, the records continuum regime firmly and consistently

[42] Currall argues the paradox of electronic records is that it is virtually impossible to permanently delete them, as it is to permanently keep them.

[43] Tough (2004) quotes Greg O'Shea in Erlandsson (1996) stating ' … the duty of archivists is to facilitate the management of the records in an accountable way, regardless of where they are located, in other words engaging with bureaucracy, and not stand back from the safe distance of

insists on the integration of records management and archival processes as a better solution for dealing with records in an electronic environment. Cunningham (1997) states that what used to be thought of as the historical recordkeeping end of the life cycle has been re-conceptualised in such a way that historical considerations can now be applied from the moment records are created.

In the post-custodial stage, records will be permanently preserved for their social and historical memory (Cook, 2006) as well as for research and accountability purposes. It is essential that the integrity and authenticity of records be appropriately captured at all the previous stages, and preserved properly over time. In the continuum model, archives remain in the individual institutions as access is not a problem in an electronic environment. Intellectually, this does not present obstacles to access to archives, provided suitable system safeguards are in place. Moss (2005) suggests that there should be a centralised control, possibly in the National Archives, to approve requests to access to archives that are stored in various locations[44]. Decentralised archives would release the responsibility of the National Archives as the sole custodian with limited human resources to manage enormous collections of national archives. However, this plan would require adequate and consistent controls and monitoring in order to achieve an ideal situation where archives can survive and accessibility be assured, irrespective of the location of the records.

Tough (2004) rightfully concludes that the one thing that unites the two schools of thought is recognition of the need to preserve the integrity and evidential value of records. It is necessary to focus on context rather than content. From a diplomatic perspective, the integrity and authenticity of records are very much dependent on metadata captured. Theoretically, the records continuum model may have a better approach in dealing with archival electronic records rather than the life cycle model. Tough (2004) argues that discussions on this matter are only at the theoretical level with little reference to empirical evidence and applicability in differing institutional settings and

---

the archival 'keep'. If archival institutions are were to sit back and wait for electronic records to become non-current before looking at them they might find there weren't any records.' (Listserv Archives, 14 February 1996, quoted in A. Erlandsson, Electronic Records Management: a literature review (Paris, 1996), Chapter 8, 'The issue of custody or post-custody of electronic archives'.

[44] Personal discussion with Michael Moss on August 2, 2005 at 3.00 p.m. in Room 201, HATII, University of Glasgow.

cultures, or even to different record types. The continuum model may encounter problems over time, until it matures. That is to say, the stability of the model can only be proven once records have reached the archival stage as the continuum regime claims that archival records can be identified as early as their creation. This can only be achieved if all metadata captured from the creation stage and beyond enables the system based on the continuum model, to function as theoretically anticipated. The system must be able to retain archival records over time to enable electronic archival records to finish in the place or space that they should be. There is, therefore, still a long way before the real world continuum model reaches stability. Only then the claim by the continuum regime that archival records do not need to be transferred to archival institution will be answered.

2.7 Risk Management and Managing Records

Risk is the chance of things going wrong, either bad things happening or good things not happening. Perception of risk influences a person's decisions and behaviour. Organisations, both in the public and private sectors, need to perceive risks in order to reduce uncertainty and to achieve economic operation and the sustainability of the organisation. Risk refers to the uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to influence the achievement of an organisation's objectives[45]. The success of risk management is partly dependent on the accuracy of records in organisations, as every judgment made must be based on reliable information. In an age where transparency, accountability and compliance are of increasing concern, it is essential for organisations to comply with regulations and, if they do not, to be able to explain why.

Risk does not end when a particular business process or transaction has been completed, but remains as a threat to the organisation until all the records are destroyed. Furthermore, some records will remain as they were 'active' for ever as archives, thus presenting endless risk, particularly to public organisations. The implementation of the FOI legislation in any jurisdiction where users have rights to access relevant records is a wake up call to the public sector to ensure that they are prepared for any consequences. It would be useful for an organisation to prioritise its business functions and identify risk

[45] Treasury Board of Canada Secretariat (2001). Available at http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/riskmanagement/rmf-cgr01-1_e.asp (15 Sept 2005).

associated in ensuring the sustainability of an organisation. A comprehensive and strategic risk management strategy is required if risk management is to achieve its full potential. The application of the strategy should be embedded into the organisation's business systems, including strategy and policy setting processes, to ensure that risk management is an intrinsic part of the way business is conducted (HM Treasury, 2004). Sampson (2002) suggests that in order to function effectively, future records managers need a wider range of business management skills and a high level of technical expertise in a number of areas, including information technologies, changing regulatory and legal issues and requirements, and the evolving information needs of the organisation. Although it will be a long and time consuming process, providing up-to-date academic and training programs is certainly a useful way to train multi-skills records managers.

2.7.1 What is Risk Management?

Traditionally risk management is about controlling loss and the financial status of an organisation, and is implicitly linked to the insurance industry (Mehr[46] and Hedges, 1974; Meulbroek, 2002). During the 1960s, companies began to employ risk managers because of the increasing cost of insurance. Thompson (2003) states during this time, multinational companies decided that corporate managers and overseas insurance brokers are needed to manage risk internationally. However, at this stage one of the key barriers faced by organisations was the lack of risk management experience and such qualifications as there were tailored to insurance managers. The change in emphasis from insurance management to risk management was slow and poorly received by senior management, due to the continuing focus on insurance controls and lack of understanding.

In the 1970s, corporate mergers and acquisitions resulted in new and unexpected risks, as the underlying nature of the business of corporations changed after merger or acquisition. Organisations quickly moved beyond buying insurance as the only risk control solution, and adopted alternative methods, such as loss prevention, loss control, and operational risk management. Then, in the 1990s, risk management expanded

[46] Mehr (1974), Professor of Finance claimed that he was first to advocate risk management in 1955, when he first published a full scale book on risk management in the insurance industry. Rationally, it is not a surprised as insurance companies are constantly exposed to uncertainly of potential claims. Hence, a comprehensive and systematic method for assessing risks is essential to reduce uncertainty and increase competitive edge in business.

further to cover areas such as industrial safety, hazard analysis and environmental planning in response to tightening controls and external pressures. Thompson (2003) also asserts that risk management now relates to the harm that may be suffered by any type of facility or activity because of an unforeseen (or indeed predicted) event, and it has been accepted as part of management science.

One of the key drivers for risk management is the necessity to comply with international legislation and expected standard of corporate governance that require organisations to demonstrate greater accountability and transparency in their dealings. However, it is dangerous to confine risk management with compliance, risk management is about clarity and the ability to not only identify the correct opportunities but also to maintain discipline in pursuing them (Sharon, 2006a). Hence, the biggest risk of all is to take no risk, and thereby fail to take opportunities. Organisations have recognised the need to respond to the effects of competition and economic change by reviewing their overall cost of business. Risk management has also become an integrated part of strategic corporate governance to ensure the integrity and accountability of organisations while at the same time pursuing organisational goals (OECD, 2001a, 2004).

Sampson[47] (2002) defines risk management as a business management function or process that analyses the costs, risks and benefits of alternatives in order to determine the most desirable or appropriate course of action. Risk management is about making decisions that contribute to the achievement of an organisation's objectives at the individual activity level and in functional areas. It assists with decisions such as the reconciliation of science-based evidence and other factors; costs with benefits and expectations in investing limited public resources; and the governance and control structures needed to support due diligence, responsible risk-taking, innovation and accountability (Treasury Board of Canada Secretariat, 2001). Risk management should be a continuous and developing process which runs across the organisation's strategy and its implementation. It should address methodically all the risks surrounding the organisation's activities past, present and in particular, its future.

[47] Karen L. Sampson heads Scenarios by Sampson, a consulting firm in Parker, Colorado. Formerly manager of records and administration for a major airline and earlier a consultant associated with other firms. She holds advanced degrees in library administration and secondary education; and has published widely on business practices. Such wide experience enables her to advocate the significant contributions of records management alongside risk management.

The UK HM Treasury's Orange Book (2004) states that risk management is not a linear process; rather it is the balancing of a number of interwoven elements which interact with each other and which have to be in balance with each other to be effective. Specific risks cannot be addressed in isolation from one another as the management of one risk may have an impact on another. Similarly, Meulbroek (2002) also states that risk management will not achieve its full potential and benefits if conducted by various individual departments across an organisation, because it tends to be tactical rather than strategic. Tactical risk management has limited objectives, usually the hedging of specific contracts or of other explicit future commitments of the firm; strategic risk management addresses the broader question of how risk affects the value of the entire business. She further elaborates that incorporating more risks results in an integrated risk management system that must embrace all risks that affect value. Operational risk, product market risk, input risk, tax risk, regulatory risk, legal risk, and financial risk compose the broad classes of risks faced by most organisations. These risks in aggregate form the overall risk exposure of the firm.

The management of risk at strategic, programme and operational levels needs to be integrated so that the levels of activity support each other. The *hierarchy of risk* model (Figure 2.7.1) suggests that the higher the hierarchy, the higher the level of uncertainty. Understandably, it is the nature of the tasks that determines the level of uncertainty. The project and operational level has the lowest degree of uncertainty as a result of highly procedural tasks and decisions which are usually operationally limited. Decisions made by project and operational managers are based on statistical data, hence, uncertainty mainly depends on the accuracy and reliability of data used. Programme level is exposed to higher uncertainty due to the choice of alternative methods or mechanisms that can be used to achieve strategic decisions made by the top management. Meanwhile the strategic level, usually the level of board of directors, focuses on strategic decision that determines the direction and sustainability of the organisation. Evidential information in the form of records is the main substance of such decision-making. Records at the operational level are used by the middle management, and their records in turn form key elements of such records that could then be used as evidence by the board of directors.

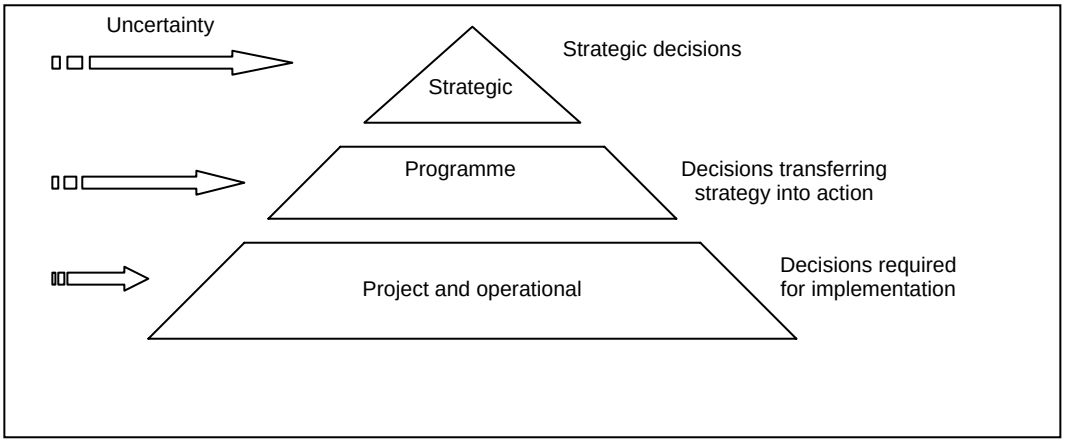

Figure 2.7.1: Hierarchy of risk (© Strategy Unit, UK, 2002).

As risk is unavoidable, every organisation needs to take action to manage risk in a way that can be justified to a tolerable level. Risk is not limited to internal threats. It is essential to be sensitive to any changes in the external environment and to the actions of competitors. It is also undeniable that the assessment of all these risks is dependant on the accuracy of the evidential information available, which is the product of systematic and comprehensive record-keeping and monitoring procedures. Risk is prioritised based on the likelihood and the impact of occurrence. Business operations of high level likelihood and impact should be given highest priority, whereas business operations of least likelihood and impact should be given least priority or perhaps tolerable to the organisation. There are four ways to deal with risk, namely: treat, take, terminate and transfer (Currall, 2006a). Indeed, it is the prerogative of the management of an organisation to decide how to deal with its risk exposure.

2.7.2 Elements of Risk Management

The risk management process consists of a series of activities to achieve organisational goals. AIRMIC, ALARM and IRM (2002) provide an explicit model of risk management processes (Figure 2.7.2). It is a cyclical experience, which allows modification of every process over time to meet organisational goals. A formal audit process will provide a check and balance for ongoing risk management activities. AIRMIC, ALARM and IRM (2002) advocate that risk management protects and adds value to the organisation and its stakeholders by:

- providing a framework for an organisation that enables future activity to take place in a consistent and controlled manner,
- improving decision making, planning and prioritisation by comprehensive and structured understanding of business activity, volatility and project opportunity/threat,
- contributing to more efficient use/allocation of capital and resources within the organization,
- reducing volatility in the non essential areas of the business,
- protecting and enhancing assets and company image,
- developing and supporting people and the organisation's knowledge base,
- optimising operational efficiency.

The most crucial part of risk management is risk assessment, which consists of two major activities that are risk analysis and risk evaluation. In risk analysis, the process of identifying risk is the trigger for subsequent activities. AIRMIC, ALARM, IRM (2002) state:

> *Risk identification sets out to identify an organisation's exposure to uncertainty. This requires an intimate knowledge of the organisation, the market in which it operates, the legal, social, political and cultural environment in which it exists, as well as the development of a sound understanding of its strategic and operational objectives, including factors critical to its success and the threats and opportunities related to the achievement of these objectives. Risk identification should be approached in a methodical way to ensure that all significant activities within the organisation have been identified and all the risks flowing from these activities defined. (AIRMIC, ALARM and IRM, 2002:5).*

In essence, risk management is a continuous process, and therefore, risk assessment should be documented in a way which records the stages of the process. The Orange Book (2004) states that documenting risk assessment creates a risk profile for the organisation which:

- facilitates identification of risk priorities (in particular to identify the most significant risk issues with which senior management should concern themselves);

- captures the reasons for decisions made about what is and is not tolerable exposure;
- facilitates recording of the way in which it is decided to address risk;
- allows all those concerned with risk management to see the overall risk profile and how their areas of particular responsibility fit into it; and
- facilitates review and monitoring of risk.

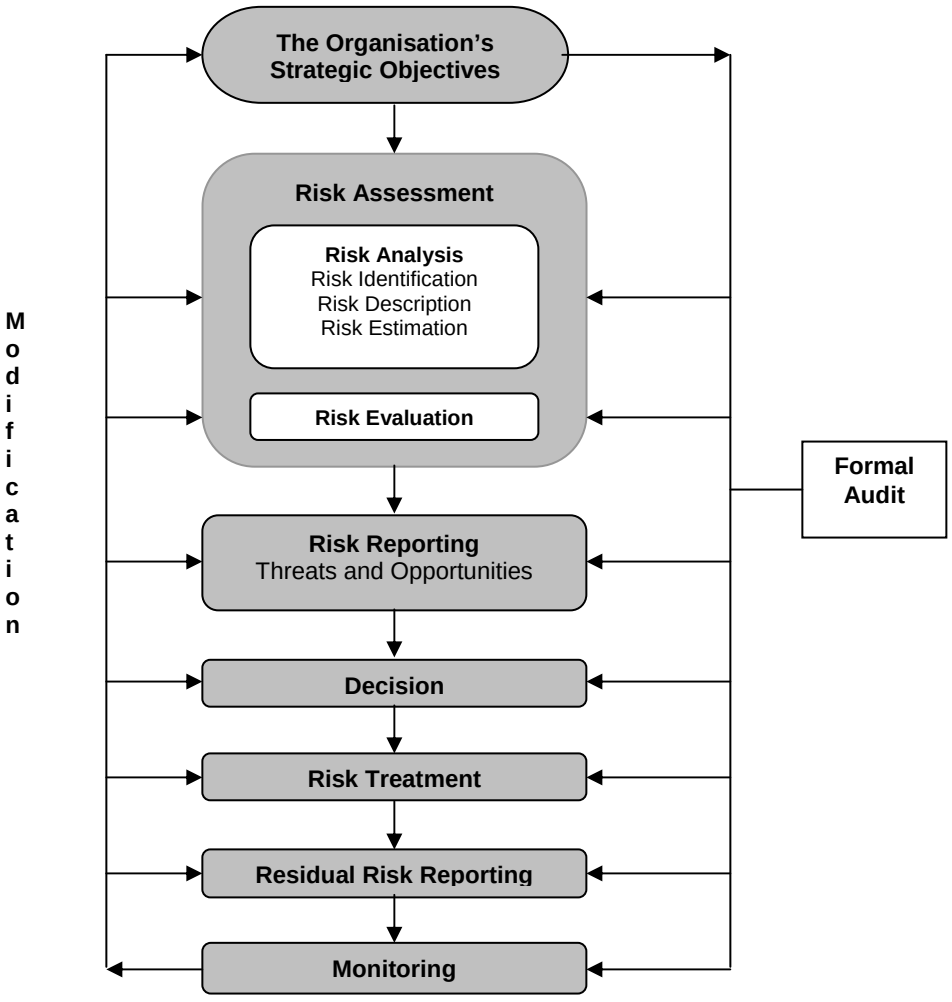

Figure 2.7.2: The risk management process (© AIRMIC, ALARM and IRM, 2002).

Theoretically it is complicated enough, but, practically it is even more complicated to secure pertinent and accurate records, which will allow a precise methodical assessment

to identify risks across an organisation. Risk description and risk estimation are the output of risk identification, which is then used in risk evaluation to compare the eliminated risks against risk criteria which the organisation has established. Subsequent activities of risk management are risk reporting, decision making, risk treatment, residual risk reporting, and monitoring, depending on the ability of the risk management team to assess and make judgement based on information available, both from internal and external resources. General perceptions cannot be used as the basis for identifying risk as they are not necessarily accurate. Decisions on the types of risk present must be based on empirical and methodical assessments of available records.

The effectiveness of risk management can be measured by conducting a formal audit, be it internal or external[48]. Audits should enable business improvement by identifying weaknesses and providing suggestion for improvement to current situations. Further discussion on audit is available in *Section 2.8.3 Audit and Internal Control.* Decisions or actions taken must be based on empirical evidence to avoid exposing the organisation to unexpected risks as a consequence of inaccurate information used in assessing risk. Lion and Meertens (2005) reveal that risk avoiders selected more positive information than risk takers, contrary to the general assumption that as risk avoiders focus more on the worst outcomes, then they would prefer negative information about risk. Risk takers, on the other hand, would prefer positive information about the risk. However, trends of information seeking differs depending on the circumstances, hence systematic and methodical assessment is deemed necessary to determine the types of records required. This is to say that, an extent record must be made available for users to choose from.

Mehr and Hedges (1974), both economists, explained that the process of analyzing an organisation's present exposure is usually called risk analysis. It needs to be done economically and effectively. It is folly to waste time and other resources in accumulating information that is not needed to accomplish the objectives. From the information and records management perspective, risk analysis would not achieve its goals in the absence of accurate records. Managing records must be given priority and adequately

[48] A newly released Digital Repository Audit Method Based on Risk Assessment (DRAMBORA) toolkit by the Digital Curation Centre (DCC) (http://www.dcc.ac.uk) and DigitalPreservationEurope (DPE) (http://www.digitalpreservationeurope.eu) would be useful for facilitating internal audit by providing repository administrators with a means to assess their capabilities, identify their weaknesses, and recognise their strengths. Further information can be found at http://www.repositoryaudit.eu/download (17 April 2007).

supported if risk management is to succeed. Simon (1999) rightfully pointed out as a company grows, the money invested in such systems (information systems) should grow commensurately. It may seem wasteful at the time, especially since success makes risk seem so remote, but it is money well spent. Unfortunately, many managers do not learn this lesson until it is too late. Radner (1992) argues that, although managers in a firm have many different functions, one of the most important is that of processing information. He further advocates that information processing is a huge decision-making machine that takes signals from the environment and transform them into the actions to be taken by the 'real workers'. The most effective way to make risk management central to an organisation is to make the process integral to the organisation's decision-making process that is central to all organisational activities especially records management. The role of a records manager is definitely integral to ensuring the availability of accurate and authentic information to underpin the decision-making process.

2.7.3 Relationship between Risk Management and Managing Records

Nevertheless, a record management team often faces difficulties in convincing senior management of the importance of its role. Records management used to be a departmental rather than an organisational issue. Problems and difficulties of managing records cannot be solved individually. Instead concerted efforts must be made to attain maximum benefits across an organisation. Today, the contribution of records management seems to be more explicit; the collapses of Enron and WorldCom have had a significant impact on the future of records management through the coming into force of the SOX which is not limited to American companies only, but touches all publicly quoted concerns across the world that trade with the US. The SOX legislation advocates good corporate governance and accountability; and the integrity of financial and accounting systems of public organisations. These requirements can only be fulfilled if the records and information that reside in the systems are authentic and reliable. Boards of directors and senior managers have now come to realise that documentation of business activities and records retention is an essential requirement of the Act.

In the wake of the SOX Act, CEOs are much more likely to regard records management as an essential function, one that they must initiate, fund and manage. The Act contains a number of important provisions, including mandated retention requirements for certain types of records (Stephens, 2005). His claims are proved by the findings of surveys and

models of business solutions by leading IT consultants. A survey undertaken by Gartner entitled 'Corporate Governance Spending Disrupts Software Purchases' reveals that records management and enterprise content management are regarded as the technologies that can contribute most to corporate governance (Figure 2.7.3a) (Getronics, 2005)[49]. For records and information management community, this is not a surprise as they have for long insisted that good record-keeping is fundamental for effective and efficient administration. The problem was (and may be is), according to Stephens (2005), many corporate executives were inclined to regard records management as a discretionary endeavour, one unrelated to the overall success of the business and therefore unworthy of their attention.

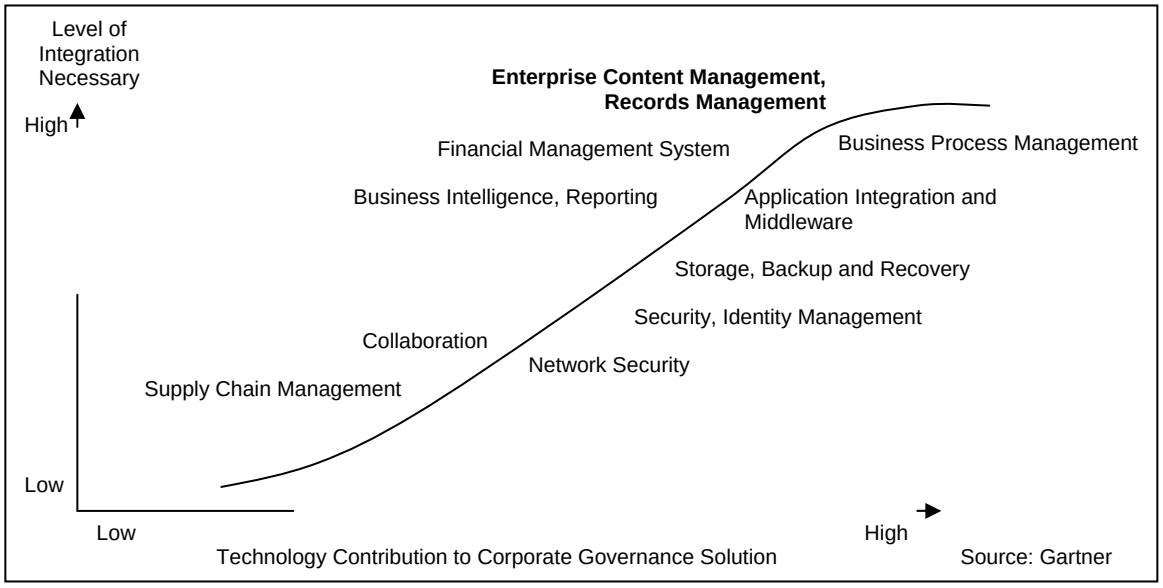

Figure 2.7.3a: Corporate governance technology components (© Getronics, 2005).

The root of today's problems is mainly a consequence of electronic forms of information. With complicated information systems across organisations, information is always at managers' finger tips. The birth of various types of information management systems, such as electronic document management, knowledge management, integrated document management, content management and enterprise content management

[49] Getronics is one of the world's leading providers of vendor independent Information and Communication Technology (ICT) solutions and services. Getronics designs, integrates and manages ICT infrastructures and business solutions for many of the world's largest global and local companies and organisations, helping them maximise the value of their information technology investments. Further information available at http://www.getronics.com.

systems, have all sidelined its fundamental ingredient, that is records management. Colledge and Cliff (2003) assert that suppliers and industry analysts can all accept some of the blame for the confusion in the market place and the loss of recognition of the importance of records management. Good record-keeping practices have been neglected, hence exposing organisation to risks from various quarters. Records are not given proper retention periods, thus making monitoring and control of record movements ineffective. The need to integrate record keeping requirements into information systems is imperative if another Enron-like collapse is to be avoided. Although the cost for having such an integrated system is high, the cost of failure to manage records effectively could be much higher as the organisation failed to grab opportunities and is exposed to indefinite risks.

Meanwhile, Sampson (2002), who viewed risk management from the records management perspective, asserts that:

> *Records and information management is a function of risk management when it is designed to minimise risks related to information security threats and government or court actions. It enables a proactive approach to potential adversities, rather than a knee-jerk reaction in a crisis. It weighs the cost, benefits, and risks of various record-keeping practices against the relative value of various record groups. Such analysis identifies those practices that will provide the most flexibility within the legal, ethical, and practical constraints. (Sampson, 2002:169).*

In the case of Enron, accounting firm Arthur Andersen was found guilty by a U.S. District Court in Texas of destroying Enron-related documents that Andersen knew (or could reasonably have anticipated) would be relevant to a Security Exchange Commission investigation (Watzke, 2005). Records were prematurely destroyed yet under the SOX Act, no records should be prematurely destroyed. The penalties if this is proven for individuals or companies are fines or imprisonment for up to 20 years, or both. Under the SOX Act, the board of directors is accountable for any action and business operation performed. Moss (2006a) has pointed out that risk cannot be delegated through an organisation, as those who are fiduciarily accountable for its management have to take

responsibility for any failure. It is no longer possible for them to claim that they are unaware of wrong doings by their officials.

Indeed, an holistic business management approach is desperately required to resolve such concerns. Oracle, one of the leading business solution vendors, produces a compliance architecture model as an option for business solution which they claim will ensure adequacy and compliance with the SOX Act (Figure 2.7.3b). The model by Oracle suggests that an holistic and orchestrated approach is required for a business to succeed.

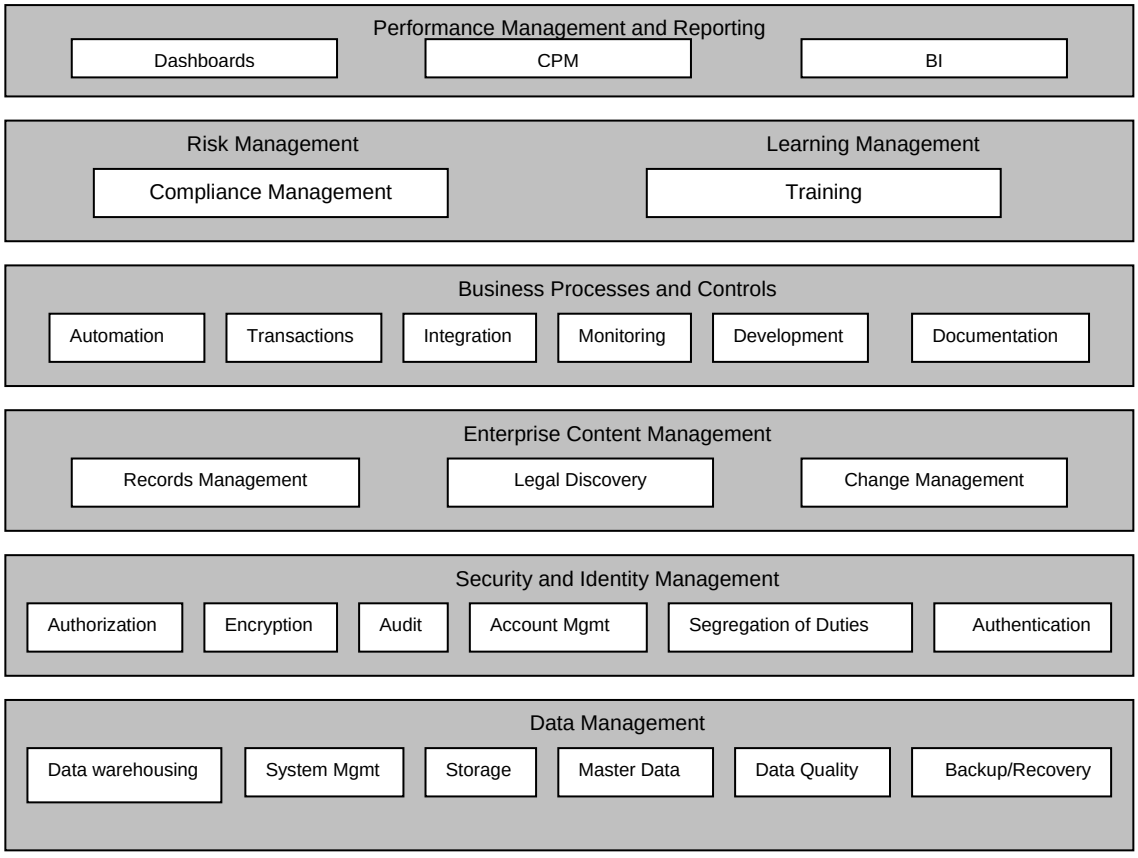

Figure 2.7.3b: Oracle Compliance Architecture – comprehensive, sustainable compliance (© Oracle, 2005).

The relationship between records management and risk management is explicitly shown in the records management which is considered an integral part of enterprise content management that underpins business processes and controls and which, in turn, underpins risk management. Rationally, decisions to keep or not to keep records must

take into account the legal needs, which accords with the risk management objective of minimising risks, as records can be used in self defence or to challenge others.

In the Oracle model it is taken for granted that the accuracy and integrity of records is highly dependant on the security and controls put in place within the systems to ensure that they cannot be tampered with. In addition, electronic records are assured to be constantly under threat as software and hardware deteriorate or become obsolete. It is proposed that there is no single digital preservation solution that fits all circumstances, thus an organisation must initiate suitable preservation methods for the safekeeping of their electronic records. It is undeniable that this model and the findings of Gartner's survey suggest a significant role for records management by ensuring accuracy and adequacy of records, not only to underpin risk management, but as importantly to ensure that organisational goals can be achieved.

Sampson (2002), who explores the relationship between these two fields, asserts firmly that the main contribution of records management to risk management is through records retention schedules, which allocate suitable retention period to various records, notably, perceived threats of litigation. Egbuji (1999) states that it will be very costly for an organisation to protect all of its records. Moss (2005) asserts that even in an era of more open government, it is inconceivable that compliant procedures can be applied uniformly as they simply cost too much. Moss further explains that audit committees will take a view that it is not worth the cost of keeping information, even if required by statute, as there is little risk of anyone wanting access.

Records must be destroyed at the time specified, as the function of records management is not just about keeping records, but also destroying in a timely and secure way, so as to achieve economic efficiency that determines the sustainability of an organisation. Hence, an organisation needs to institute a record protection activity that will use such resources as are available to identify and secure valuable and sensitive records as long as they remain valuable and sensitive. Employees cannot be blamed for destroying records according to the retention schedule as that responsibility lies with the board of directors of the organisation and in many cases comply with criteria set externally.

Risk management assists the identification of critical business functions, which in turn, identifies the level of importance and related risks. Reed (1997) suggests that not all processes generate records, and it is the role of records management working within a risk management framework to identify how far each process should be recorded. However, this role cannot be accomplished in the absence of commitment from managers of various departments across an organisation. In addition, identifying critical business functions and keeping their records are two separate tasks that require different professional qualification. Departmental managers must identify their critical business functions, and records managers are responsible for ensuring that these functions are captured accordingly for smooth operation and to meet legal requirements.

Sampson (2002) states:

> *Risk management of records enables a proactive approach to potential adversities, rather than a knee-jerk reaction in a crisis.*
> *Risk analysis should ask these questions:*
>
> - *What records truly merit protection because of their content and value?*
> - *What are the risks if the information is available, if it is not available, or if it falls into wrong hands?*
> - *What is the likelihood of litigation or investigation, and how long? and*
> - *Will there be sufficient evidence for a defence or to file a claim?*
>
> *(Sampson, 2002:169).*

A records retention schedule is an essential tool that facilitates systematic destruction of records. However, producing the schedule requires a comprehensive effort to ensure that records first fulfil their business and legal requirements prior to their destruction. In order to underpin risk management, an interwoven activity, knowledge of managing records, solely, is not adequate to enable records managers to produce a convincing and useful retention schedule. Developing a records retention schedule requires legal advice and expertise to weigh the costs, litigation risks, and benefits of retention time periods to determine the most reasonable retention period for individual record categories (Sampson, 2002). To this end, interactions with other professionals are not only

unavoidable but desirable, 'complementary rather than competing' (Murdock, 2006). It is, however, usually costly for an organisation frequently to take legal advice. Alternatively, an internal audit and risk management committee can be formed to ensure adequacy and compliance with all regulations. Further discussion on audit is available in *Section 2.8.3 Audit and Internal Control*. Retaining records as long as possible is a strategy based on the assumption that the records will be more helpful than harmful to the company. Some organisations may prefer not to keep certain records as their non-existence will not present any legal risks. Even, if there is risk, if it would not cost more than the cost required for keeping those records, these classes of records would normally be kept for a shorter period of time to meet their business functions. In such situation, risk is tolerable.

Davies (1999) states many companies have lost their 'corporate memory' and have found themselves repeating errors made in the past. There is a growing awareness of the value of knowledge and experience, and of the need to capture it for the company to use when the people in which it resides have left its employment. Although Davies advocates knowledge management to ensure the capture of the 'corporate memory', the underlying activity is records management that plays an essential role in capturing memory by documenting all necessary components of 'corporate memory'. Tombs (2004) strongly advocates the effectiveness and contribution of knowledge management systems. He asserts that records management has proved its usefulness because it reflects the real world of all time, and it is amazingly stable as it does not constantly reinvent itself as a delivery mechanism.

Furthermore, he suggests that for decades, time has shown the significant contribution of traditional records management to the efficiency and effectiveness of an organisation, whereas, knowledge management, certainly in an automated environment, is yet to prove its potential. Malhotra (2004) admits knowledge management systems often unravel and become themselves constraints in adapting and evolving such systems in business environments characterised by a high degree of uncertainty and radical discontinuous change. In essence, it is the ontology of records, which is very different from that of knowledge, which has led to this confusion.

2.8 Records and Accountability of Government

Accountability of government has become of central concern to members of the public. A government that has been elected by the people of the country and is therefore not only responsible for the governed, but it is also exposed to public scrutiny that demands more transparency and accountability. Although records provide evidence of administration and operation, they only surface when triggered by an accountability process that is intimately related to the responsibility of the government. The role of records in providing evidence of accountability has been discussed earlier in *Section 2.2.6*. *Evidence and Accountability.* The relationships between accountability, responsibility and transparency are extremely complex and the terms sometimes used interchangeably (Laffan, 2003; Kaler, 2002; and Mulgan, 2000). There is no recognised discrete boundary between accountability, responsibility and transparency.

2.8.1 Accountability and Responsibility

Day and Klien (1987) assert that accountability is not merely seen as a crucial link in the chain between governors and the governed; effective democracy, it is argued, implies a system that ensures that the former are accountable to the latter. Equally, accountability is increasingly seen as a means of stretching scarce resources; if better value for money is to be achieved in the public sector, it is argued, then an effective system of accountability is needed. Jones (1992) states that accountability is the process of being called 'to account' to some authority for one's action, and to be 'accountable' is to be 'answerable'. However, answerability requires records that present evidence of the accountability process.

Records may not exist if the issue of accountability, which is more fundamental, has not been addressed. Kaler (2002) asserts that accountability has to be understood as providing answers, as reporting or, more obviously, 'giving an account' that he claims as an informative concept. Mulgan (2000) elucidates that in the context of a democratic state, the key accountability relationships is 'to account' to some authority for one's actions, that is between the citizens and the holders of public office and, within the ranks of office holders, between elected politicians and bureaucrats[50].

[50] Mulgan also states that core accountability has thus covered issues such as voters can make elected representatives answer for their policies and accept electoral retribution, how legislators

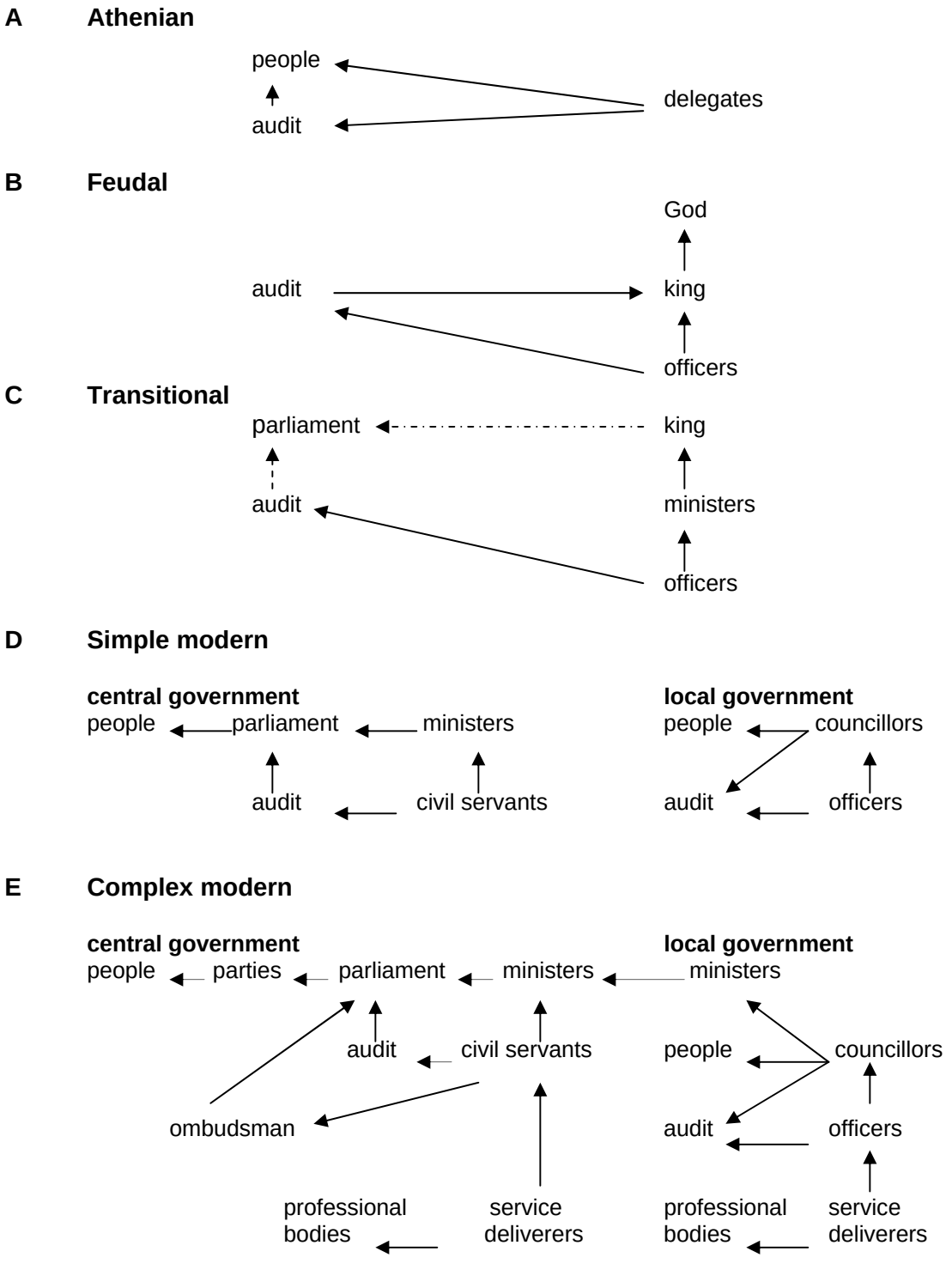

Figure 2.8.1: Models of accountability (© Day and Klien, 1987).

---

can scrutinise the actions of public servants and make them answerable for their mistakes, and how members of the public can seek redress from government agencies and officials.

Members of the public have the rights to know about the balance between accountability and efficiency, and about distinctions between political and managerial accountability. As society became more complex, there is an increasing demand for transparency and accountability. Figure 2.8.1 attempts to differentiate various models of accountability ranging from the simple Athenian model to modern complex government systems. Apparently, today's modern complex government has greater demands for accountability as the governmental machine through ministries and local government is constantly exposed to public scrutiny. Thurston and Cain (1998) assert that if governments are to be held to account and if the public are to have legally enforceable rights of access to government information, then that information must be accurately and securely preserved to ensure that there is evidence of what has been done.

Without reliable, authentic documentary evidence, government cannot demonstrate to society that it has used state resources responsibly and that it has fulfilled its mandates. Accountability mechanisms such as audit and scrutiny by ombudsmen provide essential checks and balances[51]. Both audit and ombudsman must be conducted by people with proven integrity and not subject to political influence to avoid bias and to give the public confidence in the outcomes. Power (1997) states that common sense suggests that it is often useful for operations to be checked by different people and audit practitioners are not trying to be deceptive when they seek the benefits of the assurance that auditing provides, even if they cannot be precise about these benefits.

Mulgan (2000) asserts that the term 'accountability' has been extended, and now commonly refers to the sense of individual responsibility and concern for the public interest expected from public servants ('professional' and 'personal' accountability). Secondly, accountability as 'control' is a feature of the various institutional checks and balances by which democracies seek to control the actions of governments even when there is no interaction or exchange between governments and the institutions that control

[51] OECD (2000) advocates that accountability mechanism should encourage ethical behaviour by making unethical activities hard to commit and easy to detect. Accountability mechanisms set guidelines for government activities, for checking that results have been achieved, and for checking that due process has been observed. They include internal administrative procedures (requirements that activities or requests be recorded in writing), comprehensive processes such as audits and evaluations of an agency' s performance, or new forms of procedures such as whistle-blowing, which can encourage public servants to expose wrongdoings committed by others or to say no when asked to do something inappropriate.

them. Thirdly, accountability as 'responsiveness' is the extent to which governments pursue the wishes or needs of their citizens regardless of whether they are persuaded to do so through processes of authoritative exchange and control. Fourthly, accountability as 'dialogue', that refers to public discussion between citizens on which democracies depend, even then there is no suggestion of any authority or subordination between the parties involved in the accountability relationship. In other words, today's governments are exposed to public scrutiny from various quarters, and governments must be concerned with their administrative and record keeping to ensure that they are prepared when their actions are challenged.

Accountability enables the identification of aspects of responsibility (Marshall and Moodie, 1959), but accountability was certainly not expected to cover the whole range of activities and processes covered by responsibility. It is the question of how far public servants should rely on their professionalism and sense of personal morality and how far they should simply be following instructions from their political masters (Friedrich 1940; Finer 1941). The Heiner Affair in Australia is a classic example of how political masters undermined the archives and records management profession. The affair is further discussed in *Section 3.2.1 The Crisis in the Australian Government in 1980s and 1990s*.

Responsibility is nullified when nobody knows who is responsible; nor can it be divided without being weakened (Mill, 1962). Responsibility can be delegated but accountability remains with the board of directors. Accountability can be divided into political accountability and managerial accountability. Day and Klien (1987) assert that political accountability is about those with delegated authority being answerable for their actions to the people, whether directly in simple societies or indirectly in complex societies. In contrast, managerial accountability is about making those with delegated authority answerable for carrying out agreed tasks according to good criteria of performance. They further assert that managerial accountability has a number of dimensions, fiscal, process and programme accountability, or even between regularity, efficiency, and effectiveness audit.

> *Fiscal/regularity accountability is about making sure that money has been spent as agreed, according to the appropriate rules; legal accountability can be seen as a counterpart to this, in so far as it is*

> *concerned to make sure that the procedures and rules of decision-making have been observed.*
> *Process/efficiency accountability is about making sure that a given course of action has been carried out, and that the value for money has been achieved on the use of resources.*
> *Programme/effectiveness accountability is about making sure that a given course of action or investment of resources has achieved its intended result*[52]*. (Day and Klien, 1987:27).*

In essence, the notions of these dimensions can also be conceptualised as being concerned with inputs, outputs and outcomes. Day and Klien (1987) advocate a simple hierarchical model which allocates political accountability as the highest accountability that sets policy objectives and generates the criteria used in the neutral technical process of managerial accountability, running from the relatively simple fiscal/regularity accountability to the more complex programme effectiveness accountability, from inputs to outcomes. However, this conclusion is based on three assumptions.
First, the institutional and organisational links between political accountability and managerial exist and are effective. Second, the political processes generate precise, clear-cut objectives and criteria necessary if managerial accountability is to be a neutral exercise in the application of value-free techniques. Third, the organisation structure is such that the managers accountable to the politicians can answer for the actions and performance of the service deliverers. However, in the real world, both Day and Klien (1987) admit, it is difficult to achieve such an ideal situation, mainly because political processes do not necessarily generate the kind of clear-cut objectives and criteria required if audit is to be a neutral, value-free exercise[53].

[52] Fiscal/regularity is about checking that the appropriate inputs, whether of resources or administration, have gone into the policy or service-delivery mechanism. Process/efficiency accountability is about checking the appropriate outputs have been produced, and that the ratio between inputs and outputs ('efficiency') is the most favourable possible. But programme/effectiveness accountability is about the ultimate question of whether the intended outcomes have been produced, whether the desired impact have been made (Day and Klien, 1987, p.27).
[53] Other circumstances that discourage the sustainability of the model are the 'overload' of demands for the creation of new links between the political and managerial accountability, and; compounding the arguments both for better links and for more complex system of accountability.

2.8.2 Trust and Transparency

Transparency requires reliable, relevant and timely information about the activities of government to be available to the public (Kondo, 2002). Transparency is closely associated with ideas of accountability. However, transparency alone does not empower, and, paradoxically, may even serve to pacify and neutralise other possible forms of accountability such as those based on answerability. At the extreme, audits, which have become tightly interwoven into regulatory programmes, can do more to promote obscurity than transparency (White and Hollingworth, 1999). In the complex modern model of accountability advocated by Day and Klien (1987), it is apparent that audit and ombudsmen have a critical role in achieving transparency, as White and Hollingworth (1999) advocate transparency can be achieved by the transparency of the audit process and the transparency of audit findings. The essence of transparency is far more important than the audit process itself, particularly in today's circumstances where members of the public are so concerned with government's actions and decisions. Transparency sheds light on practices, which enhances ethical and effective operations and facilitates oversight by the public and others[54] (GAO, 2005). Transparency is seen both as an instrument for ensuring accountability and combating corruption, while in some cases its main purpose is to promote democratic participation by informing and involving citizens.

The media plays a key role in generating demand for more transparency and accountability by exercising its role of scrutiny (OECD, 2000). The establishment of FOI legislation means citizens are more likely to have greater opportunities to challenge decisions on grounds of equity and fairness. In this context, scandals or wrongdoings that came to light, can be seen as a positive sign that such accountability controls are working. It is essential to remember that making more information available to the public does not mean that an organisation is more transparent. Furthermore, the sustainability of an organisation is underpinned by cost-effective operation and competitiveness and not by a higher level of transparency. The types of information to be made available to

[54] The United States Government Accountability Office was trying to redeem public trust over tax-exempt sector including charities and non-government organisations, which their governance is less transparent. Strong governance practices can help ensure that tax-exempt entities operate effectively and with integrity, public availability of key information about the entities i.e., transparency, can both enhance incentives for ethical and effective operations and support public oversight of tax-exempt entities, while helping to achieve and maintain public trust.

the public can be determined by risk management as it is crucial to balance the risk of keeping and not keeping information; the risk of disclosing and not disclosing information. The judgement must be made based on risk analysis that can only succeed with the availability of adequate and reliable records.

The demand for transparency is mainly the result of lack of trust in government, however being transparent alone does not guarantee a higher level of trust, because transparency also can encourage people to be less honest, increase deception and by so doing reduce trust, particularly those, who know that everything they say or write is to be made public, may massage the truth (O'Neill, 2002). She further argues that transparency certainly destroys secrecy but it may not limit the deception and deliberate misinformation that undermine relations of trust. In some cases, transparency may not completely destroy secrecy but it could be enough to decrease the level of trust. To restore trust, deception and lies must be reduced. Transparency and openness may not be the unconditional goods that they are fashionably supposed to be. By the same token, secrecy and lack of transparency may not be the enemies of trust. Like accountability mechanisms, trust, has to be supplemented by mechanisms that contain the risk of misplaced trust. Law and social institutions are viewed as mechanisms to co-ordinate expectations, which make the risk of loss of trust more bearable[55]. If a government institution has had a breach of trust case, it is then the role of the law and social institutions to judge whether or not they are guilty and the types of sanction to impose.

Lane (1998) proposes that trust is an ethical issue and a social phenomenon that has to be studied at an interpersonal, inter-organisational and systematic level, rather than as an aspect of individual personality. Lane's suggestion is less helpful as trust, also, has to be seen as individual personality, as Fukuyama (1995) argues trust has positive effects on performance, and the absence of trust leads to economic backwardness or underdevelopment, and he further proposes that a nation's ability to compete is conditioned by the level of trust inherent in a society. The strength of an organisation relies on trust in employees to execute their jobs responsibly. Policies, regulations and procedures would not lead to the success of an organisation in the absence of trust. It is a requirement for every new employee to agree to terms and conditions of employment,

[55] Luhmann, N. (1974: 24-5) cited in Lane, C. (1998:13).

which is an institutional mechanism to place trust in employees. According to Lane (1998) personal trust share three common elements, namely:

> *First, theories assume a degree of interdependence between trustor and trustee. Expectations about another's trustworthiness only became relevant when the completion of one's own consequential activities depend on the prior action or co-operation of other person (Luhman, 1979; Dasgupta, 1988). Individuals would have no need to trust apart from social relationships (Lewis and Weigert, 1985: 969).*
> *Second is the assumption that trust provides a way to cope with risk or uncertainty in exchange relationships. In economic theory, risk arises because trusting behaviour exposes the agent to the presumed opportunistic behaviour of her business partner. … uncertainty and risk are to be inherent in social relationships, due to problems of time and information. This requires a risky pro-commitment on the other part of one actor (Simmel 1978; Luhmann 1979).*
> *The third common assumption in the writing on trust is a belief or an expectation that the vulnerability resulting from the acceptance of risk will not be taken advantage of by the other party in the relationship. (Lane, 1998:3).*

Risk is unavoidable. And trust is always in a circle together with risk, uncertainty, transparency and accountability. Brenkert (1998) asserts that trust is an attitude or disposition to behave and respond in certain ways, namely to accept certain risks of harm or injury from another agent on the basis of a belief (for which there is some degree of uncertainty) that the other does not intend to do harm to one (or those one cares about), even though he or she could. Baier (1995) states that trust is about letting other persons (natural or artificial, such as firms, nations, etc.) take care of something the truster cares about, where such "caring for" involved some exercise of discretionary powers. In the context of the public sector, it is breach of trust that triggers the accountability process. Thus, for a government to sustain its political and coercive power, retaining the trust of the public is a pre-requisite. There have been several cases that eroded trust of the public, notably the British government's decision to go into war in Iraq and the death of

the weapons expert Dr. David Kelly[56]. O'Neill (2002) notes that the ideals of transparency and openness are now so little questioned that those who 'leak' or disseminate confidential information (other than personal data) often expect applause rather than condemnation, and assume that they act in the public interest rather than betray it. She further argues that openness and transparency has done little to build or restore public trust, instead, trust seemingly has receded as transparency has advanced.

From another perspective, Lane (1998) quotes Granovetter (1985), Sako (1992) and, Barney and Hansen (1994) as suggesting that high level of trust removes the need for any contractual and monitoring devices, because personal obligation and/or value-consensus are seen to guard against opportunism. However, this has hardly been the case as the social order becomes more complex it tends to lose this taken-for-granted familiarity, thus the need for co-ordination and for 'determining future' and – hence the need for trust – becomes more urgent[57]. The development of policies, procedures and controls should enhance trust. However, O'Neill (2002b) argues that legislation, regulations and controls are more than fine rhetoric as they require detailed conformity to procedures and protocols, detailed record keeping and provision of information in specified formats and success in reaching targets.

Indeed, record keeping is the core of every business, regardless of types and size of the business. Hence, having a systematic and efficient record-keeping system, not only ensures efficient administration and decision-making, but also stimulates transparency, which in turns increases trust in stakeholders and the public. Kondo (2002) asserts that trust, particularly in the public sector, is more likely to be strong when there is openness and transparency in decision making, and decisions are made based on evidence. Assessing information from various aspects will help institutions reach a fair judgment that can satisfy most parties, if not all. In addition, consideration of public values is also essential to retain trust.

Whenever mistakes occur, quick acknowledgement and recovery actions are helpful in regaining public confidence and trust. Meijer (2003), based on empirical research on record keeping in public organisations in the Netherlands, asserts creating institutional

[56] Further discussion on the government move into war and the death of Dr. David Kelly is available in *Section 3.2.3 The Hutton Inquiry and the Butler Report*.
[57] Luhmann, N. (1979: 20) cited in Lane, C. (1998:13).

safeguards, such as the re-introduction of an oath for a civil servant is good for increasing the sense of responsibility and accountability in their jobs and the public.

The implementation of FOI is an effort by governments to increase transparency and also to retain or to regain trust of the public. An example of the impact of FOI in increasing the transparency of government in the UK, is the case of Malcolm Hanney, who was awarded almost £18,000 in compensation, when Patricia Hewitt, the former trade and industry secretary, was found guilty of overlooking him, a strong male candidate for a job in favour of a weaker female applicant. Mr. Hanney used FOI to gain access to the interviewer's notes, which concluded that the panel 'agreed to appoint Malcolm Hanney'; but the ultimate decision was left to Patricia Hewitt, who then appointed the third ranked women to the position[58].

Since FOI implementation in the UK is in its infancy, most public organisations are still identifying the type of records that require more attention to respond to public queries. Government officials may act differently if they are able to perceive the consequences and risk of their actions and decisions. It is unlikely Patricia Hewitt would have made that decision if she knew that FOI enabled the interviewee to access the interview records and notes of panel members. FOI may force officials to act responsibly to avoid risk of any controversial decisions or actions made, but it also may tempt them into deception.

FOI legislation does not permit access to all types of information, as there are legal restrictions or exceptions through the European Data Protection legislation, where information cannot be made available to the public. OECD (2000) states that most countries legally guarantee the privacy of certain personal data, either through separate legislation or through sections within overall government access legislation. In addition to restrictions to protect personal data, numerous other exceptions are also common, such as keeping government documents closed for reasons of national security or other

[58] Patricia Hewitt is also known as 'female champion' for her relentless efforts against sex discrimination in the UK. However, in this case she did not act responsibly as there was a clear recommendation by the panel of interviewers that Malcolm Hanney, a respected international banker, as the 'strongest candidate' and the 'clear favourite' should be appointed to the position advertised. Instead, Patricia Hewitt, who had the ultimate decision appointed the third ranked women for the position. Dissatisfied, Malcolm Hanney used the Freedom of Information Act, and was given access to the interviewers' notes that reveal the panel agreed to appoint him to the position. Further information available at http://news.independent.co.uk/uk/politics/article318857.ece (12 October 2005).

national interests, to protect trade, industrial or commercial secrets, and internal working documents. Under this legislation, governments are under constant public and media scrutiny that demand higher transparency over time. Extensive public disclosure in the name of transparency is an ambient phenomenon. Disclosure can have a palliative effect on the public, and can serve to convince them that something is or will be done by someone, and can ultimately deter inquiry rather than encourage it. Disclosure can serve to amplify trust in the audit process rather than stimulate critical analysis of its results, since it often tends to shift trust towards new audit institutions, such as accreditation arrangements.

2.8.3 Audit and Internal Control

Audits are linked to ideals of organisational transparency and accountability although they do not contribute automatically to organisational transparency. Power (1994), in his comprehensive discussion on audit, argues that audits are simply answers to problems of accountability. Audit encourages the displacement of a system based on autonomy and trust by one based on visibility and coercive accountability. He argues that audit is a risk reduction practice which inhibits the deviant actions of agents, and audits are needed when accountability can no longer be sustained by informal relations of trust alone, but must be formalised, made visible and subject to independent validation. White and Hollingsworth (1999) also have the thought that audits are usually justified as enhancing the transparency of individual and corporate actions to those parties who have an interest in the nature and effects of those actions. In other words, they are thought to shift power; from professionals to the public, from experts to stakeholders.

Like risk management, audit has the same origin in financial management. Audit has expanded from specific financial audits to almost every operational aspect of an organisation. Auditing is not merely a collection of technical tasks but also a programmatic idea circulating in organisational environments, an idea which promises a certain style of control and organisational transparency (Power, 1997). The wider dimension of the audit, in the public sector in particular, requires the audit process to consider the way in which the audited body secures economy, efficiency and effectiveness in the use of all of its resources. The terms economy, efficiency and effectiveness are frequently referred to under the generic term ‘value for money’ (PricewaterhouseCoopers, 2005). This ambiguity of audits has helped it serve diverse

needs, and its opacity has helped its expanding role in government, serving the needs (and status) of the professionals involved, and comforting politicians and a wider public that things are under control. However, Power (1997) worries that paradoxically, the audit society threatens to become an increasingly closed society, albeit one with the declared programmatic foundation of openness and accountability. The result of audit process is not only the outcome, but also that the process of the audit itself has to be made transparent. Shore and Wright (2000) quote Power (1994) as arguing that audit is introduced largely when trust has broken down, and yet the spread of audit actually creates the very distrust it is meant to address', culminating in 'a regress of mistrust' in which the performances of auditors and inspectors are themselves subjected to audit'.

2.8.3.1 Internal Audit and External Audit

Compliance, particularly with international regulation, is unavoidable if organisations want to trade across national boundaries. Having an international certification, such as ISO for example, reflects the fact that the organisation has a transparent and approved method of operation. To obtain certification, all processes within an organisation have to be documented and verified as evidence of operations. The process of documenting evidence is vital but difficult, particularly in the absence of effective and systematic record keeping systems. Preparing an organisation for audit by external auditors can be outsourced to a consultant, but it would be costly and risky as it would disclose confidential information to the third parties.

Furthermore, audit is not a one-off process, hence a more economical and less risky option is to appoint an internal audit committee. An internal audit committee is part of internal control systems that are essential in preparing an organisation over time, for external compliance. Power (1997) suggests for any control system there must be a loop which formally corresponds to a certain learning potential[59]. He asserts that internal control systems are a form of structured self-observation, as internal audit observes the self-observation process and, also, is a form of second order control. He further asserts that internal audit can also perform tests on the system, just as external financial auditors do.

[59] Audit is a dynamic and cyclical process. Policies and procedures are designed for implementing and measuring performance in relation to improve the institution over time, as results are fed back into the system in form of reports, comparisons, etc. and remedial, corrective action is taken where necessary (Power, 1997:83).

In the UK, the role of internal audit has developed considerably over the last decade, since the publication of the Cadbury Report (Committee on the Financial Aspects of Corporate Governance, 1992) on corporate governance and the guidance for directors on internal control or also known as Turnbull Report (Institute of Chartered Accountants in England and Wales, 1999). The National Audit Office, UK (NAO) (n.d) encourages government departments to have internal audit committees in conjunction with audit by external auditors, either from the NAO or other professional bodies[60]. The NAO is not the only institution that oversees audit requirements, as there are three other UK national audit agencies, namely the Audit Commission, Audit Scotland, and the Northern Ireland Audit Office. Although there is no one defined public audit model in the UK, the approach to external audit by the four agencies shares a common approach (Chartered Institute of Public Finance and Accountancy, 2000). One of the critical factors for the success of audit is co-operation between internal audit committees and external auditors, making for a better informed dialogue on risks facing the organisation, leading in turn to the more effective focussing of audit effort and consequently to more useful advice to management.

Effective co-operation can only be achieved when both parties are committed to developing co-ordinated and effective audit services, though both parties have their respective roles, responsibilities and accountabilities (NAO, n.d). The effectiveness of the co-operation is highly dependent on regular and open communication, either formal or less formal, as agreed by the two parties. It is essential to document agreed procedures to facilitate such co-operation as it can be used as guidance for both parties. Dietel[61] (2000) asserts that a corporate records audit should provide an evaluation of where the company stands with its records policies, procedures, and practices. The audit should also point to what needs improvement and what plans are needed to

[60] The main reason of having an internal audit committee is to increase value for money in public services. The internal audit committee, in many ways, already co-operate with external auditors, however, by documenting co-operation, both parties can help ensure the highest standard of regularity and propriety for the use of public funds and resources and in promoting efficient, effective and economic public administration. Good co-operation maximises the benefits, which can be gained from working together in areas where there is an overlap in the work to be done (NAO, N.d).

[61] Ed Dietel, J.D., is an attorney, independent consultant, and serves as a senior consultant for Records Engineering, LLC, in Reston, Virginia. He is the author of *Designing an Effective Records Retention Compliance Program*, which was awarded the Book of the Year Award by the Preventive Law Institute.

achieve those improvements. Audit and risk management complement each other in subsequently achieving organisational goals. Further discussions on these areas are available in *Section 2.7 Risk Management and Managing Records*, and *Section 2.8.3 Audit and Internal Control*.

As audit is no longer confined to financial management, organisations have to be certain of their compliance with law and regulations. Audits embrace both technical and organisational aspects. Technical aspects relate to system functions, while organisational aspects relate to the formal design and operation of the organisation. Undoubtedly, financial audit is the most important audit process as the sustainability of an organisation relies extensively on financial stability. Global demands for accountability and transparency leave no option but for organisations to be constantly aware of the risk of compliance or non-compliance with regulations. Internal audit committees have to be certain about the requirements of formal audit by external auditors and regulators.

Hence, it is essential to have in place internal processes of checks and balances, and corrective actions to be taken prior to the formal audit. The collapse of two corporate giants, Enron and WorldCom, is the result of massive fraud involving external auditors, Arthur Andersen, and led to the implementation of SOX legislation in the US, requiring audit committees to be more responsive and effective in scrutinising financial statements prepared by the external auditors. Under the terms of the legislation internal auditors, external auditors and the audit committee are agents of accountability and transparency that are responsible to ensure compliance and ethics in conducting business. Further discussion is available in *Section 3.2.2 The Collapse of Enron*.

2.8.3.2 Audit Trail

Allinson[62] (2001) explains the notion of audit has changed from traditional audit, that was used in accounting for the checking of financial reliability of a business, to a process where a record is maintained of a particular series of events in order to provide evidence in the case of a dispute, to ensure compliance with certain rules and regulations, to check on the effectiveness of control systems, and to provide evidence in the case of criminal activity. These records are commonly known as audit trails or audit logs. Audit was not developed mainly to track or detect the culprits of mismanagement, instead it was meant for business improvement by discovering evidence through audit trails. As discussed in *Section 2.7.2 Elements of Risk Management*, audits enable the discovery of evidence by scrutinising relevant records.

Audit trails facilitate the process of determining accountability, effectiveness and integrity of an employee, a department, or even an organisation by automatic capturing and storing all the actions that are taken upon an electronic record, the user initiating and carrying out the action and the date and time of events (Hänger, 2003). All types of information systems including financial management systems need to provide audit trail feature for both audit purpose and security reasons. Indeed, decisions to prioritise the comprehensiveness of any systems must be based on the input from the risk management team. Achieving organisational goals and containing costs are their utmost important concern. Financial records, as compared to other types of records, are constantly under surveillance because this type of record presents evidence of fiscal value and have immediate impacts on the financial stability of an organisation. However, financial information is just a tangible evidence of performance and not an end in itself. The accuracy of financial records is crucial and should be constantly monitored to detect if there is any corruption or mishandled business transaction that may lead to loss or worse bankruptcy of an organisation. The rise and fall of an organisation is highly dependent on its financial status.

[62] Caroline Allinson is Manager Information Security for the Queensland Police Service (QPS) in Brisbane, Australia. She is involved in management of information security policy development, information systems access control, assisting with investigations which include evidence in court, security auditing and security advice and consultancy.

Audit trails have proved their worth in discovering evidence during investigation of many crimes, wrong doings and mismanagement. Security measures, access and privilege controls, logging and audit controls, accountability controls, and monitoring and reporting controls in accordance with the level of sensitivity of the electronically or digitally stored, transmitted and processed information, need to be built into all aspects of the system and environment. In addition, security against loss and/or damage of audit trail information to ensure the level of protection will satisfy legal requirements is a major issue. Although, it has not been addressed adequately (Allinson, 2001), it is generally assumed that the audit trail is secure, reliable and acceptable from a legal perspective[63]. Schultz (2004) states for years, information security professionals have struggled to place their information security practices into positions of prominence and influence that have strategic value to their organisation. Financial information, for example, resides on computing systems, storage devices and networks, all of which require suitable authentication and access control methods if there is to be confidence that the data are reliable. File and directory integrity and audit ability to access are also important considerations in data reliability, as is user authorization, specifically connecting each user's access to system directories and files that hold financial data to explicit authorization by management.

2.8.4 Authenticity and Integrity of Records

Quality of records is underpinned by authenticity and integrity. Records have to retain their original elements as they were initially created and used to be reliable evidence. Records either in physical or digital format establish their authenticity by possessing all metadata required throughout its life cycle. Bearman and Trant (1998) argue that authenticity becomes an issue of concern as digital technology makes purposeful fakery easier and more tempting, and more dangerously, easier for faked products to enter authoritative information streams. The InterPARES Authenticity Task Force (2001)

[63] Apart from providing evidence of compliance to a particular standard, audit trails are closely related to the security of information systems, by means of ensuring the integrity of the system itself by checking that unauthorised changes to software have not occurred, file access controls are properly set and that the communications network has not changed. They also help to ensure that the organisation is complying with regulatory controls and assist in the detection of suspicious patterns of access such as log-on attempts outside normal hours of business (Pabrai, U.O.A., Dec 2003. Auditing: Discovering Enterprise Security Gaps, *Certification Magazine*. pp 50-51. Available at: http://www.certmag.com/articles/templates/cmag_department.asp?articleid=512&zoneid=63. (21 June, 2007).

research findings indicate that in order to assess the authenticity of an electronic record, the preserver must be able to establish its identity and demonstrate its integrity. The integrity of a record refers to its wholeness and soundness: a record has integrity when it is complete and uncorrupted in all of its essential respects. This does not mean that the record must be precisely the same as it was when first created for its integrity to exist and be demonstrated.

The electronic record is essentially complete and uncorrupted if the message that it is meant to communicate achieves its purpose unaltered. This implies that its physical integrity, such as the proper number of bit strings, may not be compromised, provided that the articulation of the content and any required elements of form remain the same. Cullen (2000) describes an authentic object as one whose integrity is intact – one that is and can be proven or accepted to be what its owners say it is. It matters little whether the object is handwritten, printed or in digital form. Control mechanisms should be applied throughout the record life cycle in order to allow authorised users to create and manipulate records according to standards applied. Thus, authenticity of the records will be more reliable and trusted. Currall *et al.* (2001) argue that a digital record document creation system must be set up in such a way that the procedures for document creation and management are such that documents within it remain credible as records. This suggestion is similar to the findings of the InterPARES research project which concluded that authenticity of electronic records is assured mainly through procedural means treated as part of the management of the electronic system as a whole (InterPARES, 2001).

Even if sufficient procedural requirements are being implemented, another issue that raises concern amongst information professionals is the durability and authenticity of digital objects especially, whenever they are transferred across space and over time. The degradation of the media on which they are stored, loss of functionality of access devices, loss of manipulation capabilities, loss of presentation capabilities, or weak links in the documentation chain, are all factors that contribute to making resources inaccessible (Ross and Gow, 1999, cited in Ross, 2000). Creating an electronic file, and even marking it in such a way that will ensure its authenticity will mean little if the file itself cannot be read at any point in the future. Duff (1996) has noted that as records migrate from a stable paper reality to an intangible electronic existence, their physical attributes,

vital in establishing the authenticity and reliability of the evidence they contain, are threatened. The bits may be the same across space and time, but because of differences in the hardware and software used by recipients, the experience of viewing them may vary substantially. This raises questions about how to define and measure authenticity and integrity. InterPARES (2001) states that records created and maintained in electronic form are continually at significant risk of inadvertent or intentional alteration, and such alteration may not be readily perceptible.

The authenticity of digital objects can be attested by examining the provenance of the object using a forensic and diplomatic examination to ensure that its characteristics and content are consistent with the claims made about it and the record of its provenance; relying on signatures and seals that are attached to the object; and for mass-produced and distributed (published) objects by comparing the object in hand with other versions (copies) of the object that may be available (Lynch, 2000). He, however, argues that finding and verifying a watermark in a digital object gives only weak evidence of its integrity, because a system does not provide sufficient safeguards against the creation of fake watermarks.

There are other methods for determining the authenticity of electronic records. Levy (2000) suggests two possible solutions. First by maintaining audit trails, which indicate a series of transformations that have brought a particular document to the desktop. The second possibility is specifying properties underlying a document. The properties are a string of fixed metadata fields that underpin the existence of the document. Establishing authenticity in the digital environment is difficult and it requires more research and effort to specify appropriate methods. Implementing procedural restrictions and producing systems with embedded control mechanisms are useful in assuring electronic records which are authentic at the creation stage. However, it remains difficult and complex for information professionals to retain authenticity of electronic records across space and time.

2.8.4.1 Record Keeping Metadata

The elements of metadata were used long before the term ‘metadata’ itself was created, perhaps, since human being started recording information and contextual details. Today, ubiquitous application of ICT has resulted in the creation of enormous number of digital

objects. Managing most electronic information objects can only succeed with the availability of adequate metadata that function to aid the identification, description and location of networked electronic resources. Without metadata, electronic documents in particular, lose their original context and become less useful, as the metadata functions like a map and a compass to make it easier for everyone searching for information to find it (Hansen, 2003). Record keeping metadata, on the other hand, is not the same as resource discovery metadata that enables Web-based information to be retrieved (Cumming, 2001). There are several definitions of record keeping metadata advocated by various groups, based largely on their specific local needs. These include the Records/Documents/Information Management (RDMIS) Working Group on Work Processes and Practices (WPPWG) for the government of Canada (Government of Canada, 2001) which defines record keeping metadata as the type of information required to describe the identity, authenticity, content, context, structure and management requirements for records created in the context of a business activity.

Another working group on record keeping metadata that consists of archivists, metadata experts and computer scientists defines record keeping metadata as structured or semi-structured information that enables the creation, management, and use of records through time and within and across domains (Working Meeting on Recordkeeping Metadata, 2000)[64]. However, the group admit that record keeping metadata may or may not follow a structured schema for organising metadata. The group also agrees that it was unlikely a single fixed metadata schema could be developed or would be accepted to serve all record keeping environments. Establishing a fixed record keeping metadata schema across an organisation would only generate more problems rather than facilitating the management of organisational records.

In most situations a semi-structured schema is more suitable as different departments may require different metadata fields adequately to represent their business operations. It is, therefore, more appropriate to have a core set of metadata elements that meets the

[64] Working Meeting on Recordkeeping Metadata, Castle Bergh, the Netherlands, June 7, 2000. Participants at the meeting were Wendy Duff, Hans Hofman, Margaret Hedstrom, Adrian Cunningham, Barbara Reed, Sue McKemmish, Peter Horsman, Heather MacNeil, Peter Hirtle, Anne Gilliland-Swetland, David Wallace, Gabriel David, Meg Sweet, Ingmar Koch, Nigel Ward, Carl Logoze and Christina Robero. This meeting aimed to propose research, standard initiatives, and other projects that might link the recordkeeping community and its interests more closely with other metadata initiatives.

minimum requirements for describing and sharing information, while at the same time facilitating interoperability between departments. In addition, departments with specialised needs should be allowed to add new elements and/or sub-elements to the basic metadata in order to satisfy their particular business requirements (Government of Canada, 2001; Hänger, 2003).

Record keeping metadata has two important functions, to support the transfer of records across domains and over time (Working Meeting on Recordkeeping Metadata, 2000). As records provide evidence of business transactions, and must be accurate over time, the comprehensiveness of record keeping metadata captured should not only identify the who, what, where and why of business, but also identify the management processes required to maintain records. Record keeping metadata contextualises and facilitates the management of records (Cumming, 2001), as well as facilitating risk management by ensuring the accuracy of information (Duff, Hofman and Troemel, 2003). Cumming (2005) further advocates that effective metadata implementation also facilitates the ability to increase access and use of organisational information securely as a valuable commodity in today's business environment.

The benefits of effective record keeping metadata can only be achieved with the existence of policies or standards that would attract, if not oblige, organisations to adopt good record keeping practices (Hofman, 2005; McDonald, 2005; Cumming, 2005; Duff, 2003; Shepherd and Yeo, 2003). For the records management community, there was light at the end of the tunnel when the ISO 15489:2001 was introduced as a part of requirements for the ISO standard. In addition, a more recent technical specification ISO 23081-1:2006[65] was published in January 2006, which superceded ISO 23081:2004, would enhance the management of record keeping metadata. It is a high level standard which explains what records management metadata is, why it is necessary, what roles and responsibilities can be identified in its implementation, what types of metadata exist and how to manage them (Hofman, 2005).

Among others, the ISO Technical Specification states that the purpose and benefits of metadata are to support business and records management processes by:

[65] *ISO 23081-1:2006 : Information and documentation – Records management processes – metadata for records – Part 1: Principles.*

i. Protecting records as evidence and ensuring their accessibility, and usability through time
ii. Facilitating the ability to understand records
iii. Supporting and ensuring the evidential value of records
iv. Helping to ensure the authenticity, reliability, and integration of records
v. Supporting and managing access, privacy and rights
vi. Supporting efficient retrieval
vii. Supporting interoperability strategies by enabling authoritative capture of records created in diverse technical and business environments and their sustainability for as long as required
viii. Providing logical links between records and the context of their creation, and maintaining them in a structured, reliable and meaningful way
ix. Supporting the identification of the technical environment in which digital records were created and the management of the technological environment in which they are maintained in order that authentic records can be reproduced as long as they are needed, and
x. Supporting efficient and successful migration of records from one environment or computer platform to another or any other preservation strategy (cited in Duff, 2003).

Many of these benefits have been advocated by various electronic records management initiatives including InterPARES[66], the Pittsburgh Project, the Preservation of the Integrity of Electronic Records which is also known as the University of British Columbia Project[67], the US Department of Defence's DOD5015.2-STD[68], the New South Wales Recordkeeping Metadata Standard[69], the UK's Functional Requirements for Electronic Records Management System[70] and the European Model Requirements for the Management of Electronic Records or MoReq [71]. Although these projects and other smaller scale projects were developed in effort to satisfy their local business requirements, their findings have contributed to the establishment of the international standards for records management such as ISO 15489-1:2001 – Records Management

[66] http://www.interpares.org
[67] http://www.interpares.org/UBCProject/index.htm
[68] http://jitc.fhu.disa.mil/recmgt/p50152stdapr07.pdf
[69] http://www.records.nsw.gov.au/publicsector/erk/metadata/metadata-std/NRKMStitle.htm
[70] http://www.nationalarchives.gov.uk/recordsmanagement
[71] http://www.cornwell.co.uk/moreq

Standard; ISO 23081-1:2006 – Information and documentation – Records management processes – Metadata for records, and ISO 14721:2002 – The Open Archival Information System (OAIS) Reference Model (An, 2005).

The purpose of the ISO document is to provide guidance in understanding, implementing and using record keeping metadata and establishing metadata management frameworks, not to specify a mandatory set of record keeping metadata (metadata schema[72]) (McKemmish, Reed and Piggott, 2005). Nevertheless, it is undoubtedly due to its status as an internationally respected organisation, ISO made a tremendous impact on both public and private organisations in improving their record keeping systems that eventually will increase, not only their business profitability, but also accountability and transparency by ensuring the availability of authentic records.

The reason for better acceptance of standards such as ISO 15489 is, perhaps, according to Murdock (2006a), because such standard presents a credible, independent and natural view of record keeping by identifying a set of principles based on a common vocabulary, which is an effective reference point for records managers and archivists when dealing with sceptical management. In addition, legislations such as SOX Act in the US and the FOI Act in the UK encourage organisations to improve their record keeping practices or else expose themselves to the consequent risk. Having an effective record keeping system which is underpinned by effective management of metadata will enable organisations to comply with these legislations. To this end, metadata should document content, context, and structure at the time of capture, and also should document records management and business processes throughout the life cycle of records, including changes to the structure or context (Duff, 2004).

Record keeping metadata is the life blood of a record, therefore they must be captured adequately though the task is complicated and challenging. The effective management of electronic records is not just a technology issue but also requires an infrastructure of extend laws, regulations and policies, standards and practices, systems and

[72] A metadata schema provides semantic and structural definitions of metadata, including the names of metadata elements, how they are structured, and their meaning. Archival descriptive standards and records system specification can be envisaged as traditional forms of recordkeeping metadata schema (Sue McKemmish, Barbara Reed and Michael Piggott (2005:185)).

technologies, and qualified people, all supported by an effective management framework and leadership capable of continually aligning the infrastructure in support of the business of the organisation (McDonald, 2005). Metadata is a tool and only one component of accountable record keeping and business infrastructures. Therefore, managing records must be business driven by and needs to be managed in a controlled and coherent fashion (Cumming, 2005).

Since metadata is the life of a record, Moss and Tough (2003), from their first hand experience, rightly pointed out that one of the major challenges is to design systems that derive metadata from the directory structure or file plan and attach them automatically to documents at the point of creation, thereby minimising human intervention and opportunities for human error. Indeed, in an electronic environment this should apply throughout the records life cycle, as contextual information of records can easily be changed, either deliberately or accidentally, whenever records have been accessed, transferred or modified.

Electronic records can only be regarded as authoritative and potentially as authentic if they are accompanied by metadata that identifies them and testifies to their appropriate management (Cumming, 2005). In essence, it is contextual information that is more essential than the content and structure of a record, as it facilitates audit that eventually determines accountability. The design of a record keeping system must reflect the organisation's business structure, and this can be demonstrated by the directory or file plan structure. Implementing and organising record keeping metadata requires extra resources in term of time and effort (Currall *et al, 2001*). It is important, therefore, to keep in mind that automating a non-effective directory or file plan structure will not improve the situation, but waste money and resources.

An effective directory or file plan structure must precisely represent every business function and its context so as to facilitate the capture of adequate metadata. Undoubtedly, a better option is if the directory or file plan structure has proved its effectiveness in the analogue order it only requires to be replicated in an electronic environment. This is to say, a comprehensive study is required to avoid over-engineering of existing systems, which simply increases cost whilst delivering a diminishing return for investment. As mentioned earlier in *Section 2.7 Risk Management and Managing*

Records, the strength and effectiveness of a record keeping system mainly depend on the effectiveness of risk management that prioritises and identifies risks across an organisation. Allocating the identified risks into an organisational directory or a file plan structure enables the identification of contextual information, which in turn ensures that the authenticity and integrity of electronic records is under controlled.

2.8.4.2 Preservation of Records

Preservation has a tremendous impact on the longevity of the life span of records as it ensures the availability of records over time. Rothenberg (2000) advocates preservation of any informational entity is ultimately defined in terms of which of its attributes that can and must be preserved to ensure that it will fulfil its future use, whether originally intended, subsequently expected or unanticipated[73]. Preservation strategies and techniques have evolved from preserving physical records to preserving electronic records in line with the expanding usage of ICTs in workplaces. In many organisations, decisions whether or not to preserve records depend on various needs.

A study conducted by ERPANET[74] reveals four core drivers for preservation: core business focus; re-use; legal and regulatory compliance; and experience of information loss. Preservation for cultural and historical value was given the lowest priority (Ross, 2006). Understandably, operating under massive regulatory and compliance regimes, organisations are exposed to risk from many quarters, hence preserving some records to fulfil core business focus, re-use, and compliance is inevitable. Indeed, preservation itself is a risk management activity at every stage (Ross and McHugh, 2005). To this end, having a comprehensive, functional and effective records retention schedule is certainly helpful in the appraisal process, which subsequently enables determination of appropriate preservation strategies.

These should be developed in collaboration with individual business units, risk managers, legal advisors and ICT experts. Indeed, on the top of fulfilling the needs of all individual units or departments within an organisation, digital preservation also is about striking the

[73] Although unanticipated use means it can be any type of usage of a record, but it is supposed to be within the usage of a record during its initial creation and use stages. Literally preservation means maintaining original or existing state, it is therefore extremely difficult, although not impossible, to ensure that records can be used in a way that has never been used in the initial stage.

[74] http://www.erpanet.org

balance between containing operating costs, making profit, complying with regulations and maintaining the organisations competitiveness. Unfortunately, the reality is in most organisations that they are not keen to commit digital preservation. Understandably, this is mainly because high costs are required and the value of digital preservation is only apparent long after the initial investment has had to be made (Ross, 2006).

Traditional preservation strategies, techniques, and paradigms developed in the pre-digital era do not always translate into the digital environment (Harvey, 2003). Physical records with attributes that carry the look and feel are much easier to preserve. Contextual information of physical records can easily be retained as it is tangible, hence the existence can easily be attested. The digital world has transformed traditional preservation concepts from protecting the physical integrity of the object to specifying the creation and maintenance of the object whose intellectual integrity is its primary characteristic (Conway, 1996). Contrary to managing preservation of physical records, strategies and techniques for preserving electronic records must be tailored to meet different software and hardware environments.

Preservation of analogue records may involve four activities, namely:

i. *Maintenance: The daily care of records and archives, particularly in the current and semi-current records environment, when they are housed in offices or records centres; maintenance ensures the general protection of records against environmental hazards or other physical dangers.*
ii. *Examination: The preliminary procedure taken to determine the original materials and structure of an item and to determine the extent of its deterioration, alteration or loss.*
iii. *Conservation: The intrusive protection of archival material, by the minimal physical and chemical treatments necessary to prevent further deterioration, which will not adversely affect the integrity of the original.*
iv. *Restoration: The repair of an item when aesthetics and reproduction of the original appearance is more important than the preservation of the integrity of the item. Restoration is not generally viewed as an archival activity. (IRMT, 1999a:34).*

Preservation efforts should embrace the record life cycle and not be limited to any specific stages due to the need to keep and maintain metadata for accessibility and authentication. Although the concept of preservation remains the same, the practice differs considerably. Preserving electronic records requires both preserving the container and the content of electronic records.

A record is, understandably, a specific entity and is transaction oriented. It is evidence of activity that can only be preserved if one can maintain its content, structure, and context. Structure is the record form, context is the linkage of one record to other records and content is the information, but content without structure and context cannot be information that is reliable (Cox, 2001). Apart from these three types of metadata, the Digitale Bewaring Testbed (2003), is also known as Digital Preservation Testbed[75] , in the Netherlands, which advocates that there are two more elements that must be considered in preserving electronic records, namely appearance and behaviour.

The Testbed project team assert that the appearance refers to the ultimate presentation of a record, that is, the form in which the digital record is displayed onscreen, including characteristics such as the font, font size and the use of underlined, and bold or italic letters. Nevertheless, the underlying element that underpins the authenticity and integrity of electronic records is no other than metadata, particularly preservation metadata. Preservation metadata is the information a repository uses to support the digital preservation process (PREMIS, 2005), which includes evidence of provenance and relationships, as well as technical, administrative and structural metadata (Ross, 2006).

Hence, ensuring the accuracy of metadata is essential as the right metadata is the key to preserving digital objects (Duff, Hofman and Troemel, 2003). Metadata must be derived from an analysis of the organisational business processes, functional requirements and needs (Ross, 2000). The process of identifying relevant metadata, particularly contextual metadata, would be more effective with the existence of a comprehensive directory or file plan structure that allocates the position of individual business units. Some metadata can be automatically generated by systems, and others have to be manually inputted into

[75] http://www.digitaleduurzaamheid.nl/home.cfm

the system (Gilliland-Swetland, 2000). Marciano and Moore[76] (2005) assert that most metadata of preservation actions taken is manually recorded. Moore, from his wide first hand experience, explains:

> *Preservation metadata used to describe the authenticity and integrity are normally not maintained by storage system. Thus, information about the creator of a record, the institution that sponsored the creation of a record, or a check sum that can be used to validate the integrity of a record are not stored as attributes in the storage repository along with the record. The preservation environment includes not only storage repositories for the records, but also storage repositories for the preservation metadata. The technology that is used to support the preservation environment must link metadata stored in database with records stored in archival storage systems, and maintain the link through all future upgrades of the software and hardware technology. (Marciano and Moore, 2005:82).*

Separating preservation metadata from records presents a downside in which a risk that the link between records and metadata may be broken, particularly when records are transferred from one computing environment to another. If this happens, records become unmanageable or unusable (Shepherd and Yeo, 2003). It is undeniable, in this case that managing records is and must be intimately related to risk management. The level of probability to occur, and the impact the risk would enable adoption of suitable strategies by the organisation.

Apart from that, in the perspective of records community, internal procedures, control and monitoring mechanisms are certainly crucial to ensure all preservation actions are conducted accordingly in order to maintain the authenticity and integrity of records by preserving their availability, accessibility and understandability. Marciano and Moore (2005) conclude that a preservation environment is viable if its digital holdings can be extracted and migrated into a new preservation environment without compromising either the authenticity or integrity of the records. This, however, does not mean that metadata of the migrated version has to be exactly the same as the previous version.

[76] Moore is Director of Data and Knowledge at the San Diego Supercomputer Centre, where he co-ordinates research efforts in development of data grids, digital libraries and preservation environments. He has a PhD in plasma physics from the University of California, San Diego (1978).

Duranti (2001a) argues that there are components of the record that can be lost without compromising its substance and the ability to verify its authenticity over time, but others the loss of which would be equivalent to the loss of the record. It is therefore essential to identify and thoroughly preserve the key metadata throughout the record life cycle for authenticity and integrity to remain. An electronic record is successfully preserved if its availability, accessibility and understandability are preserved. Electronic records can be preserved through three techniques namely emulation, migration and eXtensible Mark-up Language[77] (XML) (Digitale Bewaring Testbed, 2003). However, none of emulation, migration nor XML offer a complete preservation solution for all formats of electronic records with different characteristics, ranging from the simple text documents to highly complex databases. In addition, preservation solutions also need to suit either short or long-term organisational needs. In other words, it is essential to adopt a standard that facilitates preservation of electronic records over time, though it would be a challenging task due to the rapid change of technology.

Emulation is used in computer science to denote a range of techniques, all of which involve using some device or program in place of a different one to achieve the same effect as using the original. In the digital preservation context, emulation means keeping the original file formats, but producing a software application or complete system that allows original software to be used to access the information (Public Record Office, 2001). Thibodeau (2002) suggests that emulation is, perhaps, the best method for digital preservation because it retains the original formats of digital objects.

Based on first hand experience, Digitale Bewaring Testbed (2003) asserts that emulation would involve either hardware emulation or a Universal Virtual Computer strategy (UVC)[78]. Hardware emulation is preferable as it enables future computers to 'impersonate' any obsolete computer, virtually recreating the obsolete computer and thereby allowing its original, obsolete software to be run in the future (Digitale Bewaring

[77] XML itself is not a means of digital preservation. It is an open standard that enhances preservation, although it cannot in itself achieve it. For further information, please refer to Harold, E.R. (2003). *XML 1.1 Bible. 3rd ed*. Indianapolis: Wiley Publishing, Inc.

[78] The complexity of emulation was explored and comprehensively discussed by Digitale Bewaring Testbed. A report entitled '*From digital volatility to digital permanence: preserving database'*, which can be found http://www.digitaleduurzaamheid.nl/bibliotheek/docs/volatility-permanence-databases-en.pdf (17 March 2006).

Testbed, 2003). Its major advantage is, according to the Testbed team, that the original file does not have to be migrated or converted, and hence, retains the authenticity and integrity of the file. However, the Testbed team also admit that the downside of emulation is it suffers from a number of disadvantages including the technical complexity and time-consuming nature of the design, testing, use and durable preservation of the emulator.

The Testbed team describe that emulation using the UVC strategy differs to some extent from the original emulation concept. An emulator must still be written, but in this case it is for a non-existent, virtual computer, that is the UVC. The UVC has a simple architecture and a simple set of instructions, thereby ensuring that it will be easy to write an emulator at some point in the future. From their empirical findings, the Testbed team admit that UVC strategy is highly promising for durable preservation of electronic records, though it will be necessary to devote time and effort to the development of data format decoder programs for customary proprietary file formats.

Migration essentially involves moving a file on one type to a new environment before the pathway from the older format to the newer one disappears. However, it is not easy as migrations will be time and labour dependent and will be influenced by processes, systems and best practices (Ross, 2006). Another disadvantage of migration is it normally affects a record's authenticity, by jeopardising the structure, context and content of records, as Walton (2003) states the cumulative effect of multiple migrations over time could damage the authenticity of the document as they were reproduced.

Migration must be carried out with extreme care to ensure that their bit streams are not modified in any way that affects their interpretation, since programs and their data files can be corrupted by the slightest change (Rothenberg, 1999). Records managers together with IT experts, therefore, need to develop strategies for migration, which is normally based on the assumption that software is compliant with widely adopted standards, and provides utilities for upward migration and swapping documents and databases between software systems.

XML is a mark-up language based on text characters used to enrich data with information about structure and meaning. XML can also be used as a file format[79]. XML is suitable for digital preservation as it is not dependent upon a specific platform and can be read using a simple word processor (Digitale Bewaring Testbed, 2003). The Testbed team further advocate that XML is an excellent choice of format for long-term preservation of databases as it can be used to specify the context, content and structure of database[80]. The findings of the Digitale Bewaring Testbed reveal that there is another option of digital preservation strategy which has a better potential to be widely adopted though more research needs to be conducted to testify the feasibility.

Preservation of availability means that records must remain readable. This is to say that records can be processed on a computer system or device other than those on which they were initially created, or stored. Ability to preserve records availability does not guarantee that records are accessible, if the computer system failed to transform the binary digit into forms that are readable by humans. Thus, records manager must take into account strategies that can be implemented to retain records accessibility, such as preserve the technology on which the records depend; operational software; presentation capability; or eliminate dependency of the records on specific technologies. It is imperative for records managers to upgrade their knowledge of IT in order to facilitate collaboration with IT experts through meaningful communication and understandings.

The ability to preserve records availability and accessibility does not mean that understandability is simultaneously preserved. Understandability means that users are able to know the records content and more importantly the context in which the records was initially created and used. Preservation of understandability can be achieved by preserving information about records and preserving information that is not contained in the records. Records have to be preserved over the life cycle in order to ensure contextual information that underpins the understandability is systematically captured. Shepherd and Yeo (2003) describe that full contextual information must be preserved for the life of each record, if contextual information about digital objects depends in part on an electronic folder structure, this too must be preserved when records are migrated. To

[79] For further information, see http://www.w3c.org
[80] Unfortunately, the Testbed team did not mention the impact of XML on the preservation of behaviours, which is another critical element of a database.

this end, a records manager must understand the nature of the business of the organisation[81].

Although generally records managers do not have a comprehensive knowledge of various departments within the organisations, this does not mean that adequate contextual information cannot be identified. In this situation, a strategic approach is essential to develop a meaningful relationship between a records management department and individual business operation departments to facilitate the task of acquiring adequate contextual information. Since the management of electronic records begins even before the creation of the records themselves, therefore records managers must be involved in the design of information systems to ensure the task of preserving electronic records can effectively and systematically be executed.

In a nutshell, it is likely to be expensive to preserve electronic records over time, as all the options of preservation require considerable funds. In addition, there is no 'one-size fits all' preservation strategy that accommodates various types of electronic records and different circumstances. Whichever preservation method is adopted, emulation, migration or XML, records managers must be alert to associated costs to avoid preservation efforts coming to an early halt. A comprehensive risk assessment and cost-benefit analysis is certainly essential to identify appropriate preservation strategies. Managing and preserving electronic records can only be successful if records managers or archivists are able to communicate professional ideas in a way that is acceptable to the culture of the organisation in which they are working (Murdock, 2006a). Failure of preservation efforts means the organisation is at risk of losing evidence and would be in a helpless state should any legal proceeding occur where they needed full access to all their records.

2.8.5 Security and Confidentiality of Records

Information and records are assets, and like other business assets they also require sound protection. Records with different value and level of confidentiality require different levels of protection. It is the value of the information contained that determines

[81] This does not mean that records managers have to understand every single business operation of the organisation, as they are the ultimate responsibility of individual operational managers. But, at least, records managers must have brief understandings of the function of every business department to help identify contextual information of their records.

the level of access and security required. Apart from access to physical records that have long been in place, governments have now through e-government initiatives, also provided online access to some public information. This, on the one hand satisfies public needs, but on the other hand exposes their records to security threats.

Security threats come in various forms both externally as well as internally. It is complicated enough to protect records from unauthorised external access, but it is far more complicated to protect records from unauthorised internal access. Leach (2003) states, many organisations suspect that their internal security threat is more pressing than their external threat. Schultz (2002) asserts although external threats, such as hacking attempts or viruses, have gained a lot of publicity, internal threats pose a significantly greater level of risks, as the controls and tools used for protection from external threats, such as firewalls and intrusion detection systems, are not effective in preventing internal threats.

Internal threats encompass a broad range of events, incidents and attacks, all connected by being caused not by external people who have no right to be using the corporate IT facilities but by the company's own staff, its authorised IT users. Buzzard (1999) suggests that the risk management approach can be applied as it is almost impossible to protect systems and networks against every conceivable eventuality[82]. Risk management enables an organisation to operate at an optimum economic cost by predicting the level of risks, and helps determine suitable action to mitigate the risks[83].

Internal security threats are mainly a result of staff actions, hence they can be minimised by improving user behaviour. Leach (2003) quotes the Information Security Forum (2003) report that suggests as many as 80 per cent of major security failures could be the result not of poor security solutions, but of poor security behaviour such as a lack of security common sense, users forgetting to apply security procedures, user taking inappropriate risks as they did not understand the level of risk involved, acts of

[82] Buzzard suggests that in this situation risk can be defined as the likelihood of a successful attack resulting in a breach in security and/or damage. It is a function of threat (from both malicious and accidental acts) and vulnerability, compounded by other factors such as value, system size, complexity and attractiveness to the attacker.
[83] Further discussion on risk management is available in *Section 2.7 Risk Management and Managing Records*.

negligence, and deliberate attacks. Leach (2003) advocates three key factors to improving user security behaviour, namely:

- The behaviour demonstrated by senior management and colleagues
- The user's security common sense and decision-making skills, and
- The strength of the user's psychological contract with the company.

Systems and security measures are man-made products, hence, their efficiency is highly dependent on human ethics. Practice by senior management and colleagues easily influence other staff attitudes. To prevent is always better than to cure. Therefore, increasing awareness among staff of their responsibility is essential to prevent any wrongdoing though it does not guarantee none will occur. Although, information systems come with audit trail features, foul play can only be detected after it occurs. Sometimes the cost of recovery can be formidable. Clear security and confidentiality policies and continuous awareness efforts on the importance of good user behaviour are essential for minimising internal security threats, and also leave more resources for the organisation to protect their records from external security threats.

CHAPTER 3

CASES OF POOR GOVERNANCE

3.0 CASES OF POOR GOVERNANCE

3.1 Introduction

This chapter attempts to discuss the impact of poor record keeping practices, both in the public and the private sector. The strength of a government is mainly dependant on the trust of the people it governs. A government is accountable to the people of the country to ensure its socio-economic and political stability, which, nowadays can only be achieved by being efficient and transparent in governance.

3.2 Cases of Poor Governance

The benefits of having an effective record keeping system only tend to surface after a corporate disaster has occurred. McKemmish (1999) reminds us that the relationship between record keeping and public accountability can be most spectacularly demonstrated through such failures. In a democratic country where accountability and value for money is important for a government to retain authority, a corporate disaster, particularly in a public organisation can have damaging consequences, thus eroding people's trust (Quirk, 1997). This may affect the government's chance of retaining power. A corporate disaster in the private sector can also have an indirect impact on government, as it reflects on the effectiveness of government regulations. The following cases reflect the impact of poor record keeping on both public and private organisations.

3.2.1 The Crisis in the Australian Government in the 1980s and 1990s

The national system of government in Australia draws both from the UK and the US, as well as having its own unique characteristics[1]. The management philosophy and practice in the Australian Public Service have changed since the 1970s. Reviews have been made by several groups including Metropolitan Ambulance Service Royal Commission Inquiry, Review of Commonwealth Functions, Review of Commonwealth

[1] The Australian Constitution provides for the powers of the Commonwealth of Australia to be exercised at three levels: 1) Power is conferred on the Parliament, 2) Executive power, to assent to and administer laws, and to carry out the business of government, is conferred on the Governor-General, Ministers of State, departments, other government agencies, and the defence forces, and 3) Judicial power is vested in the High Court of Australia and other courts established by the Parliament. Further information on the Australian Government structure, can be found in *Commonwealth of Australian Constitutional Act (The Constitution)*, available at http://www.comlaw.gov.au/comlaw/comlaw.nsf/440c19285821b109ca256f3a001d59b7/57dea3835d797364ca256f9d0078c087/$FILE/ConstitutionAct.pdf (4 September 2009)

Administration, Public Service Act Review Group and State and Territory Public Sector Reviews (Australian Public Service Commission, 2003). The resulting reforms have progressively reduced centrally administered, detailed controls over departmental staffing and finances.

From a records management perspective, there were two major cases of mismanagement or failures of public services, which occurred in 1980s and 1990s, involving three State governments, namely Queensland, Victoria and New South Wales. The Australian Society of Archivists (ASA) argues that these cases were alarming as they demonstrated serious disregard for the integrity of public records.

3.2.1.1 Heiner Affair

Following a written complaint of physical and sexual abuse of children in the John Oxley Youth Detention Centre (JOYC) by a staff member, the Department of Family Services (DFS) on 13 November 1989, appointed a retired Stipendiary Magistrate, Mr Noel O. Heiner, to carry out a Ministerial Inquiry to investigate and report back on the specific complaints against Mr Coyne, Manager of the JOYC and other matters touching JOYC security and treatment of detainees. The Heiner Inquiry subsequently became known as the 'Heiner Affair' as it failed to accomplish its objectives, but instead implicated more people including union leaders and ministers of the new Queensland government. Lindeberg (1999) contends the failure of the Heiner inquiry disclosed a comprehensive cover-up by the Labour government which cost him his job. The Heiner Affair received nation-wide media coverage, particularly in the state of Queensland. The following chronology of events demonstrates how the Heiner inquiry developed[2].

The Heiner Inquiry was established during the National Party government and lasted only for approximately four months when its termination was announced on 12 February 1990, by the newly elected Labour government led by Premier Wayne Goss. Since

[2] Only key events relevant to issues of accountability and records management are included. More detailed chronology of the Heiner Affair is available in a report by the House of Representatives Standing Committee on Legal and Constitutional Affairs, which is available at: http://www.aph.gov.au/house/committee/laca/crimeinthecommunity/subs/sub142.pdf (21 June 2007); and in a paper entitled 'The Beginnings of Shreddergate: the Shredding of the Heiner Inquiry Documents and Related Materials: The Chronology of Events' which is available at: http://www.gwb.com.au/gwb/news/goss/history99.doc (8 May 2006).

then, for fifteen years and under two premierships[3], of Wayne Keith Goss and Peter Douglas Beattie, and even with 28 months gap between the two, the Heiner Affair continued to tarnish the reputation of the Labour government after investigations by subsequent committees failed to identify the culprits in the case.

The underlying problem in the Heiner Affair, which led to lengthy and complicated investigations, was the destruction of evidence gathered by Heiner. So as to substantiate the original written complaint against Mr Coyne, Mr Heiner gathered evidence from JOYC staff on tapes and records on computer discs, and then transcribed to paper. Pressured and worried about his position, Mr Coyne approached the JOYC Director General, Mr Alan Pettigrew seeking (1) a copy of all written complaints; (2) written advice on the process of how the complaints were going to be investigated; (3) and the opportunity to organise and conduct a defence against the complaints laid. However, he was refused access to specific written complaints, instead was only given a brief one-page outline. The original written complaints were kept in the DFS and acquired status of 'public records' thus subject to Public Service Management and Employment (PSME) Regulation 65.

On 2 December 1989, the Queensland Government changed when the new Labor government came to power. Mr Wayne Keith Goss, a qualified solicitor, became Premier and Minister responsible for the State Archives. Ms Anne M Warner, former Shadow Spokesperson and aware of activities inside JOYC, became the Minister for Department of Family Services and Aboriginal and Islander Affairs (DFSAIA). Ms Ruth L Matchett was appointed as acting Director General by the Minister replacing Mr Pettigrew. On 14 and 18 December 1989, Mr Coyne officially asked Ms Matchett for copies of the original complaints and transcripts of evidence gathered by Mr Heiner in order to defend himself. He also questioned the legal validity of the inquiry and informed Ms Matchett that he would sue for defamation if his career suffered as a consequence of the inquiry. Once again, his request was turned down. On 11 January

[3] The premiership period of Wayne Keith Goss was from 7 December 1989 to 19 February 1996, and it was the first time in 32 years of the Australian Labor Party (ALP). However, the ALP failed to remain in power as the National Party of Australia and Liberal Party of Australia formed a coalition government but only for two years from 19 February 1996 to 26 June 1998. The Australian Labor Party returned to govern Queensland on 26 June 1998 until now under the premiership of Peter Douglas Beattie. Further information is available at: http://www.australianpolitics.com/states/qld/premiers.shtml (10 May 2006).

1990, during a full-day of evidence gathering from Mr Coyne, Mr Heiner confirmed that allegations of criminal conduct have been made against him (Mr Coyne). Under mounting pressure, Mr Coyne through his solicitors, Rose Berry Jensen, threatened a writ of prohibition on the DFS regarding natural justice being afforded to him during the inquiry process. The department was given twenty-four hours to respond.

Ms Matchett consulted the Crown Solicitor for advice on how to deal with Mr Coyne's solicitor's letter and on the legality of the Heiner inquiry. The situation later implicated Mr Kevin Lindeberg, the organiser of the Queensland Professional Officers Association (QPOA), and Ms Janine Walker, the Queensland State Services Union (QSSU) Industrial Relations Director, when Ms Matchett requested 'off-the-record' meetings with them. Mr Lindeberg and Ms Walker were informed that the Heiner inquiry has been closed, and she (Ms Matchett) has taken possession of all the Heiner documents. Mr Lindeberg indicated that his QPOA member, Mr Coyne, still wished to see the written complaints against him, and there would be no further 'off-the-record' meetings with the DFS[4].

At a Cabinet meeting on 12 February 1990, the Heiner inquiry was officially terminated and all the evidence gathered by Mr Heiner was secretly transferred to the Office of Cabinet from DFSAIA. Two days later, Mr Coyne instructed his solicitor to serve notice on the DFSAIA of his intention to commence court proceedings to gain access to the documents. On 19 February 1990, despite being informed of Mr Coyne's intention to commence court proceedings, the Goss Cabinet decided to seek urgent approval from the State Archivist to destroy the documents. On 23 February 1990, the Acting Cabinet Secretary, Mr Tait wrote a letter to the State Archivist seeking her immediate approval to destroy the documents on the Cabinet's view that they are "… no longer required or pertinent to the public record"; but failed to mention Mr Coyne's intention of commencing court proceeding.

[4] Mr Lindeberg initially was not aware of the child abuse cases in the JOYC until 1998. He fought for Mr Coyne to gain access to official complaints against him (Mr Coyne) without realising the fact that there were criminal cases in the detention centre. Mr Coyne was also a member of Queensland Teachers Union (QTU). He was eventually immediately dismissed after 6 years as senior organiser of the QPOA for allegedly inappropriate and over-confrontationalist behaviour, against Minister Anne Warner. Further information is available in *The Beginnings of Shreddergate: the Shredding of the Heiner Inquiry Documents and Related Matters*. http://www.gwb.com.au/gwb/news/goss/history99.doc (8 May 2006).

On the very same day, the documents were transferred from the Cabinet Office to the State Archives. Unbelievably, Ms Lee McGregor, the State Archivist, faxed written approval in less than a working day for the destruction of the material despite having over 100 hours of taped evidence and other materials to check and ensure that the material had no informational, administrative, data, historical or legal value, necessary to comply with standard archival appraisal principles and her statutory duty under the Libraries and Archives Act 1988. Although Ms McGregor recognised that the documents were defamatory in nature, she did not specify how it was. The documents were returned to the Cabinet office later on the same day. This troubled the Australian Society of Archivists and Chris Hurley, as is discussed later in this section.

From 23 February to 23 March 1990, there were further events involving Ms Matchett and her Assistant Executive Mr Trevor Walsh, Mr Coyne and his solicitor, DFSAIA Minister Warner and her private secretary Ms Norma Jones, Mr Lindeberg, QPOA General Secretary Mr Donald Martindale and Assistant General Secretary Ms Roslyn Kinder, and the Acting Cabinet Secretary Mr Tait. On one occasion on 13 March 1990, Minister Warner refused to meet Mr Lindeberg as she did not want to deal with him on the 'Coyne Case', instead only met Mr Martindale and Ms Kinder. Understandably, it was the Minister's reaction to Mr Lindeberg's constant demands to access the Heiner documents, including the use of legal procedures that caused most concern. The actual destruction occurred on 23 March 1990 after a senior archivist was despatched from the State Archives to the Cabinet Office. Together with Ms Matchett's executive officer Mr Trevor Walsh, they secretly destroyed the Heiner documents.

Mr Coyne subsequently became aware of the destruction of the evidence and wrote a letter to Ms McGregor seeking confirmation as to whether the Heiner documents had been destroyed. Ms McGregor did not respond to his letter, instead contacted Ms Matchett's executive officer Mr Walsh. Ms Matchett sought the Crown Solicitor's advice only for permission for her to amend his (the Crown Solicitor's) letter sent to Mr Coyne's solicitor and QTU. The letter stated that her Department did not hold the original complaints sought by Mr Coyne, and all the Heiner documents had been destroyed. On 23 May 1990, Ms Matchett's Principal Liaison Officer, Mr Donald A C Smith, without

prior lawful approval from the State Archivist, shredded the photocopies of the original complaints.

Since then, several investigations have been established including the Forde Inquiry[5], however, these failed to identify the culprit in the case until May 2002, when the House of Representative Standing Committee on Legal and Constitutional Affairs began to investigate the case. It was Mr Lindeberg who became the scapegoat, but also the crusader who revealed a cover-up of illegal behaviour by the then Premier Wayne Goss and his Cabinet Ministers when they joined together to authorise the destruction of evidence taken by Mr Heiner in 1989.

The investigation led to the conviction of Pastor Douglas Ensbey, who on 11 March 2004, was found guilty under section 129 of the Queensland Criminal Code Act 1899 of destroying the diary of a child abuse victim six years prior to the girls reporting the incident to police, and the possibility of instituting legal proceedings. He was given a six month wholly suspended sentence. Ensbey was stationed at the Sandgate Baptist Church in the mid-1990s when the parents of a girl who was a JOYC detainee, gave the diary to Ensbey to carry out an internal church investigation. Ensbey, however, called the girl a liar and advised the family against going to the police, cut up the notes in his parish guillotine after the abuse victim's mother demanded the pages back[6].

If there has been no cover up by the Labour government of Queensland, the Heiner Inquiry would have been completed far earlier. Over the fifteen years of investigation the cost of the investigations was considerable, yet only one person was convicted, whilst others including senior government officials and politicians, despite the disclosure of their mismanagement, escaped scot-free.

---

[5] The Forde Inquiry is the informal title of a lengthy report presented to the government of Queensland, Australia in May 1999. The formal title of this document is *"The Report of the Commission of Inquiry into Abuse of Children in Queensland Institutions"*. During the period from August 1998 through May 1999, the commission conducted intensive inquiries into the current and past administration of various orphanages, reformatories, and detention centres for wayward children maintained in Queensland. Further information available at: http://www.fordefoundation.org.au/about_the_forde_inquiry.html (6 October 2009).

[6] Pastor Sacked for Shredding Abuse Evidence, *The Age*, 21 December 2004. http://www.theage.com.au/news/National/Pastor-sacked-for-shredding-abuse-evidence/2004/12/21/1103391750380.html (26 June 2006).

3.2.1.2 Victoria Metropolitan Ambulance Service

The delegation of power and administration of public services, to some extent, has resulted in mismanagement and corruption as some public officials turned their back on delivering accountable, effective and efficient services to the public. Beechey (1997), a journalist of Green Left Weekly[7] reported that on 7 May 1997, two fire emergency vehicles raced through rain and peak hour traffic to the inner suburb of Carnegie in Victoria, where a semi-trailer had reportedly overturned, trapping its driver. Finding nothing, the crews requested further information and were eventually told that the accident was in Sydney.

The incident prompted the United Firefighters Union (UFU) to announce it would stop work, under provisions of the Occupational Health and Safety Act, if concerns over the Intergraph emergency dispatch system were not resolved. According to Peter Marshall, secretary of the UFU, firefighters have lodged nearly 1500 reports of problems involving Intergraph since July 1996. Most of these involved delays caused by wrong addresses or Melway references, or inappropriate vehicles being sent. In an emergency service, any delay is potentially life-threatening. On 19 May, the Coroner's Court heard that a 26-year-old man had died in February of a drug overdose after an ambulance took over an hour to arrive. The court was told that Stewart Marshall might have been saved if he had received paramedic help before he stopped breathing, 25 minutes after his father found him unconscious and dialled the emergency service. There had been six other coroner's inquests into deaths involving delays in ambulance or fire services since 1994.

A report of an investigation by the Auditor-General of Victoria, Ches Baragwanath, raised much concern about the probity of contractual and outsourcing arrangements at the Metropolitan Ambulance Service (MAS) over the period April 1993 to March 1995 (Victoria Government, 1997). Baragwanath made a very strong statement that a legal inquiry, in which witnesses were required to give evidence under oath, may be necessary to determine whether the various contractual arrangements of the service,

[7] *Green Left Weekly* is an independent media committed to human and civil rights, global peace and environmental sustainability, democracy and equality. Although it is radical, the fact of this case revealed by the media is similar to the ones available in the report by the Auditor-General of Victoria. Further information available at http://www.greenleft.org.au/what.htm. (22 June 2006).

which at best involved serious mismanagement, or at worst, constituted corrupt activity. The report illustrates that former senior management at MAS throughout the period showed a total disregard for the Government's outsourcing guidelines and normal tendering processes as reform goals were swiftly pursued. However, Premier Jeff Kennett, health minister Rob Knowles and former health minister Marie Tehan all denied any knowledge of breaches, saying that the government became aware of the situation only in May 1996, when Knowles ordered the auditor-general's investigation into the tendering process. Ironically, on 20 May, a memo written in February 1996 from the chief executive officer of MAS, Peter Olszak, to Tehan was leaked to the press. The memo referred to freedom of information was requested by Labor health spokesperson John Thwaites, and warned of political risks from the fact that MAS did not comply with normal procedures in obtaining at least three independent bids. Tehan, however, maintained that she did not see the memo.

The report also revealed serious deficiencies in contract management, which led to poor service performance that spurred complaints particularly by the public, and also the UFU. The investigation was into the behaviour of the former chief executive of MAS, Mr J. Firman and his hand-picked administrator, Mr J. Perrins, who was a partner in the chartered accounting and business advisory firm, Price Waterhouse; two consultancy companies namely, Griffiths Consulting Pty Ltd and Henderson Consultants; and three other companies namely Intergraph Corporation Pty Ltd, Emergency Services Pty Ltd, and JMJ Fleet Management Pty Ltd. The report identified six serious deficiencies, namely:

- *engagement of Griffiths Consulting Pty Ltd to provide numerous consultancies encompassing the total management of several tender arrangements and of a contract subsequently entered into with appointed tenderers (actual cost: $1.5 million);*
- *management of tendering processes by Henderson Consultants for a new computerised ambulance dispatch system and the sub-contracting by the MAS of certain non-emergency services (actual cost: $216, 000);*
- *the awarding of the contract relating to the outsourcing of new computerised communications systems in March 1994 to Intergraph Corporation Pty Ltd (initial cost: $7.5 million over 4 years);*

- *the outsourcing of the operation of new financial and management information systems and the MAS's subscription system under which a contract was ultimately awarded to Emergency Services Pty Ltd, a company established by the chartered accounting firm Arthur Andersen (current cost estimate of approximately $15 million over 4 years);*
- *the outsourcing of the management and maintenance of the MAS's ambulances and other vehicles leading to a contract let to JMJ Fleet Management Pty Ltd (estimated cost of approximately $2 million a year); and*
- *the sub-contracting of particular non-emergency ambulance services to 4 separate companies (estimated cost of approximately $6 million a year). (Victoria Government, 1997:4).*

The investigation discovered that the management of MAS created an environment that enabled the consultancy firms to reap significant financial benefits without challenge. Tenders were not sought for services provided by these firms and there was no evidence to indicate that consideration was given to ensuring that conflicts of interest did not arise from previous working relationship between Mr Firman and the firms. In addition, there was no key documentation encountered during an audit process, making it impossible for the audit team to fully evaluate the soundness of recommendations made by consultants. This also hampered earlier police investigation.

It was also discovered that Mr Firman, despite been alerted by MAS's then manager of information systems about major functional and technical shortcomings of the future system. He made personal comments on the "quality of needs" analysis of a computerised communication system prepared by Henderson Consultants. Mr Firman accepted the proposal and hurriedly, within less than a month, assigned the development and implementation of the system to Intergraph Corporation Pty Ltd (Intergraph) in September 1993. There were doubts as to the integrity of the tendering process, as tender documents were distributed to four short-listed companies on 30 August 1993. The companies needed to respond by 29 September 1993. However, only three companies responded following a formal withdrawal of a company which believed that it was impossible to deliver a professional document and install a working system within the time frames defined within the tender. That company also suggested that other vendors may be prepared to gamble on meeting them, or perhaps plan to re-

negotiate the schedule after the tender phase, which, it believed was not the correct way to conduct a business partnership.

Eventually, in March 1994, Intergraph was awarded the contract. A nine-day visit was made to Intergraph sites in North America by three MAS senior officials. The visit was organised and funded by Intergraph to inspect its systems and organisation. Strangely, however, the timing of the visit was two days after the signing of the contract with Intergraph. The auditor-general noted that although a request for approval was submitted by MAS prior to signing the contract, a serious doubt was given concerning the proprietary of accepting any benefit from an appointed contractor. He wondered why such trip did not occur before formal signing and what could be gained from such trip after that contract had been signed (Victoria Government, 1997).

Subsequently in December 1994, the contract was changed to allow Intergraph not only to supply, but also to operate the emergency system. Mr Firman also failed to satisfy adequately a key condition set by the Government that the new system must be capable of integration into the planned State-wide emergency communication system, irrespective of the eventual supplier. The implementation of the system with major shortcomings resulted in chaos in the delivery of emergency services to the public. Escalating complaints came from the UFU and those who were affected by the failure of the emergency system. Subsequently police investigation was carried out due to the absence of documents. Eventually the auditor-general was forced to investigate the problem.

Beechey (1997) also reported that during 1993 to 1994, Firman instituted a series of three-day live-in courses for MAS middle management. These courses were described by some participants as “mini-Camp Wacos” at which participants who expressed critical opinions of the new management line were subjected to emotional and personal abuse. They became exhausted and traumatised. Over this period, the number of full-time operational officers dropped from 768 to 674, and the cost of departure packages jumped from $1m to $5m. The MAS Regional Training Unit was closed, and attempts were made to force ambulance officers to improve their knowledge and skills in their own time. The saga of Mr Firman and his associates continued until March 1995, when

Intergraph appointed Griffiths Consulting's owner, Grant Griffiths, as director and CEO of its Australian subsidiary, Intergraph Public Safety.

Another former MAS manager was responsible for outsourcing contracts for non-emergency patient transport, and he was also involved in a company in which he had been awarded one of the contracts. In September 1995, the ministers responsible for emergency services approved the extension of Intergraph to fire and police services, despite a November 1994 report from the Metropolitan Fire Brigade's director of technical services describing Intergraph as "a very high risk and significantly lacking in its ability to meet MFB requirements".

The Intergraph system was not operated by qualified fire, police or ambulance officers, but by employees who are expected to determine the urgency of response by asking a series of set questions. The system was designed to transfer information quickly to mobile computer terminals in emergency vehicles, eliminating the need for radio directions, which can be misinterpreted. However, this equipment was never delivered. When several emergencies happened at once, then bottlenecks occurred. Following complaints by the UFU and Ambulance Employees Association (AEA), MAS and Intergraph agreed to improve the services. However, it failed to meet minimum requirements, including a failure to employ adequate staff and, to provide necessary training and equipment. Reflecting the continuous failure by MAS and Intergraph, the Secretary of the AEA, Rod Morris noted that the worst aspect of the Intergraph affair is not the cost, but the fact that the government lost control of essential services, and as a result people died unnecessarily[8].

The auditor-general's report also revealed that the salaries of Mr Firman and other senior staff were paid into Firman's private company, Pinelow Pty Ltd. This revealed that Mr Firman breached the trust of his authority as the chief executive officer of MAS. Mr Firman was an opportunist who abused trust and systems, whilst the government of Australia tried to improve public services through corporatisation and privatisation. As a result, more power was delegated to public organisations, including MAS in order to facilitate decision making processes. However, those public organisations had to generate revenue reaching targeted amounts anticipated by the government.

[8] http://www.greenleft.org.au/back/1997/276/276p7.htm (22 June 2006).

Unfortunately, in the case of MAS, the absence of a proper record keeping system enabled Mr Firman and his associates easily to exploit various circumstances to hide their corrupt practices.

These would be clearly seen from the very beginning of the tendering process of the emergency system. The way the invited tenderers were given was an unrealistic time frame to prepare tender details and to implement such complicated and vital emergency systems are impossible. There was an unrecorded assessment of two separate teams, as Mr Firman wanted, and that led to the project being awarded to Intergraph. Reflecting the rampant mismanagement and corruption in the MAS, McKinnon (1994)[9] stated that 'poor record keeping attracts corruption like a carcass attracts flies'[10].

Mr Firman's and his associates' heyday ended when they were replaced by a new management team in May 1995, which faced an uphill task as Mr Firman had failed to secure estimated savings of $20 million that MAS envisaged could be achieved over a four year period from the start of the outsourcing arrangements. Furthermore, the new chief executive officer faced a major and resource-demanding task of achieving satisfactory performance from the outsourced arrangements. The report into MAS stated that the new management team had progressively implemented a new records management system as a part of initiatives to improve the processes and integrity of contracts management (Victoria Government, 1997).

3.2.2 The Collapse of Enron

On 26 May 2006, Kenneth Lay, the founder of Enron, and Jeffrey Skilling, his former chief executive, faced long terms in jail after a jury found them guilty of conspiring to commit one of the biggest frauds in the US history[11]. Lay faced a maximum jail sentence of 165 years if given the full term for each guilty verdict. Skilling faced a maximum prison sentence of 185 years. Earlier, in June 2002, Enron's accounting firm,

[9] McKinnon, J. (1994). The 'Sports Rorts' Affair: a Case Study in Recordkeeping, Accountability and Media Reporting, *New Zealand Archivist,* V(4), Summer/December 1994, pp. 1-5. Cited in McKemmish (1999)

[10] Cited in McKemmish and Acland (1999).

[11] Lay was found guilty on all six charges of fraud and conspiracy, and was also found guilty of four separate bank fraud charges that were heard in a trial without a jury. Skilling was found guilty of 19 counts, and not guilty of a further nine charges of insider trading. Lay died of a heart attack on 5 July 2006, six weeks after he was found guilty.

Arthur Andersen was found guilty of obstruction of justice and forced out of business. In October 2002, Andrew Fastow, Enron former chief financial officer was indicted on 78 counts of fraud and conspiracy. Eventually, in January 2004, Fastow pleaded guilty to fraud-related charges. The verdict on Lay and Skilling marked the final episode of the virtually demise of Enron. Enron filed for bankruptcy on 2 December 2001 in what was then the largest corporate failure in US history. At the time of the collapse, Enron was ranked as the seventh largest company in the US with over $100 billion in gross revenues and 20,000 employees worldwide[12]. As a consequence, thousands of people lost their jobs and life savings[13].

The history began when Enron was founded in 1985 as the product of a merger of two natural gas pipeline companies – Houston Natural Gas and Internorth – Enron owned from its outset the largest interstate network of pipelines. Coffee[14] (2006), asserts that as late 1990, Enron remained primarily in the pipeline business until deregulation of gas prices led to increased used of spot market transactions[15] that naturally produced greater volatility in gas prices[16]. Coffee further states that Jeff Skilling advised that Enron should create a natural gas 'bank' that would intermediate between suppliers and buyers of natural gas. Enron, then began to offer utilities and other major customers long-term fixed price contracts for natural gas. It then protected itself by using financial derivatives – chiefly, swaps contracts – to hedge this risk. This business model largely worked as Enron could profit from trading in the natural gas market where it had superior information. By 1992, Enron had become the largest seller of natural gas in North America, and its trading activities were the second largest contributor to its overall income.

---

[12] *The Role of the Board of Directors in Enron's Collapse: Report Prepared by the Permanent Subcommittee on Investigation of the Committee of Governmental Affairs*, United States, 107th Congress, 2nd Session, Report 107-70 (8 July 2002), p7. Cited in Coffee, J.C. (2006:18).
[13] Enron Chiefs Face Rest of Their Lives in Prison, *The Guardian*, 26 May 2006, p1.
[14] Listed as one of the 100 most influential lawyers in the United States by *the National Law Journal*, United States, and Adolf A. Berle Professor of Law at Columbia University Law School.
[15] By 1990, 75 percent of gas sales between pipelines and their utility customers were conducted on a spot market basis. (Coffee, 2006:48).
[16] A comprehensive story of the collapse of Enron can be found in his recently published book, *Gatekeepers: the Professions and Corporate Governance*. However, his definition of the term 'gatekeepers' does not include professional records managers or archivists, instead it embraces audit committee, auditors, securities analysts, attorneys and credit rating agencies, who are responsible for ensuring the accuracy of information used for decision-making within their capacity and responsibility in the chain of the business.

The following table by Healy and Palepu[17] (2003) provides a timeline of critical event leading to the collapse of Enron.

Date	***Event***
14 August 2001	Jeff Skilling resigned as CEO, citing personal reasons. He was replaced by Kenneth Lay
Mid- to late August 2001	Sherron Watkins, an Enron vice president, wrote an anonymous letter to Kenneth Lay expressing concerns about the firm's accounting. She subsequently discussed her concerns with James Hecker, a former colleague and audit partner at Andersen, who contacted the Enron audit team.
12 October 2001	An Arthur Andersen lawyer contacted a senior partner in Houston to remind him that the company policy was not to retain documents that were no longer needed, prompting the shredding of documents.
16 October 2001	Enron announces quarterly earnings of $393 million and nonrecurring charges of $1.01 billion after tax to reflect asset write-downs primarily for water and broadband businesses.
22 October 2001	The Securities and Exchange Commission opened inquiries into a potential conflict of interest between Enron, its directors and its special partnerships.
8 November 2001	Enron restated its financials for the prior for years to consolidate partnership arrangements retroactively. Earnings from 1997 to 2000 declined by $591 million, and debt for 2000 increased by $658 million.
9 November 2001	Enron entered merger with Dynegy.
28 November 2001	Major credit rating agencies downgraded Enron's debt to junk bond status, making the firm liable to retire $4 billion of its $13 billion debt. Dynegy pulled out of the proposed merger.
2 December 2001	Enron filed for bankruptcy in New York and simultaneously sued Dynegy for breach of contract.

Table 3.2.2: The timeline of critical events for Enron in the period August to December 2001, (© Healy and Palepu, 2003).

Skilling proposed in the late 1990s that Enron should transform itself further by adopting what he termed an 'asset light' policy, which means that Enron should dispose of 'heavy

[17] Paul M. Healy is the James R. Williston Professor of Business Administration and Krishna G. Palepu is the Ross Graham Walker Professor of Business Administration, both at Harvard Business School, Boston, Massachusetts.

assets', to the extent that they generated useful information that could be used in its trading activities. Coffee (2006), however, argues that Skilling's strategy, in turn would lead to a problem of finding buyers as many of Enron's 'heavy assets' were overvalued or unattractive to strategic buyers. Coffee (2006) suggests the strategy was the ultimate cause of its downfall as a result of failure to find third party buyers. This means that Enron had to sell those assets within itself – or, more accurately, he argues, to control affiliates in non-transparent transactions.

Coffee suggests that by the late 1990s, Enron had come to believe that it could profit by trading in a variety of volatile markets, namely energy, electricity and broadband communications. Enron disguised the lack of success of these businesses by exploiting accounting rules and conventions to present only an opaque picture of its operations that hid much and revealed little. In order to enter a long-term contract in providing energy at a fixed price and receive a sizeable cash or down payment, the accounting rules require organisations to present the value of long term contracts. In other words, Enron needed to provide evidence of financial affordability to invest in such businesses. Coffee (2006) cynically argues that,

> *Enron took to this task like a duck to water. It enthusiastically valued twenty-year contracts, always estimating their net future cash flows to produce a large profit for Enron. Probably the most extreme example was a twenty year contract, entered in July 2000, with Blockbuster Video to develop a system of entertainment-on-demand services across a range of U.S. cities by year-end. Enron's role was to store and broadcast the entertainment on its still underdeveloped broadband network. Based on only a few pilot projects in three cities, Enron recognised profits of $110 million from the Blockbuster deal, even though it had not yet solved such technical problems as delivering broadband over the 'last mile' to the consumer or gauging the level of market demand. Similarly, Enron marked to market a fifteen-year period to supply electricity to Eli Lilly's Indianapolis plant, valuing contract over $500 million. Yet, because Enron had to estimate the present value of the costs of servicing this contract in order to book a profit because Indiana had not yet deregulated electricity, this forced*

> *Enron to predict when, over the fifteen years period, Indiana would deregulate electricity prices and what the impact would be on the costs of servicing the contract. (Coffee, 2006:21).*

Enron's fake financial stability was also camouflaged through its a lattice of 3,000 separate subsidiaries and proxies[18], or what Enron termed as 'special purpose entities', to artificially boost profits and hide liabilities. Irregular transactions between Enron and its 'special purpose entities' were known to Enron's audit committee and its external auditors, but neither appears to have expressed any serious concerns before the collapse. Instead, it was Sherron Watkins[19], a finance executive, and the whistleblower of the case who wrote a memo to Skilling warning that dubious bookkeeping could cause Enron to 'implode in a wave of accounting scandals'. However, her warning was diplomatically ignored when Enron conducted a bogus investigation using its auditors, who had found nothing out of place.

On 22 October 2001, the Securities and Exchange Commission (SEC) opened inquiries into a potential conflict of interest between Enron, its directors and consolidate partnerships. Enron, in turn, was asked to restate its financials for the prior four years to consolidate partnership arrangements retroactively. Ironically, earnings from 1997 to 2000 declined by $591 million, and debt for 2000 increased by $658 million. Eventually, when these irregularities were discovered, Enron was forced in October 2001 to disclose that it had overstated its earnings for 1996 to 2000 by some $613 million (or 23 percent of reported profits over this period). The only option to remain in business, on 9 November 2001, was for Enron to enter into a merger agreement with Dynegy, a much smaller competitor in its field. However, subsequently on 28 November 2001, Dynegy pulled out of the merger as it discovered Enron's serious financial position. With no option available, Enron eventually filed for bankruptcy in New York as a direct consequence of a lack of ethics and greed by its senior management.

---

[18] Enron: Bad Business, *The Guardian*, 26 May 2006, p38.

[19] Sherron Watkins was the former vice president of Enron Corporation when she alerted then-Chief Executive Officer, Kenneth Lay to accounting irregularities within the company. *TIME magazine* named Sherron, along with two others, as their 2002 Persons of the Year for being "people who did right just by doing their jobs rightly." Now an independent speaker and consultant, she co-authored *Power Failure: the Inside Story of the Collapse of Enron* (Doubleday, 2003). She is a Certified Public Accountant and holds a Masters in Professional Accounting as well as a B.B.A. in accounting and business honours from University of Texas at Austin.

3.2.3 The Hutton Inquiry and the Butler Report

The Hutton Inquiry, perhaps, is one of the highest profile investigations in decades in the UK. Table 3.2.3 provides the chronology of events surrounding the Hutton Inquiry and the Butler Report. It was named after Lord Brian Hutton, the chair of the public inquiry. It was an inquiry into the circumstances surrounding the death of Dr David Kelly, who took his own life on 23 July 2003. Dr Kelly was a dedicated scientist and weapon expert at the Defence Evaluation and Research Agency (DERA), an arm of the Ministry of Defence, UK (MoD), and was one of the chief weapons inspectors in Iraq on behalf of the United Nations Special Commission (UNSCOM).

Date	***Event***
24 September 2002	The Labour Government released Iraq's Weapons of Mass Destruction dossier.
22 May 2003	Dr Kelly met a BBC's journalist Mr Andrew Gilligan in the Charing Cross Hotel.
29 May 2003	Mr Gilligan's broadcast on the BBC Today programme.
9 July 2003	Dr Kelly's name was disclosed by the MoD
17 July 2003	Dr Kelly committed suicide.
18 July 2003	Lord Hutton was requested by the Rt Hon Lord Falconer of Thornton, the Secretary of the State for Constitutional Affairs, to conduct an Inquiry into the death of Dr David Kelly.
1 August 2003	A preliminary sitting of the Inquiry was held.
4 September 2003	First stage of the Hutton Inquiry commenced.
28 January 2004	The report of the Hutton Inquiry was published.
3 February 2004	Butler Report was established to review the intelligence on WMD.
7 July 2004	A 1,000-page report by US Chief Weapons Searcher, Charles Duelfer was released. Confirmed no WMD in Iraq as claimed by President George W. Bush.
14 July 2004	Butler Report was published.

Table 3.2.3: The timeline of events surrounding the Hutton Inquiry and the Butler Report.

Dr Kelly had a considerable reputation as a weapon inspector, not only in the UK but internationally too. He was dubbed as an 'inspector's inspector' by journalists for his

dedication, professionalism and expertise. The issues surrounding the death of Dr Kelly was of much public concern as it was connected to the decision by the Labour government to go to war in Iraq despite lack of evidence to support its claim that Iraq had chemical and biological weapons that were deployable within 45 minutes. Dr Kelly, who had been involved in investigating a biological warfare programme in Iraq since 1991, must have known full well about the integrity of this claim. Furthermore, there was only one source of the information used by the Joint Intelligence Committee (JIC), and the accuracy of the information had never been verified. On 22 May 2003, Dr Kelly met a BBC journalist, Andrew Gilligan, who later announced the alleged claim on the BBC Today programme on 29 May 2003. The Government probably knew that the 45 minutes claim was wrong, even before it decided to put it into the dossier.

The Hutton report concluded that Gilligan's allegation was unfounded. Dr Kelly's name was later disclosed to the press by the MoD in the midst of a major controversy relating to Mr Gilligan's broadcasts. The report contained very grave allegations about the integrity of the government. The government's concern was it would be charged with a serious cover up if it did not reveal that a civil servant had come forward[20]. The report also revealed that after meeting Mr Gilligan, Dr Kelly subsequently realised that the meeting was unauthorised and he was acting in breach of the Civil Service code of practice. It was suggested that after Mr Gilligan's broadcasts, Dr Kelly came to realise the gravity of the situation for which he was partly responsible by commenting on intelligence matters. He admitted this to his friend and colleague Ms Olivia Bosch after the meeting with Mr Gilligan[21]. The report also noted the major factor contributing to the death of Dr Kelly was severe loss of self esteem, resulting from his feeling that people had lost trust in him and his dismay at being exposed in the media[22].

The Hutton Inquiry was specifically meant to investigate the circumstances surrounding the death of Dr Kelly. The conclusions of the Inquiry did not satisfy many as the main issue about the Government's role in 'sexing up' the dossier was not resolved. It was seen as a whitewash according to two surveys, while others believed the government

[20] Hutton Inquiry, p 324.
[21] *Ibid*. p 321.
[22] *Ibid*. p 325.

had been damaged by the affair[23]. Deliberately or otherwise, Dr Kelly had raised wider questions about the quality, interpretation and presentation of intelligence that Hutton left unanswered. In the midst of massive pressure to resurrect its reputation, the Labour Government, on 3 February 2004, announced the formation of a Committee of Privy Councillors in the House of Commons, which is also known as the Butler Inquiry, to review intelligence on WMD which played a key role in the Government's decision to invade Iraq[24].

The Butler Report was released to the public on 14 July 2004. Like the Hutton Inquiry, the Butler Report did not satisfy many and its conclusion was regarded as a very British one – yes there were failures but no, no individual can be blamed (Reynolds, 2004). Although the report did not identify any culprit, many expected the government to be found guilty. It clearly stated the committee's concern that government's machinery was less effective than it used to be (Committee of Privy Councillors, 2004). This is based on evidence received from two former Cabinet members, one of the present and one of a previous administration, who expressed their concern about the informal nature of much Government decision-making, and the relative lack of use of established Cabinet Committee machinery. It is also noted that papers on the Cabinet agenda were not distributed in advance, plainly reducing the ability of the Cabinet members to prepare properly for discussion of such important issues.

The committee concluded that the informality and circumscribed character of the Government procedures in the context of policy-making towards Iraq risks reducing the scope for informed collective political judgement. Moss (2005) explains that this was also of concern of the editor of the *Times*[25], who wondered how the Cabinet Office had become effectively an electronic office without adequate record keeping practices. He further argues that it is extraordinary that on the evidence presented to Hutton, only two

[23] See Hutton Report Seen as Whitewash – Poll. Available at: http://www.dailymail.co.uk/news/article-207019/Hutton-report-seen-whitewash--poll.html (4 September 2009)

[24] A similar commission was formed in the United States, when President George W. Bush, on 6 February 2004, announced the formation of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. The Commission concluded that the Intelligence Community was 'dead wrong' in almost all of its pre-war judgements about Iraq's WMD and that this constituted a major intelligence failure. Further information available at: http://www.gpo.access.gov/wmd/pdf/full_wmd_report.pdf (4 September 2009).

[25] http://www.timesonline.co.uk

drafts of the dossier were submitted. This suggests, as he reckons, that it is possible that the dossier was created by exchanging electronic copies in which changes were not tracked and that is unlikely. It is imperative to improve the present record keeping practice in the government as the public can no longer accept such unconvincing explanations for the controversial dossier. This can only be achieved if the government is committed to demonstrate accountability and transparency, without the need to worry about any contingent liabilities that may surface as a result of keeping the records of their actions and decisions.

3.2.4 Dr. Harold Shipman Serial Killer

Harold Frederick Shipman was convicted at Preston Crown Court on 31 January 2000, of the murder of 15 of his patients while he was a General Practitioner (GP) at Market Street, Hyde, near Manchester and of one count of forging a will. He was sentenced to life imprisonment. The trigger point of his arrest was the forgery of the will of his last victim, Mrs Kathleen Grundy. The Shipman Inquiry's First Report (2002) reveals that Shipman sought to obtain the whole of Mrs Grundy's substantial estate, leaving nothing to her well-loved daughter and grandchildren. He chose to forge the will of a woman whose daughter, Mrs Angela Woodruff, was a solicitor, who might therefore be expected to know something about her mother's previous testamentary arrangements. The forged will, which was produced using his old-fashioned Brother portable typewriter, and with odd signatures, looked thoroughly unprofessional and it was wholly foreseeable that it would arouse suspicion even from a non-expert. Mrs Grundy's body was exhumed on 1 August 1998, after Mrs Woodruff became suspicious about the forged will.

A subsequent post-mortem found traces of diamorphine in her body. Shipman was charged with Mrs Grundy's murder on 7 September 1998, after going to Ashton-Under-Lyne police station for an interview. Police had also investigated allegations that he might have murdered many more patients while he was a GP in Hyde and Todmorden. Between 1 August to 8 December 1998, nine more bodies were exhumed, and Shipman was subsequently charged with their murder on separate occasions, including the final charge of murdering Mrs Muriel Grimshaw, together with another six patients whose bodies were cremated after he admitted that he had been present at the death of four victims, Mrs Kathleen Wagstaff, Mrs Lizzie Adams, Mrs Norah Nuttall, and Mrs

Maria West. He claimed he was not present at the death of the other two victims, Mrs Pamela Hillier and Miss Maureen Ward, but the jury plainly disbelieved him.

Following his conviction, there were growing worries among Shipman patients' families who suspected their deceased family members had met the same fate as the pattern of Shipman's killings emerged. On 1 February 2000, the Secretary of State for Health announced that an independent private inquiry would take place to establish what changes to current systems should be made in order to safeguard patients in the future. However, there were objections from victims' families. Sections of the British media sought a Judicial Review in the High Court, which found in their favour and recommended that the Secretary of State for Health reconsider his decision that the Inquiry should not be held in public. As a consequence, in September 2000, the Secretary of State for Health announced that the inquiry would be held in public. Subsequently, Dame Janet Smith DBE, a High Court Judge, was appointed Chairman of the Shipman Inquiry and the independent public inquiry began in February 2001. The Inquiry's First Report was published on 19 July 2002 and its Final Report on 27 January 2005[26]. Dr Shipman, however, committed suicide on 13 January 2004, on the eve of his 58th birthday in his cell at the HMP Wakefield, West Yorkshire[27].

Three reports, published prior to Shipman's suicide, revealed overwhelming evidence of his crimes. The Inquiry's First Report (2002) concluded that Shipman killed 215 people, although another investigation by Professor Richard Baker of University of Leicester, suggested the real minimum number of Shipman victims was 236[28]. The Final Report (2005), however, confirmed the number of victims was 218. Smith also concluded that she suspected that Shipman might have been involved in the deaths of 62 other

[26] All together, there were 6 reports published under the Shipman Inquiry, namely 1) Death Disguised – published 19 July 2002, 2) The Police Investigation of March 1998 – published 14 July 2003, 3) Death Certification and the Investigation of Deaths by Coroners – published 14 July 2003, 4) The Regulation of Controlled Drugs in the Community – published 15 July 2004, 5) Safeguarding Patients: Lessons from the Past – Proposals for the Future, and 6) Shipman: The Final Report. Further information is available at http://www.the-shipman-inquiry.org.uk/reports.asp

[27] The victims' families felt 'cheated' as his suicide meant that they would never have the satisfaction of Shipman's confession, and answers as to why he had committed his crimes.

[28] Professor Richard Baker is Director of Clinical Governance Research and Development Unit, University of Leicester. He carried out the original clinical audit of Shipman's practice in Todmorden and Hyde, which was commissioned by the Chief Medical Officer and published in January 2001. His report was the main evidence at the Shipman Inquiry.

patients, but she did not have sufficient evidence to reach a final decision on them[29]. The first victim of Shipman's 23-year murder spree was Mrs Eva Lyons, who was killed in March 1975, when Shipman was practising in Todmorden, and the last victim was Mrs Kathleen Grundy, who died in June 1998.

The report states that Shipman killed his victims by administering lethal opiate doses, most frequently diamorphine[30]. It also noted that Shipman was able to obtain very large quantities of controlled drugs illegally and without complying with any of the statutory requirements for record keeping[31]. In the conclusion of the First Report, Smith stated that it is deeply disturbing that Shipman's killing of his patients did not arouse suspicion for so many years because the record keeping systems which should have safeguarded his patients against his misconduct, or at least detected misconduct when it occurred, failed to operate satisfactorily[32]. She further stated his crimes were discovered by accident. If it had not been Shipman's grossly incompetent forgery of Mrs Grundy's will, it is by no means clear that his crimes would ever have been detected.

The inquiry found fundamental weaknesses in the existing systems that enabled Shipman to kill and not be discovered for many years and that enabled Shipman to amass large quantities of diamorphine, notwithstanding regulations designed to prevent such stockpiling (Esmail[33], 2005). Shipman was also able to certify a cause of death of patients whom he had killed and so to avoid reporting the deaths to the coroner. There was no effective check on the information that he recorded on cremation certificates. Apparently, Shipman managed to escape attention through the confidence he established with patients and their families and the respect he earned from professional colleagues, which eventually charmed them mistakenly into placing their trust in him. This was compounded by the absence of the system for monitoring the number of death certificates signed by a given doctor, so no one noticed the large number signed by Shipman.

---

[29] This, perhaps, makes Shipman the most prolific serial killer in the history of the United Kingdom – and probably the world.
[30] *The Shipman Inquiry. (2002). First Report: Volume 1: Death Disguised*, p 2.
[31] *Ibid*. p 107.
[32] *Ibid*. p 200.
[33] Aneez Esmail was a medical advisor of the Shipman Inquiry chairman, Dame Janet Smith. He is professor of general practice in the Division of Primary Care, University of Manchester, United Kingdom.

More horrifying evidence was discovered when audit trails of computerised medical records showed that Shipman altered and falsified his patient records. There were false backdated entries on most of his patient records, even after their death, to support diagnosis of his victims and to be consistent with his claimed cause of death. Apart from computerised medical records, an examination of his paper records also revealed poor quality recording and care. Records were often incomplete. This was to facilitate his altering of victims' records after their death. For example, information about key clinical indicators such as blood pressure level is more often recorded than the information given by, or given to, the patient. In one case, the handwritten summary card of Mrs Ivy Lomas, who died on 29 May 1997, states the last entry, dated 1991, said 'IHD', which means ishaemic heart disease. However, the computerised records contained no reference to heart disease of any kind and Mrs Lomas was not receiving any medication for a cardiac condition. Examination concluded that the summary card was false and had been so entered in order to lend plausibility to Mrs Lomas' death supposedly from a heart attack[34].

In its Fifth Report, the Shipman Inquiry (2004) criticised the General Medical Council[35] (GMC) for 'looking after its own' and doing too little to protect patients, despite their claim of making wholesale changes[36]. The GMC has a reputation of being too lenient on medical practitioners, for example, the infamous Dr John Bodkin Adams who was charged with killing two patients. At his trial he admitted to 'easing the passing' of some of the old patients, possibly up to 400, who died under his care. Despite evidence shown that Bodkin Adams was mentioned in 132 of the wills of his patients, he was found not guilty on 15 April 1957 (Kinnell, 2000). Under the theme 'Protect Patients – Guide Doctors', the Shipman Inquiry made over one hundred recommendations that require a radical shake-up in the GMC structure. Among its main recommendations are:

- Change GMC structure to remove medical majority

[34] See no. 30, p 266.
[35] The General Medical Council (GMC) was established under the Medical Act of 1858, which gives it powers to protect, promote and maintain the health and safety of the public. Further information available at: http://www.gmc-uk.org/about/legislation/index.asp.
[36] Shipman Report Demands GMC Reform, *BBC News*, 9 December 2004. http://news.bbc.co.uk/1/low/health/4081425.stm (22 July 2006).

- The GMC no longer have sole responsibility for assessing doctors' fitness to practise
- The GMC to be directly accountable to the Parliament
- Improvements to the way doctors' performance is assessed
- A central NHS database containing information on all doctors
- Systems to be in place to allow staff to raise concerns

Mrs Smith admits that she cannot guarantee that even if all the recommendations are implemented it will be impossible for a doctor who is determined to kill a patient to do so without detection, but she believes that the deterrent effect will be considerable, and the chances of a doctor such as Shipman escaping detection will be very much reduced.

3.3 Discussion on Various Themes Related to the Cases

The cases of poor governance discussed in the previous section raise various issues for discussion. Good governance relies on efficient administration and societal values, which in turn, spurs transparency. These cases of poor record keeping reveal the absence of critical elements that underpin accountability and good governance. Three elements have been identified as the main contributing factors in these cases, namely:

3.3.1 Trust

Trust is an ethical value, which together with competencies contribute to the smooth operation and success of an organisation. Trust has positive effects on performance. The existence of procedures and guidelines will be less meaningful in the absence of trust and competencies because, as Fukuyama (1995) suggests, the absence of trust leads to economic backwardness or underdevelopment, and a nation's ability to compete is conditioned by the level of trust inherent in a society. The chronology of the Heiner Affair reveals a series of apparent acts of breach of trust by the government of Queensland and its officials. The House of Representatives Standing Committee on Legal and Constitutional Affairs (2004) concluded that the Goss Cabinet and the ALP's transition-into-government team were fully aware of why the Heiner Inquiry was established and the type of evidence it was gathering, and to suggest otherwise was not credible. With such a state of knowledge, it was never legitimately open to the Queensland Government to destroy such important evidence as it may have revealed

inappropriate and/or criminal behaviour against children in care as was later established, after a decade of cover-up, to be true.

Hurley (1999a) asserts that the destruction of the Heiner Inquiry evidence was done by a new and inexperienced government that did not know how to handle properly aborted inquiries or the orderly destruction of official records. Hurley further suggests that if destruction is to take place, then it has to be done systematically without leaving traces of the action. Twenty years earlier, Clanchy (1979) commented that monks, who were traditional experts in writing, were also the greatest forgers in the twelfth and thirteen century. Forgery requires high degree of skill to produce copies that are difficult for others to challenge its unauthenticity. Tracking evidence of the destruction of records would be much more difficult if the destruction was organised and executed by records management professionals. In an electronic environment, computing experts know better than records management professionals how this can be done, as extensive technical skills and knowledge is required to avoid deleted records being traced by investigators.

Without trust, especially among experts and senior officials, an organisation is more vulnerable to maladministration and abuse of power. In the case of Enron and WorldCom, it was breach of trust of senior management, together with the external auditor that eventually led to the collapse of these giant companies. Despite procedures and legislation, cases of breach of trust continue, as it is difficult to close all the loopholes. In the search for greater trust and efficiency, public administration in any truly democratic community must consistently demonstrate incorruptibility, fairness and accountability. The impact of breach of trust or abuse of power by government officials has greater consequences for the public sector, as government is mandated by the people. On the other hand, the impact of mismanagement, fraud and corruption in the private sector depends on the scale of the organisation itself. There were many fraud and mismanagement cases in the US at the time of the collapse of Enron and WorldCom, however, only these cases attracted attention across the world. Arguably, this was largely because of the impact on the wider economy and society.

In the case of Enron, Sherron Watkins, the whistleblower, responded to a claim by defendants that Enron's accounting was simply creative by saying that accounting just

does not get that creative[37]. Rationally, accounting does not need to be creative and tricky. It should be straightforward as it provides financial facts. Manipulating financial figures to camouflage overvalued businesses is a clear evidence of fraud. Possibly the temptation of a luxury life-style stimulated Skilling, Lay and Fastow to aggressively interpret accounting rules and conventions, as Coffee (2006) points out that allowed the allocation of Enron's exercisable shares to its officers and directors[38]. There were no restrictions on subsequent re-sale of the stock, providing room for exploitation by irresponsible individuals. Enron's senior managers were estimated to have paid themselves more than $1 billion[39]. This was done through massive systemic deceptions that eventually contribute to the collapse of the business. This suggests that to be able to conduct such fraud over time, they must have been very familiar with the comprehensiveness of record keeping systems within Enron.

There must have been two sets of records – first the records of the exact account; second the records of the faked account. Enron's external auditors, Arthur Andersen, attempted to cover up any improprieties in its audit by shredding supporting documents, that is the actual account, after investigations of Enron by the SEC became public (Healy and Palepu, 2003). On 15 June 2002, Arthur Andersen was found guilty of obstructing justice that marked an ignominious ending for the firm that had operated since 1913 and grown into one of the world's most-trusted institutions, with offices in 84 countries (Stephens, 2002). This suggests the exact records were secretly kept and only known to those involved in the underground activities, whereas the faked accounts were made available to others. This enabled them to consciously commit deception by manipulating information, particularly financial figures, to camouflage their deceitful intentions.

---

[37] Profiles the Guilty Men and the Whistleblower: Conspiracy and Obsession, *The Guardian*, 26 May 2006, p31. Employees or individuals must be legally protected to ensure that they are not at risk of victimisation or dismissal for disclosing information of malpractice or corruptions. Legal protection for whistleblowing varies from country to country such as the Public Interest Disclosure Act 1998 in the UK. In the US, legal protections vary according to the subject matter of the whistleblowing, and sometimes in the state which the case arise. http://whistleblowerlaws.com/ (8 October 2009).

[38] Within 60 days from 15 February 2001, stock options covering 12,611,385 of Enron's shares became exercisable by its officers and directors, including 5,285,542 by Kenneth Lay, its then CEO, and 824,038 by Jeff Skilling, who soon became its CEO. (Coffee, 2006:24).

[39] See no. 18.

Ironically, Lay insisted that Enron had corporate social responsibility, which meant Enron needed to expand its businesses in order to benefit society by providing services and jobs opportunities to the public. However, this does not excuse Enron's betrayal of its shareholders and stakeholders by massive deception, which is morally unjustified. Sacred intentions simply do not permit cruel execution. Considerable research shows that situational factors are more relevant than personal dispositions in explaining individual's actions (Bansal and Kandola, 2003)[40]. People who act responsibly in one situation may act irresponsibly in another, because of the context in which their actions occur. Lay's act was clearly a breach of trust crime, deserving conviction.

Although the culprits have been found guilty, the Federal Government of the US responded to such previously unimaginable corporate failure by tightening regulation through the introduction of new SOX legislation. In its early implementation stage, many described the act as going too far, though they realise it was probably inevitable to avoid any Enron-like corporate failure in the future. Understandably, it was burdensome for organisations, particularly to ensure compliance with Section 302[41] and Section 404[42], which require effective documentation to ensure adequate evidence is available for audit requirements. Based on their experience as auditors to private companies, Wagner and Dittmar (2006) of Deloitte & Touche, assert that senior management complained about the time and cost in the initially stage when SOX came into effect, that required massive documentation of activities, updating operations manuals, revising personnel policies, and recording control processes. These complaints, however, gradually disappeared as companies discovered the many fringe benefits of having a control environment.

---

[40] Pratima Bansal is the Shurniak Professor of International Business at the Richard Ivey School of Business, the University of Western Ontario, Canada. Sonia Kandola is an MBA student at the school and a co-founder of Ivey Connects.

[41] Section 302 requires CEOs and CFOs personally to certify the accuracy of financial statements and disclosures in the periodic reports and that those statements fairly present in all material aspects the results of operations and financial condition of the company. Furthermore, the executives must certify that financial controls and procedures have been implemented and evaluated, and that any changes to the system of internal control since the previous quarter have been noted.

[42] This section calls for an annual evaluation of internal controls and procedures for financial reporting. Like Section 302, Section 404 requires CEOs and CFOs periodically to assess and vouch for their effectiveness. This section also obliges companies to include an internal-control report in their annual report.

Wagner and Dittmar (2006) further assert that organisations with strong governance provide discipline and structure; instill ethical values in employees and train them in the proper procedures; and exhibit behaviour at the board and executive levels that the rest of the organisation will want to emulate. In other words, it is a matter of the attitude and values of executives and directors and the degree to which they recognise the importance of method, transparency, and care in the creation and execution of their company's policies and procedures. According to Wagner and Dittmar, these are the components of 'control environment' that underpins internal control. Internal controls rely extensively on the consistency of documentation, which means records must be made available as evidence of commitment and for the needs of continuous assessment of compliance. Undoubtedly, an effective records management system certainly has an important role in ensuring the success of internal controls, by providing proper documentation and record keeping guidelines or procedures.

It is vital to retain trust as it is extremely difficult to restore it once lost. Trust among shareholders and stakeholders can only be retained when organisations can demonstrate compliance by being consistently transparent. Under the new legislation, CEOs and CFOs are personally responsible for attesting that adequate internal controls have taken place and accurate financial statement produced. Apart from CEOs and CFOs, audit committees and boards of directors can no longer take things as lightly as they used to, since SOX clearly demands them to be accountable for their organisation. Previously, the role of records managers and archivists was not significant in many organisations. However, the implementation of SOX has increased demands for records management professionals because of the increasing responsibility and risk to directors, CEOs and CFOs in running their businesses.

Records management professionals must take this opportunity to redeem their profession by regaining their meaningful contribution to organisations as it used to be in the UK public sector, as noted by Moss (2005), almost a hundred years ago, when records and their movements were accurately documented in a registry by registry clerks who were expected to act fiduciarily. Once the parameters for record keeping have been set, they are not negotiable and must be observed. No one can afford to run the risk of non-compliance with protocols who put them in place by audit and risk

management committees. Good record keeping goes beyond cost saving[43] (Wagner and Dittmar, 2006). Further discussion on how records managers can contribute significantly to the organisations is available in *Section 3.3.3 Authority of Records Managers and Archivists.*

Contrary to the claim by Wagner and Dittmar (2006), compliance with SOX is only affordable by large and medium companies. The chairman and chief executive of the American Stock Exchange, Neal Wolkoff (2006), argues that after four years of its implementation, SOX has unintentionally created an environment that discourages smaller, innovative companies from accessing US capital markets and impedes the ability of US exchanges to compete against foreign exchanges. Since SOX makes no distinction between a $50 billion large company and a $75 million small company, the consequence is a growing trend amongst entrepreneurial (small) companies deciding not to go public or listed companies opting to delist because of the high costs of complying with Section 404, which requires designing, documenting and auditing of financial controls.

Wolkoff (2006) further asserts that the excessive and costly SOX regulation was good medicine for corporate ills, but even good medicine prescribed without due care for side-effects can be toxic. He, therefore, suggests three recommendations to mitigate the unintended consequences of SOX while retaining the public benefits of high standards of investor protection. First, it clearly defines through a public company for accounting oversight board interpretation of specific standards, which could differ based on criteria such as revenues or market certification, for compliance with Section 404. Second, it relieves companies that receive clean Section 404 certifications from the cost of annual certification in favour of bi- or tri-annual certification. Third, it allows the smallest public companies to choose an exemption from Section 404 compliance and allow for disclosure to investors of such choice. These suggestions may enable small companies to prosper whilst ensuring compliance and good governance.

The circle of trust is very subjective and complicated as it may be seen differently by different people and from different perspectives. For example, in the case of Dr Kelly,

[43] RSA Security, PepsiCo and Yankee Candle are a $600 million purveyor of scented candles and other household items. Further information is available at: http://www.yankeecandle.com. (11 July 2006).

the Hutton Inquiry concluded that his meeting with Mr Gilligan was breaching the Civil Service code of procedure, despite suggestions that the meeting was not on Dr Kelly's personal initiative. Instead, he was instructed by someone in a higher political position whom they believed to be the government press secretary Alistair Campbell, to brief journalists about the controversial dossier. Mr Gilligan believed that Mr Campbell was the driving force behind the alteration of the controversial dossier (Hutton, 2004). The government was in a difficult position as there were massive public protests about the dossier following Mr Gilligan's broadcast. Unfortunately, Dr Kelly was made a scapegoat whilst the culprit remains unconvicted.

Dr Kelly's claim that there were no such WMDs in Iraq, as appeared in Mr Gilligan's broadcast, was considered to be unfounded by the Hutton Inquiry. It was subsequently proved to be true when, on 6 October 2004, a report of investigations by a US chief weapons inspector, Charles Duelfer, revealed that Saddam Hussein ended his nuclear program in 1991 following the Gulf War[44]. Eventually, the defiance of the Labour government ended on 6 July 2004, when Blair admitted that they were wrong and such WMD would never be found. Had Dr Kelly still been alive, he would have walked with his head high when the truth was eventually disclosed. The Hutton Inquiry concluded that it was the gravity of the consequences of the exposure that led to Dr Kelly's suicide. Indeed, it is always difficult for whistle-blowers to cope with the consequences of exposure as it is an act of an individual against an organisation. Further discussion on whistle-blowing includes the experience of the tobacco whistle-blower, Dr Jeffrey Wigand, is available in *Section 3.3.3 Authority of Records Managers and Archivists.*

Generally, the medical profession enjoys great trust from society by giving them immense power. The Shipman case was clearly a betrayal of trust, as Smith noted that as a GP, Shipman was trusted implicitly by his patients and their families. Smith further insists Shipman, however, betrayed their trust in a way and to an extent that is unparalleled in history[45]. His 'non-violent' killing seems almost more incredible than violent deaths of which we have heard, for example in Baghdad. The existing procedures for death registration and cremation certification should have been made possible for the detection of Shipman's crimes, if there had been effective monitoring

[44] Final Report: Iraq had no WMDs, *USA Today*. 6 October 2004.
[45] See no. 30, p 201.

and controls. Shipman managed to override the procedures by developing a reputation as a very good doctor and for being caring and hardworking, which earned him the complete trust and confidence of his patients, but also the respect of his professional colleagues.

The Inquiry's Final Report (2005) states that because of this trust, confidence and respect, Shipman was able to kill patients and avoid detection. His false explanations for events were accepted without questions[46]. Esmail (2005) states that considering the role of trust and accountability in doctor-patient relationships, regulators and professional organisations must aim to equalise the power of imbalance. He further suggests that the best safeguards against another Shipman include encouraging a more questioning attitude towards doctors and implementing better systems for monitoring their work, especially their care of most vulnerable patients. This means that greater regulation of the medical profession is required. This suggestion is consistent with O'Neill's (2002c) recommendation that to restore trust, deception and lies must be reduced rather than secrecy, as some sorts of secrecy indeed support deception.

Tighter regulations and consistent monitoring and controls should be able to detect and react against such wrong doings in order to protect patients and also to redeem trust in patients. There were two issues involved. First, is about thinking the unthinkable – that is thinking of the unimaginable mass murdering doctor. It was certainly hard to believe that a person of Shipman personality could commit mass killings. Second, is the issue of self versus external regulation. The Shipman's Inquiry made a sensible recommendation that GMC, a self-regulated organisation, should remove the medical majority in the council to enable non-biased decision-making. The GMC was criticised for lenient actions against medical professional wrong doers and this was admitted in a press statement in response to the Shipman Inquiry recommendations. Its existing fitness to practice procedures were not adequate[47]. It is hard to see how the present

[46] The Inquiry also discovered that Shipman ingratiated himself with senior staff, particularly senior nurses, including with Mrs Ghislaine Brant, manager of the pharmacy next door to his surgery in Market Street, Hyde. This was deliberately done to have Mrs Brant's complete confidence in him. Then she would supply him with ampoules of diamorphine in circumstances where she ought not to have done, at least without asking him to justify his requests. Her admiration for and confidence in him deprived her of her professional objectivity. The Shipman Inquiry: Final Report (2005), p 42.

[47] http://www.gmcpressoffice.org.uk/apps/news/latest/detail.php?key=144 (22 July 2006).

GMC can function neutrally for the benefit of the patients, whilst maintaining its medical majority. It is imperative to have an independent council in order to constantly safeguard patients. May be the GMC can adopt the concept of the Financial Services Authority, an independent non-governmental body, which is an open and transparent organisation and provides full information for firms, consumers and others about its objectives, plans, policies and rules[48]. However, monitoring body such as the Financial Services Authority must be dynamic and conscious of changes in order to remain relevant to their purpose.

3.3.2 Transparency

Transparency was the missing key element that contributed to the collapse of Enron. A massive systemic deception could not last for that long had a check and balance mechanism functioned in the way it was supposed to be. Enron was in an alarming situation when asked by the SEC to restate its financial status for the period of 1997 to 2000 by consolidating its accounts. This suggests that Enron's check and balance agents, its auditors and audit committee, were implicated by closing their eyes on the way in which records were manipulated. Arthur Andersen, the Enron's auditors for over 16 years, did not act responsibly, instead compromised its reputation by endorsing Enron's financial reports that may have been technically legal but taken together were fraudulent. Arguably, it was a matter of conflict of interest as Arthur Andersen earned $25 million in revenues for auditing Enron and $27 million in revenues for consulting (Bansal and Kandola, 2003).

The audit fees contributed roughly twenty seven percent of the audit fees of public clients for Arthur Andersen's Houston office (Healy and Palepu, 2003). Probably, it is not too harsh to implicate Enron's audit committee of failure to detect any irregularities in the financial statements. Apart from external auditors, the audit committee was also a check-and-balance agent, responsible for endorsing Enron's financial statements. Audit committees usually meet just a few times a year, and their members often have only modest backgrounds in accounting and finance, but this was not the case with Enron[49]. As non-executive directors, they rely extensively on information from

[48] http://www.fsa.gov.uk/Pages/About/Who/index.shtml (22 July 2006)
[49] Enron's audit committee had more expertise than many. It included Dr Robert Jaedicke of Stanford University, a widely respected accounting professor and former dean of Stanford Business School; John Mandelsohn, president of the University of Texas' M.D. Andersen Cancer

management and tend to believe auditors. If the management is fraudulent or the auditors fail, the audit committee probably will not be able to detect the problem fast enough (Healy and Palepu, 2003). It is hard to accept that the audit committee was not aware of the fraud in Enron which occurred for almost five years. They compromised their integrity by blindly accepting audit statements prepared by Arthur Andersen, at the time when it was one of the most trusted public accounting firm in the world.

Traditionally, the role of an audit committee was to oversee, monitor, and advise company management and external auditors in conducting audits and preparing financial statements, subject to the ultimate authority of the board of directors. However, in the wake of high profile corporate scandals such as Enron and WorldCom, their role has changed. With the new legislation being implemented, Brodsky *et al.* (2003) recommend that audit committees need to ensure the accountability of the management and internal and external auditors. It also ascertained that all those involved in financial reporting and internal control processes understand their roles and gain input from the internal auditors, external auditors, and outside experts when needed; and safeguard the overall objectivity of the financial reporting and internal control processes[50].

Center; Paolo Pereira, former president and chief executive officer of the State Bank of Rio de Janeiro in Brazil; John Wakeham, former U.K. Secretary of State for Energy; Ronnie Chan, a Hong Kong businessman; Wendy Gramm, former chair of U.S. Commodity Futures Trading Commission. However, the audit committee seemed to share the common pattern of a few short meetings that covered huge amounts of ground. Healy and Palepu (2003) states a meeting on 12 February 2001, lasted only 85 minutes, yet covered a number of important issues, including: a) a report by Arthur Andersen reviewing Enron's compliance with generally accepted accounting standards and internal controls; b) a report on adequacy of resources and related party transactions; c) a report on disclosures relating to litigation risks and contingencies; d) a report on the 2000 financial statements, which noted new disclosures on broadband operations and provided updates on the wholesale business and credit risks; e) a review of the Audit and Compliance Committee Charter Report; f) discussion of a revision in the Audit and Compliance Committee Charter; g) a report on executive and director use of company aircraft; h) a review of the 2001 Internal Control Audit Plan, which included an overview of key business trends, an assessment of key business for 2001 compared to the period 1998 to 2000. This suggests that the audit committee relied extensively on information provided by the management, external auditors and internal auditors and, without doubt endorsed all the strategic issues. As a consequence, Enron eventually demise can be attributed in part to an ineffective audit committee as well as corrupt practices by the management. For further information read Healy and Palepu, (2003).

[50] Cited in the American Institute of Certified Public Accountants. Available at: http://www.aicpa.org/audcommctr/guidance_resources/improve_function/build_foundation_governance/26.htm (6 July 2007).

As non-executive directors, it is much easier for audit committee members to act professionally, without bias, in ensuring the accountability and transparency of the organisation. Reflecting the importance of the audit committee as agents of accountability and transparency, they needed to feed adequate information to investors regarding a firm's economic liability and any category of risks to which it may be exposed. Healy and Palepu (2003) propose that the audit committee should be renamed the 'transparency committee'. Their suggestion, however, has not been widely accepted because there is a growing trend of renaming the audit committee as audit and risk management committee, which more appropriately reflects their functions.

In the case of mismanagement and corruption at the MAS, there was no key documentation encountered during an audit process, preventing the audit team from fully evaluating the soundness of recommendations made by consultants, and also impeding the police investigation. This suggests that Mr Firman deliberately did not document the outsourcing processes in order to avoid discovery of his wrong doings. He also deliberately hid the development and implementation of the new computerised system from the Government by not integrating it into the planned State-wide emergency communications systems. Eventually Mr Firman was trapped by his own actions.

Failure to integrate his malfunctioning emergency communications system spurred concerns in Government, particularly MAS which failed to achieve the projected savings of $20 million. Understandably, Mr Firman thought that integrating his malfunctioning system would trigger investigation that would eventually disclose his wrong doings. However, failure to integrate the system would also produce the same consequences, thus leaving him and other actors with no options. Although the investigation was delayed by the absence of key documents as witnesses were required to give evidence under oath, the truth was eventually discovered.

Despite the exposure of the memo in the media, the denial by the state government of Victoria, (and in particular by the former health minister, Marie Tehan) did little except disclose the true facts of the case. Her claim that she did not see the memo was simply unacceptable considering her specific responsibility and the alarming situation in MAS.

Even, if she was right, it was an embarrassment to the government, as minister, she failed to perform her job satisfactorily. Inability to react promptly, allowed corruption and mismanagement to continue. If the government had reacted earlier, such immoral activity could have been halted sooner, and the UFU and more importantly the public would not have faced such fatal consequences.

Arguably, the health minister's decision not to be transparent was to preserve the public trust as she personally (or the government collectively), may believe that admitting her mistake could damage the reputation of the government. Transparency can increase the level of trust, but by the same token can also decrease the level of trust if it discloses corruption or mismanagement of the organisation[51]. Transparency is certainly not a problem in the absence of deception or mismanagement. In the context of the MAS, the Victorian government faced a crisis of trust as they were forced to admit that they were aware of the corruption. Such disclosure may lead to worse consequences jeopardising its potential to retain authority. Mr Firman believed that his maladministration would not be easily detected as it was not transparent. Such deception can never be sustained, as no matter how long it takes to investigate, eventually adequate contextual information will perfectly locate every piece of a jigsaw in its place. The impact of Mr Firman's corrupt practices was not limited to his department only, but also implicated the government as they denied being aware of such malpractice.

Medical records are confidential, just like criminal records. All such records containing personal information in Europe are bound by the Data Protection Act (1998), making it hard to demonstrate transparency in the NHS, except when there is legal justification for access to the records for such purpose. Physicians are required to swear the Hippocratic Oath[52], an oath that binds them to observe high ethical standards in performing their jobs. This makes physicians less likely to be suspected of wrong doing, particularly a person like Shipman, who enjoys a good reputation and is respected by their professional colleagues. No one suspected him of killing his patients,

[51] A comprehensive discussion on transparency and trust available in *Section 2.8.2 Trust and Transparency*.

[52] *'Whenever I go into a house, I will go to help the sick and never with the intention of doing harm or injury. If, therefore, I observe this Oath and do not violate it, may I prosper both in my life and in my profession, earning good repute among all men for my time. If I transgress and forswear this Oath, may my lot be otherwise.'* Segen (2006, p301).

hence it was not imperative to scrutinise his patients records as there were no calls for transparency.

Other than authorised officials, legal permission is required to view criminal records, which in the process, sometimes may lead to other consequences. Moss (2005) argues that a strict interpretation of the Data Protection Act by individual officials contributed to the killing of two little girls (Holly Wells and Jessica Chapman) at Soham in Cambridgeshire, by Ian Huntley, a school caretaker in August 2004[53]. In conjunction with his conviction for the murder of the two little girls, it was revealed that Huntley had been accused but not convicted of a string of sex crimes involving young children, before his appointment as a school caretaker. It is worthwhile noting that it was the murders that triggered the whole sequence of events, not the imperative to improve poor record keeping regimes in police departments. Because Huntley was never convicted, negligent record keeping was not considered that important.

The Bichard Inquiry[54] (2004) discovered that no record of Huntley's past had been retained by Humberside Police, even though he was charged in one rape case. The report further stated that the Humberside Police lacked effective guidance and training, and there was ignorance and confusion about the creation, reviewing and deleting of records. It is just a matter of time, though the probability is tiny, for all entities involved to collectively malfunction, as in the Huntley's case that involved Humberside Police, Cambridgeshire Police, education authorities, and North-East Lincolnshire Social Services. As a result, Huntley managed to slip through the net of the vetting system enabling him to reach his victims. Had any of these parties functioned responsibly, then Huntley would never have been able to reach his victims. Although this case has eroded public confidence, we cannot help relying on the police to protect us, since they have a monopoly of law enforcement – even if we are suspicious of them (O'Neill, 2002c).

---

[53] The Bichard Inquiry found that David Westwood, chief constable of Humberside, had been wrong to blame the Data Protection Act for his force's decision to delete police information on the girls' killer Ian Huntley, but stopped short of calling for the legislation to be reviewed.

[54] The Bichard Inquiry was established to examine the effectiveness of Humberside and Cambridgeshire police forces' relevant intelligence-based record keeping, vetting practices and information sharing with other agencies. Further information available at: http://www.bichardinquiry.org.uk/report/.

In both cases, public organisations were called upon to demonstrate transparency, which eventually disclosed their day-to-day modes of operation. In the Shipman case, there were adequate records available, though some were dubious, but it was mainly due to the absence of proper monitoring and controls that enabled the crimes to continue for over 23 years. Whereas, in the Huntley case, the scenario was worse as it revealed poor record keeping in the police departments, which are supposed to be responsible for the public safety. For many reasons forced transparency through public inquiries, which are usually formed to investigate high profile cases. This could lead to deterioration in public confidence and trust in the institutions involved as they cannot obstruct the investigation. Hence, the consequence is beyond their control. Further discussion of transparency is to be found in *Section 2.8.2 Trust and Transparency*.

3.3.3 Authority of Records Managers and Archivists

Record keeping used to be essential in the administration of government offices in the British Civil Service in the nineteen century. In fact, in many developed countries that was the situation prior to the introduction of computers, with their impressive advantage that information can be managed and retrieved much more cheaply, securely and effectively (Moss, 2005). Traditionally, the effectiveness of record keeping was underpinned by registries, as Moss (2005) describes that apart from providing an accurate journal of transactions and thereby precedent, the registry also protected the impartiality of Civil Servants as the records were managed by registry clerks who were expected to act fiduciarily. Moss further describes that there were elaborate safeguards, by which documents and later files had to be signed in and out, papers could only be added to a file or docket by an authorised registry clerk, and all those who consulted a file or docket had to be initialled. Such arrangements, according to Moss, represented the classic distinction between the front and back office and the security it affords. The absence of such security could have a serious impact which, for example, led directly to the collapse of Barings, the London merchant bank in 1995.

The Butler Report disclosed weaknesses of record keeping practices in the government, whether deliberately or otherwise in the case of the WMD dossier, and public confidence has certainly receded. In order to restore public confidence in the machinery of the government, Moss (2005) advocates that authority for managing information must continue to reside with the Cabinet Secretary, the Head of the Civil

Service and other permanent secretaries and be much more explicitly exercised. Those officials, like chief executives in the private sector, must take responsibility for good record keeping and should lose their jobs if there is evidence of systemic failure, as had happened at the Prudential insurance company in 1995 (Moss, 2005).

The role and circumstances of records management professionals in the public sector is different from their colleagues in the private sector. For example, in the public sector in the UK, records managers and archivists, under the National Archives, have limited power and protection in performing their jobs. Moss (2005) reminds us of a critical role of the National Archives is to hold the records of courts of law as their fiduciary agents and not the agents of government. This is vital to ensure evidence of governance, either good or bad, is well kept for research by future generations. Meanwhile, in the private sector, archivists are called for different responsibilities according to the context in which they work (Duranti, 2005)[55] and cannot be held personally accountable for destroying records under instruction from their employers. It is not an individual responsibility but the responsibility of all employees. The board of directors is ultimately responsible for ensuring good governance (Moss, 2006b).

In relation to the investigation of the corruption in the Victoria Metropolitan Ambulance Service, the Auditor-General of Victoria, Baragwanath states that the various checks and balances in the public accountability process may be costly to administer. Some would argue that it would be a bureaucratic hindrance to the effective management of functions such as purchasing, but they are designed to protect a government's reputation and the interest of the public at large. Such a strong statement should awaken and motivate records managers and archivists to strengthen their role by ensuring the records are managed and kept according to rules and regulation. However, Hurley (1999a) argues in order to function without political interference, records managers and archivists must be authorised and protected by legislation.

Hurley further explains that in the Heiner case, there were three disposals of documents. The first was a destruction ordered by the Goss cabinet and approved by the State Archivist. In this case, Hurley (2005) argues that it raised questions

[55] Luciana Duranti, *Meeting the Challenge of Contemporary Records: Does It Require a Role Change for the Archivists?* http://www.archivists.org/governance/presidential/duranti-2.asp#endnotes (8 August 2006).

surrounding the second level of record keeping accountability that is the accountability of the record keeper in the role and function as an agent of accountability[56]. The second and third (one involving shredding and the other involving the hand over of documents to a union) did not involve the cabinet or the archivist. Hurley (1999a) also advocates that abuse of documents and abuse of process which was the real corruption and the root cause of child abuse because they permitted and nurtured the cover up that allowed systemic child abuse to occur. Accountable process involving proper regulation of documentation should prevent it. The case was so difficult to resolve because it was not the work of an individual, but of a system, which made it impossible to confine an investigation of abuse to the corruption of the individuals who abused the children.

This is similar to the case of Enron. The whole system in Enron was abused by senior management to enable their corrupt activities, which were partly assisted by its check and balance agent, Arthur Andersen, that compromised its reputation whilst ensuring its revenues from Enron. Organisations should learn from the catastrophic consequences resulting from Andersen's failure to follow its own record retention policies, particularly its decision to initiate the shredding of documents on the eve of a government investigation. Although their responsibilities are not much different, records managers and archivists in the private sector have less authority than their colleagues in the public sector. Nonetheless, the authority in the public sector is inadequate to enable them to function as agents of accountability.

Despite limited authority, records managers and archivists must never put themselves in legal jeopardy in exchange for a pay-check from their employers, particularly in the private sector. Stephens (2002) suggests that if employees have questions concerning the legality of any records disposal action, they should contact their legal department. If they are still not satisfied, they should contact regulatory authorities. If employees are forced to choose between their company and the law, they should comply with the law and cooperate with authorities, even if it means resigning their position. This, however,

[56] Hurley discusses extensively about the role of record keepers as agents of accountability, mainly as a consequence of the Heiner affair. He raised concerns about the need for legal protection to enable record keepers to function un-biasedly, without political intervention. The absence of such legal protection may lead to selective archival collection, which does not provide an accurate record for future generation to judge and research.

is far easier said than done as, for example, former vice president for research and development for Brown & Williamson and the tobacco whistle-blower, Dr Jeffrey Wigand, described the consequences of telling the truth, as:

> *You feel a very deep, inner conflict between your loyalties, your loyalty to your family, and supporting and protecting your family, the supposedly loyalty that you're supposed to have through the corporation that's actually paying to you support your family.*[57]

This proves that protection by law is imperative. An employee would be better protected and feel more certain about the consequences that he or she might face for whistle blowing, though sometimes it goes beyond expectation.

In the wake of the emergence of information and knowledge management, Hurley (2004) points out that records management cannot stand by itself, instead must necessarily be part of a team approach which blends a variety of skills, disciplines and methods involving other departments within the organisation. Currall and Moss (2006) share the same view that it is no longer the question of 'how' but 'why', hence a team approach could help records managers and archivists understand the needs of the organisations. Ability to understand 'why' enables records managers and archivists to be more adaptive to various organisational cultures, which in turn, enables them to be a significant team player for the success of the organisation. Otherwise, the records management profession will eventually diminish as a consequence of the dominance of information and knowledge management, particularly in the private sector, as Hurley (2004) rightly points out. He hopes that records management professionals will not lose their separate identity by merging into the pool of Information/Knowledge Management. An integrated approach is vital as good record keeping does not guarantee the integrity of an organisation, if there is no effective monitoring and controls.

The Shipman case provides evidence that procedures alone cannot stand by themselves as Shipman managed to override them. The Inquiry revealed that all the cremated victims that relied on MCCDs completed by Shipman, showed that cremation procedure was simply ignored. The procedure requires, before a cremation can be

[57] *Inside the Mind of a Whistle-blower: Tobacco Whistle-blower Jeffrey Wigand on the Risks and Rewards of Telling the Truth*. http://www.msnbc.msn.com/id/8077025 (7 August 2006).

authorised, a second doctor must confirm the cause of death and the cremation documentation must be checked by a third doctor employed at the crematorium. These procedures are intended to safeguard the public against concealment of homicide. Yet, Shipman was able to kill 218 people without detection for over 23 years. It was not about poor record keeping but all about poor monitoring, controls and audit. Legislation and regulations are meaningless in the absence of effective monitoring and controls, even if adequate records are available to detect a wrong doing. The benefit of good record keeping, apart from effective operation, will only emerge when there are consistent and effective monitoring and controls in place. Otherwise, record keeping is regarded as a less important activity, dealing with non-current information and conducted by a less important profession.

Evidence of Shipman's crimes was available since he killed his first victim in 1975. He had them recorded by himself in all his patients' records, though some were falsified. They only surfaced when Professor Baker examined Shipman's patients' medical records in conjunction with the cremation Forms B and the pattern of killings emerged[58]. Though it is too late, it is better than never as the benefit of good record keeping eventually surfaced after almost thirty years since the death of his first victim in 1975 and four years after that of his last in 1998. His crimes, however, could have been detected much earlier by regular monitoring and auditing. Neither records management nor well-designed procedures or frequent monitoring, controls and audit can individually significantly contribute to an effective operation. Hurley (2005) advocates that effective record keeping can assist those in power perform their tasks by preserving memory, but if the watchdogs keep silence, or are terrified to open their mouth, memory alone cannot achieve results. The most that can be fairly claimed, therefore, is that effective record keeping which is a necessary, but not a sufficient, condition for accountability. In today's massive regulation age, an integrated approach inclusive of risk and records management, as well as independent audit, is the way forward to add value to the organisation.

[58] Professor Baker notes that the cremation certificates showed that Shipman reported having been present alone or with others at half of the deaths in respect of which he completed Forms B. Those patients appeared to have died more quickly than the patients of other doctors, including the patients of doctors working on the medical wards at the same time as Shipman. It was also noted that high proportion of deaths certified by him occurred during the evening.

In the age of ICT where organisations are digitally networked, spending money and other resources on specific individual department's needs, particularly in the public sector, is less meaningful as the benefit is only limited to the individual department. Integrating various information systems cannot be done as an instant task or in response to urgent needs, but must be carefully designed to ensure effective communication between different hardware and software platforms, particularly when it involves data integration from different systems. Arguably, the underlying element of the availability of records, regardless of form, is good record keeping practice that ensures accuracy and consistency of metadata and content of records, which in turn facilitates integration. Taxpayers should not be continuously burdened with the cost of public or private inquiries, which are the spin-offs from ineffective government mechanisms. The Shipman Inquiry alone cost nearly £21 million ($40.4 million) (Esmail, 2005) over four years of examining approximately 2,500 witness statements and approximately 270,000 pages of evidence scanned into the Inquiry database[59].

Perhaps, Shipman's killings were a rare case but its unimaginable scale simply reduces public confidence and trust in GPs. Tighter regulations and consistent monitoring and controls not only detect and prevent crimes occurring, but also ensure that taxpayers' money is not spent on investigating crimes that can be prevented. Undeniably, public inquiries produce recommendations for improvement, but we should not forget that improvements can also be initiated without the need to react to such failures. However, it is not easy to promote good record keeping in the GMC, with its reputation and past history, that is consistent with what Sir George Matthewson states 'We don't have a problem with regulators telling us that we should tie our shoe laces, but we don't want them to tell us how to do it' (Currall and Moss, 2006). Such an arrogant statement certainly makes life more difficult for records managers, particularly in an environment where they are surrounded by highly professional employees such as doctors, lawyers, engineers and accountants. Indeed, the political, organisational, social and administrative environments in which record keepers operate mean that their conditions of employment will determine their actions.

[59] Information available at: http://www.the-shipman-inquiry.org.uk/qanda.asp#whensetup. The Bichard Inquiry costs under £2 million, http://www.bichardinquiry.org.uk/faq/.

In such situation, employers should not forget about compliance with regulations that can only be supported by the availability of records, which falls within the responsibility of records managers. The task of a records manager will be slightly relieved by an audit committee through internal controls and external audit, though it does not transfer the responsibility of managing records. Certainly, an independent audit is an ideal solution in ensuring good faith in organisations, as Power (1994) advocates audit is a risk reduction practice which inhibits the deviant actions of agents, and audits are needed when accountability can no longer be sustained by informal relations of trust alone, but must be formalised, made visible and subject to independent validation. This is not to say that audit is meant not to deter wrong doers, but equally to ensure businesses are conducted in compliance with regulations. Further discussion of audit is available in *Section 2.8.3 Audit and Internal Control*.

The Bichard Inquiry (2004) reveals the Soham killings occurred partly as a consequence of the lack of clear and understandable national standards and guidance on the subject of records creation, retention, review and information sharing which most likely contributed to the failure in record keeping in the Humberside Police. This subsequently hampered the tracking of information about Huntley by the Cambridgeshire Police had they properly vetted Huntley, though it emerged that they did not ask for the information from the Humberside police. It was also discovered that the North-East Lincolnshire Social Services failed to update Huntley's criminal records and even failed to pass on to police a letter from a local deputy head teacher concerning Huntley. Hence, the Inquiry recommended that a new code of practice on information management should be produced covering record creation, review, retention, deletion and information sharing.

Bichard insisted that such a code needs to be clear, concise and practical and should supersede existing guidance. Interestingly, whilst insisting on the importance of having good record keeping in police departments, the Inquiry urged the Home Office to introduce a national IT system, for England and Wales (since Scotland already has one) to support police intelligence. This is much-awaited opportunity for the National Archives, the sole government records management authority, to promote and implement a sustainable record keeping system, though it is not mentioned specifically as responsible for implementing this recommendation. Indeed, it is not limited to police

departments only, but all public organisations as they are accountable to the public. It is the question of how records management can be integrated with information systems, which are dominated by ICT professionals. This is certainly a good opportunity for records managers in the public sector to collaborate with ICT professionals in order to develop an information system with adequate record keeping features.

From all the cases discussed - the Heiner affair, corruption in the Metropolitan Ambulance Service, the collapse of Enron, the Hutton Inquiry and the Butler Report, the crimes of Harold Shipman and Ian Huntley – it can be concluded that wherever corruption and a failure of accountability are found, an associated failure in record keeping practices is, almost invariably, identified as part of the cause. Inevitably, the government is accountable, either directly when it involves public organisations, or indirectly when it involves private organisation through its regulatory machineries. Out of the seven cases discussed, six involving public organisations, and only one involving a private organisation, Enron. Such failure of record keeping may lead to organisational risks and societal risks as McKemmish and Acland (1999) suggest, namely:

Organisation risks

- Lack of evidence that an organisation did something under contract or according to regulation
- Inability to find mission critical information
- Loss of proof of ownership, rights, obligations
- Lack of documentation of who knew what when
- Inability to locate its proper context information that may be incriminating in one context and innocent in another
- Inability to demonstrate that policies and procedures were in place and consistently followed

Societal risks

- Impairment of functioning of society and its institutions
- Loss of evidence of the rights of people as citizens and clients
- Inability of societal watchdogs to call to account governments, corporations and individuals
- Loss of collective, corporate and personal identity

- Loss of individual, corporate and collective memory
- Inability to authenticate and source mission critical information

These suggestions of risks were drawn up as a result of Australian experience of corruption in the governments across the nation in the late 1980s and 1990s. In fact, in Australia, and anywhere else in the world, regulations will always be tightened in response to any catastrophic event, either in the public or private sector. It is reactive rather than proactive as it is extremely difficult to perceive future circumstances, hence imposing unnecessary legislation is not welcome by many. But one thing that is for sure is an effective record keeping system which ensures compliance with any regulations across time provided it is based on a comprehensive feasibility study.

In a nutshell, the authority of records management will gradually be established through a strategic approach that is in line with organisational strategic objectives. The way forward is if records management can take risk management onto a level where it is more concerned with operational and strategic success, helping their organisation to succeed then they could be riding high (Currall and Moss, 2006). However, this can only be achieved if records managers and archivist are willing to engage senior management, ICT professionals and departmental business managers rather than waiting for them, which is unlikely, to make an approach.

CHAPTER 4

CASE STUDIES

4.0 CASE STUDIES

4.1 Introduction

The government is the backbone of the stability of a nation. Accountability and transparency is now an international agenda. The public, nowadays, are more concerned about the government's governance, mainly because of the escalating cost of living, particularly in form of taxes paid to the government. To retain public trust, the government must be able to demonstrate accountability and transparency whilst achieving value for money in public services. Accountability and transparency can only be demonstrated when organisations function according to regulations and compliance requirements, and supported by adequate records that are reliable, timely and accessible. This depends on an effective record keeping system that ensures records are systematically created, used, stored, maintained and retrieved throughout the life cycle.

In the interest of the general citizen in a democratic country, the public sector should possess as good if not better record keeping systems than the private sector, the government is accountable to the people of the country, directly through its public organisations and indirectly through the regulations imposed on private organisations. However, records management is rarely considered as important in underpinning efficient services. A failure, particularly a major one, in any public organisation will have a direct and immediate impact on the reputation of the government. As a consequence, public trust will diminish even though subsequent investigations may identify and punish the culprit. This, in turn, requires an effective record keeping system to facilitate investigations by providing adequate and reliable evidence.

It should be remembered that reputation lags behind performance (Mehr and Hedges, 1974). Undeniably, in every case of corruption or mismanagement, poor record keeping is one of many reasons identified as the contributing factor to the failure. Generally, private organisations, especially those involved in financial and insurance businesses, are thought to have reliable and efficient record keeping systems largely because they are heavily regulated. Public organisations, on the other hand, are on the whole more lightly regulated and may as result possess less efficient record keeping systems. These presumptions, however, may not necessarily be true as organisational

culture differs from one organisation to another and one country to another. Cases such as the death of Dr David Kelly and the decision by the UK Labour government to go into war in Iraq, serial murders by the physician Harold Shipman, the killings of two young girls in Soham by Ian Huntley, the collapse of American corporate giants, Enron and WorldCom and, cases of rampant corruption in Australian governments in the 1980's and early 1990's – all disclosed the failure or manipulation of record keeping in both public and private organisations.

Research conducted in the Netherlands discovered that public organisations operate efficiently despite inadequate record keeping practice (Meijer, 2003). These findings may not be the same in other circumstances and context. Further empirical investigations are needed to confirm them. To this end, three case studies have been conducted involving three different institutions namely, Standard Life in Edinburgh – an international financial organisation in the private sector; the European Investment Bank (EIB) in Luxembourg – a European Union (EU) public institution with legal immunity; and National Health Service Greater Glasgow and Clyde (NHSGGC) – a fully public organisation. The objective in selecting these organisations was to identify best practices that can be adopted elsewhere and highlight any shortcomings.

Standard Life, a newly listed public company, operates under a strong legal and compliance regimes whilst satisfying shareholders and stakeholders, and maintaining effective operational costs. In the name of accountability and transparency, the EIB, though possessing legal immunity, is compliant with Basel II, which is an international financial services requirement[1]. Meanwhile the NHSGGC has recently completed a massive restructuring process as a result of integration with the dissolved NHS Argyll and Clyde, and in effort to improve the level of accountability and transparency in delivering healthcare services. Managing NHSGGC is not all about managing healthcare services as it is also about managing other related support services, such as the purchase of medical equipments and laundry services. Since NHSGGC is the largest public organisation in Scotland, managing it is certainly complicated.

[1] Basel II is also known as The New Accord is the second Basel Accord and represents recommendations by bank supervisors and central bankers from 13 countries making up the Basel Committee on Banking Supervision (BCBS) to revise the international standards for measuring the adequacy of a bank's capital. It was created to promote greater consistency in the way banks and banking regulators approach risk management across national borders. Further information available at http://www.bis.org.

Given that, the availability and accuracy of records is a key factor in ensuring legal compliance, it is essential to investigate record keeping practices in private organisations that enable them to comply with the meticulous requirements of regulations. Although, Standard Life and the EIB are in different areas of businesses, the documentation of events and the management of records should not be that dissimilar. It can be presumed that, there is a correlation between the nature of an organisation and the level of commitment to establish an effective record keeping system. It is extremely difficult for public organisations to imitate practice in the private sector, because the constraints and the social responsibility of public organisations are more complex than in the private sector (Moss, 2006a).

From a records management perspective, records play an essential role in the accountability processes, though less fortunately, records management is not regarded as essential for good governance by senior management in either the public or private sector. Today, accountability and transparency of governance is a global agenda. In order to demonstrate transparency, the ability to recognise and gauge the types and levels of risk is definitely useful in generating cost effective operations. An organisation must strike a balance between the cost of operations and managing information and records within the context of the risks they face. There is, indeed, an increasing need to integrate records management with risk management and by so doing add value to the pursuit of strategic objectives.

However, an integrated records and risk management approach is yet to be seen explicitly being practiced in the public sector, though it has been implemented in many private organisations, such as the Standard Life. An organisation, be it public or private, must achieve cost effective operations that can be only achieved in the context of an organisational-wide risk management culture. Whenever possible, public organisation should imitate the practice of the private sector in order to reach operational cost efficiency. It does not matter, which party is mimicking which, as the main objective is to deliver value for money services to the public. The following case studies describe various circumstances and approaches used by organisations in ensuring their sustainability and competitiveness whilst improving their accountability and governance.

4.2 Methods of Data Gathering

Data and information from all the case studies was gathered through document analysis and interviews. Annual reports, meeting minutes and the organisations' websites provided essential information particularly on background, performance and achievement of the organisation. Meanwhile, interviews with various officials enabled gathering of empirical data and information such as interviewees' first hand experience and their perception on certain things with regards to the research. All interviews were of semi-structured type. Questions were designed based upon the research questions and objectives. Data and information gathered were then cross-checked with information from annual reports and the organisation's website. Drafts of reports were sent to the respective organisations for approval of the accuracy of the information.

4.3 Standard Life plc, Edinburgh

4.3.1 Background

The Standard Life Assurance Company ("Standard Life") was established in 1825 and the first Standard Life Assurance Company Act was passed by Parliament in 1832. Standard Life was reincorporated as a mutual assurance company in 1925.
Standard Life originally operated only through branches or agencies in the UK and certain other countries. It withdrew from many overseas markets during the inter-war years except for Canada (founded in 1833) and Ireland (founded in 1838). This largely remained the structure of Standard Life until 1996, when it opened a branch in Frankfurt, Germany with the aim of exporting its UK life assurance and pensions operating model to capitalise on the opportunities presented by EC Directive 92/96/EEC (the "Third Life Directive"). It offered a product range in that market with features that local providers were unable to offer. In the 1990s, Standard Life also sought to diversify its operations into areas which complemented its core life assurance and pensions business, with the intention of positioning itself as a broad range financial services provider. The following range of products is offered by the Standard Life Group:

i. Banking, Healthcare & Investments –
   The group set up Standard Life Bank, as its UK mortgage and retail savings banking subsidiary, in 1998 and Standard Life Investments, which had previously been the in-house investment management unit of the group's life assurance and

pensions business, was separated into a distinct legal entity in the same year, with the aim of establishing it as an independent investment management business providing services to both the group and third party retail and institutional clients. The group acquired Prime Health Limited (subsequently renamed Standard Life Healthcare) in the UK in 2000. Standard Life Healthcare expanded in March 2006 with the acquisition of the Private Medical Insurance[2] (PMI) business of FirstAssist.

ii. Standard Life Asia Limited/Joint ventures

The group's Hong Kong subsidiary, Standard Life (Asia) Limited ("SL Asia"), was incorporated in 1999 as a joint venture and, when the joint venture partners withdrew, became a wholly-owned subsidiary of Standard Life in 2002. This was established to give the group a presence in the Far East from which it could expand into China. The group's joint venture in India with Housing Development Finance Corporation Limited ("HDFC") was incorporated in 2000 (in relation to life assurance and pensions) and 2003 (in relation to investment management). The group's joint venture in China with Tianjin Economic Development Area General Company ("TEDA") became operational in 2003.

iii. Standard Life International Limited

Standard Life also incorporated Standard Life International Limited ("SLIL") in 2005 for the purposes of providing Standard Life with an offshore vehicle, based in Ireland, through which it could sell tax-efficient investment products into the UK. Sales of these products commenced in 2006.

iv. Service company

Following Standard Life's strategic review in 2004 and the announcement of its decision to proceed towards demutalisation, Standard Life established a service company structure for the provision of central corporate services to the group's business units. Standard Life Employee Services Limited ("SLESL") supplies a wide range of central services to the rest of the group, including IT, facilities, legal and human resources services, and employs staff working in the group's UK and Irish operations (other than SLI, SLB and SLH, which employ their staff directly). This

[2] Private Medical Insurance is designed to allow policy holders to receive treatment privately, avoiding delays through NHS in securing treatment for eligible medical conditions. Private Medical Insurance provides cover for acute, treatable medical conditions.

service company structure was created to enable Standard Life to comply with regulatory restrictions on the provision of non-insurance services and to exploit group-wide synergies.

4.3.2 Governance of Standard Life

Standard Life Plc owns all of the businesses and companies in the group. It is a holding company which is owned by its shareholders (including those eligible members who received and retained shares received as a result of demutualisation). The Group is seriously affected by the volume of regulation. It is increasingly squeezed between the need to perform, and avoid negative impacts, as well as reduce costs (Raschen[3], 2005). Good corporate governance is increasingly essential if the Group is to remain competitive and demonstrate transparency which is a key requirement, particularly for its shareholders and stakeholders.

Figure 4.3.2 The Structure of Standard Life outlines the components of the Group. Directly beneath Standard Life plc are Standard Life Employee Services, Standard Life Canada and Standard Life's interests in its Chinese and Indian joint ventures. Also underneath Standard Life plc are Standard Life Healthcare, Standard Life Investments and Standard Life Assurance Limited, the new UK life assurance company, which will also carry on business through branches in Germany, Ireland and Canada. This new company has With Profits funds[4], Non Profit funds[5] and Shareholder funds. Standard Life makes use of the With Profits Fund, Standard Life Investment Funds and Standard Life Bank makes use of the shareholder fund.

---

[3] Henry Raschen, head of Market Strategy, HSBC Securities Services Europe, quoted in Kalpana Limbachia (2005). 'Ever-increasing complexity favours the specialists regulation, compliance and governance: many institutions choose to hand the task to their custodian' *Financial Times*, 6 September 2005.

[4] A with-profit fund is a fund into which the premiums paid by individual with-profits policyholders are pooled and invested together with premiums paid by other policy holders, including other classes and generations of policyholders. The investment return (including losses on this pooled funds is then available to be shared by the policyholders in the fund and also, where applicable, by shareholders. Further information available at: http://www.fsa.gov.uk/pages/Library/Other_publications/Miscellaneous/2005/wp_supervision.shtml (13 November 2006).

[5] A non-profit fund is a long-term insurance fund which is not a with-profits fund. http://fsahandbook.info/FSA/html/handbook/Glossary/N (9 November 2006). The FSA states that a firm must maintain in a separate accounting record in respect of each of its long-term insurance funds (including with-profit funds) http://fsahandbook.info/FSA/html/handbook/PRU/7/6#D1295. (9 November 2006).

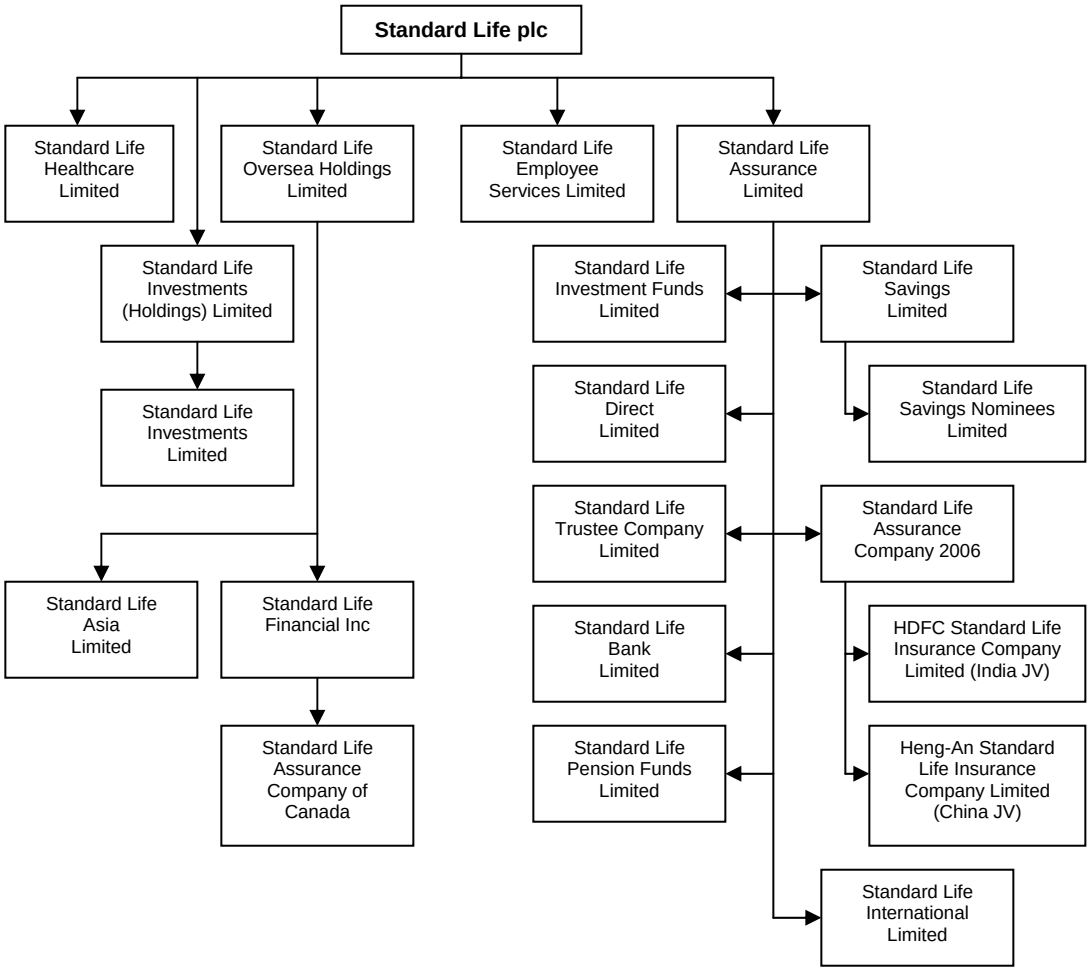

Figure 4.3.2: The structure of Standard Life[6].(20 April 2007)

The organisational structure of the Group is clearly defined by reference to business units, including subsidiary companies and branch operations. Authority for managing the Group is delegated to the executive directors and senior managers. For each subsidiary, the appropriate senior managers have been appointed as executive directors. The boards of key operating subsidiary companies also include an appropriate number of independent non-executive directors. The management of each individual business unit is the responsibility of the relevant directors and senior management. The roles and responsibilities of the Board of Directors includes approval of the objectives and strategies of the Group and its subsidiaries and

[6] Further information available at: http://ukgroup.standardlife.com/html/about/governance.html (20 April 2007).

branches, approval of significant changes in the Group's capital or corporate structure or in its structures of management or internal control and the approval of specific transactions, communications and appointments.

The Board comprises of the Chairman, four executive directors, and eight independent non-executive directors. The Board meets on a monthly basis to consider key business issues, and more frequently when necessary. Directors receive relevant papers in advance of Board and committee meetings, and receive regular reports on the Group's financial position, key areas of the Group's business operations and other material issues. All non-executive directors are independent in character and judgement. The division of responsibilities between the Chairman and Group Chief Executive is clearly defined and the roles are separate. The Chairman is responsible for the leadership of the Board, and the Group Chief Executive for the day to day management of the Group. In discharging his responsibilities, the Group Chief Executive is advised by the executive directors and senior managers of the business units.

The Group has two senior management risk committees, namely the Group Asset and Liability Committee (ALCO) and Group Operational Risk Committee (GORC). The Group ALCO functions to ensure the financial risks (credit, market, liquidity and insurance) inherent in the Group's activities are identified and managed in accordance with the appetite and limits approved by the Board. The Group ALCO is chaired by the Group Finance Director, and its members include senior finance representatives of the Group companies. The Group GORC is chaired by the Director, Group Risk and Compliance and its members include senior managers with operational responsibilities at each Group company.

The Group strives to operate with integrity and fairness. Corporate social responsibility is a fundamental part of their business philosophy and culture. The Group believes that a company run in the long term interests of its shareholders should manage its relationships with its employees, suppliers and customers and behave responsibly towards the environment and society as a whole. The Group states further that companies that can demonstrate a commitment to environmental and social responsibility are likely to enjoy comparative advantage in the long term. Being in the business for nearly two centuries, this statement reflects its long term commitment

towards those constituencies that makes the Group one of the key players in its market. The Group's corporate social responsibility programme covers five key areas namely:

- Engaging with its external stakeholders
- Managing and developing its people, including human rights
- Being active and responsible investors (shareholders responsibilities including socially responsible investment and corporate governance)
- Protecting the environment
- Investing in local communities.

A corporate social responsibility committee was established to represent its operations, not only in the UK but also in other countries.

4.3.3 Risk Management in Standard Life

Managing pension schemes and equities requires awareness of changes of regulation over time as financial institutions are constantly exposed to various risks, particularly pension mis-selling, stock market falls and money laundering. The Group has learnt from experience that pension mis-selling can be costly to resolve. Since 1988, employees could opt out of joining or being a member of an occupational pension scheme and the exercise of this option was encouraged by government. However, the full blame (rightly in some cases) and subsequent costs were laid at the door of companies selling personal pension products on the grounds that they had not fully alerted customers to the possible consequences of opting out of final salary occupational pension schemes. Although Standard Life was convinced that the number of mis-sellings was small, the process of examining every mis-sold contract required considerable effort over several years and was expensive (Moss, 2000).

Moss further explains that many people were wrongly advised to transfer existing benefits to a personal pension or to take out a personal pension in preference to their occupational scheme. As a consequence, Standard Life had to compensate some of its policy holders. Mis-selling of pension schemes did not occur in Standard Life alone, but in other companies selling personal pension products as well. Generally, the impact of the mis-selling was damaging to the public's confidence in life assurance and pension products. Moss asserts that in the first quarter of 1995 sales of regular premium pension and individual life products by the whole insurance industry in the UK plunged by 20 per cent compared to the first quarter of 1994, itself a poor year.

Several companies sold their life assurance interests and a few life offices were forced to find protection through amalgamation.

Today, financial institutions are facing greater than ever risks following the terrorist attacks in New York on September 11, 2001, and bombings in London on July 7, 2005. In order to avoid financial institutions being used by terrorists to transfer funds, the FSA suggests that financial institutions should adopt a risk-based approach in managing their operations. In line with the suggestion, the Group adopts an organisational-wide risk management strategy in achieving its corporate, financial and regulatory objectives. The Group Risk Management Policy ensures that the risks taken in meeting the Group's corporate, financial and regulatory objectives are identified and managed in accordance with the approved risk framework. The types of risk inherent in the pursuit of these objectives and the extent of exposure to these risks form the Group risk profile. The risk profile of the individual business units within the Group is similarly set by reference to its objectives.

Risks are managed through the group risk management framework, which allows the identification, assessment, control and monitoring of risks across the organisation. The Group and each individual business unit establish effective risk management systems and controls within the framework for the following high-level categories of risk: insurance, credit, liquidity, market and operational. There are separate Group Risk Policies for each category of risk specifying the procedures to be taken across the Group to identify, assess, control and monitor the risk. The governing body of each individual business unit also approves, as applicable, its own risk policies in line with the applicable Group Risk Policy. Each Group Risk Policy sets out minimum standards to which each individual business unit should adhere in constructing its own policies and procedures.

The Board delegates responsibility for the implementation of the day-to-day process for the management of risk across the Group, to the Group Chief Executive. The Group Chief Executive is supported in this role by the Group Executive Committee and assisted by the Group Technical Risk Committee and the Group Operational Risk Committee. These committees are constituted with formal terms of reference. The Group has an established risk management function whose role is to support the

Board, the Group Chief Executive and the risk committees in meeting their risk management responsibilities. This centralised function is headed by the Director, Group Risk and Compliance, who reports directly to the Group Finance Director and is the FSA Approved Person[7] charged with reporting to the Board on setting and controlling risk exposure across the Group. A consolidated Board report is prepared on a quarterly basis summarising the information reported to the Group Risk Management Committees. The report comprises detailed sections on:

- Business Unit Risk Profiles
- Strategic Risks
- Group-wide Project Risks
- Operational Risks
- Technical Risks.

The Group has identified five types of risk, namely:

a) Insurance risk

Insurance risk arises from the inherent uncertainties as to the occurrence, amount and timing of insurance liabilities. It is the risk of adverse deviations from the cash flows assumed when pricing or reserving insurance contracts.

b) Credit risk

Credit risk is the risk incurred whenever the Group or individual business units are exposed to loss if a counterparty fails to perform its contractual obligations, including failure to perform those obligations in a timely manner.

c) Liquidity or funding risk

Liquidity risk is the risk that the Group or individual business units, although solvent, do not have sufficient financial resources available to meet their obligations as they fall due, or can secure them only at excessive cost.

[7] An approved person is an individual who has been approved by the FSA to perform one or more 'controlled functions' on behalf of an authorised firm. The purpose of the direct approval of individuals who perform controlled functions is to complement the regulation of the authorised firm for which the approved person(s) performs the function. An individual cannot be approved in advance of a firm becoming authorised, but the application will be co-ordinated to ensure that the approval coincides with the giving of permission to the firm. Approval must be obtained before a person can perform a controlled function. Further information available at: http://www.fsa.gov.uk/Pages/Doing/Regulated/Approved/index.shtml (13 November 2006).

d) Market risk

Market risk is the risk that as a result of market movements the group or individual business units may be exposed to fluctuations in the value of its assets, the amount of its liabilities or the income from its assets. Sources of general market risk include movements in interest rates, equities and foreign exchange rates.

e) Operational risk

Basel II has shifted attention from credit to operational risk, and increasing concentration of securities markets has concerned regulators in terms of systemic credit collapse and business continuity (Limbachia, 2005). Operational risk is defined as the risk of loss, or adverse consequences for the business, resulting from inadequate or failed internal processes, people and systems, or from external events. The types of operational risk the Group is exposed to are identified using the following operational risk categories: fraud or irregularities; regulatory or legal; customer treatment; business interruption; supplier failure; planning; process execution; and people. Activities are undertaken to ensure the practical operation of controls over financial risks (i.e. market, credit, liquidity and insurance risk) are treated as an operational risk.

A strategy to control the operational risk exposures identified is based on a combination of one or all of the following: modify operations such that there is no exposure to the risk; accept exposure to the risk and choose not to control the risk; or accept exposure to the risk and choose not to control the risk; or accept the exposure to the risk and control the exposure by risk transfer or risk treatment. The level of control and nature of the controls implemented is based on, amongst other things:

- Potential cause and impact of the risk
- Likelihood of the risk happening in the absence of any controls
- Ease with which the risk could be insured against
- Cost of implementing controls to reduce the likelihood of the risk occurring
- Operational risk appetite

Existing and newly implemented controls are identified, including key controls, documented and their performance subject to self-assessment by business managers at least quarterly. A conclusion as to the adequacy of these controls is documented and subject to ongoing self-assessment by business managers. The assessment of operational risk exposures is performed on a quantitative and qualitative basis using a combination of likelihood and customer, financial and reputational impact. The accuracy of the assessment relies on the availability of adequate and up-to-date records. This in turn, produces records which subsequently will be managed by the Group Records Management Division.

As part of the development of their business plan each Group company ensures that relevant stress testing is carried out, at least annually, to help identify the exposure to operational risk. The operational risks faced by the each Group company and its exposure to these risks forms it operational risk profile. Each Group company is required to understand and review its profile by monitoring its key operational risk exposures, compliance with approved threshold, loss experience and the results of control self-assessment. The impact of a new product, a significant change, or any one-off transaction on the operational risk profile of each Group company is assessed and managed in accordance with established guidelines or standards.

Table 4.3.3 is an illustration of the risk scorecard use in Standard Life. The risk scorecard includes the types of operations or tasks, legal compliance requirements, present status, the levels of likelihood and impact of risk and the types of risks perceived.

Item	Operation /Task	Legal Compliance	Present situation	Risk Level		Types of risk perceived
				Likelihood	Impact	

Table 4.3.3: An example of a risk scorecard in Standard Life.

The remedies for these risks involve having better information, reporting, documentation and collateral management, and above all transparency process. In future, custodians will be required to take on a more consultative role and work in partnership with their clients so as to ensure that they meet compliance, regulation, and governance demands. Compliance, indeed, is a fact of life in financial services and much of what has now become regulation previously existed as best practice (Limbachia, 2005).

Money laundering has increasingly concerned financial institutions and regulatory bodies. The directive of the European Parliament and the Council on the prevention of money laundering and terrorist financial system for the purpose of money laundering and terrorist financing spell out a series of money laundering regulations to curb and monitor such activities. In conjunction, the FSA urges all financial institutions to ensure that they have robust and effective controls from a Know Your Customer (KYC) perspective if they are to meet operational standards. KYC is the collection and use of information about a customer over and above the collection of basic evidence of identity such as passports, driving licences and utility bills (FSA, 2002). Indeed, KYC is a vital record that must be properly managed for subsequent use.

Managing capital is an on-going process of determining and maintaining the quantity and quality of capital appropriate for the Standard Life Group and ensuring capital is deployed in a manner consistent with the expectations of the Group's stakeholders. It is important to note that the Group considers their key stakeholders are the FSA and the providers of capital (their members and holders of their subordinated liabilities). Managing capital should be seen from a wider risk management perspective to instigate and cultivate an organisational-wide risk management culture. If this can be achieved, the Group should be able to attain its strategic objectives whilst striking the balance between effective operational cost and minimising risk.

4.3.4 Audit Committee of Standard Life

The Board has approved the Group Risk Management Policy which sets out the overall framework through which risks are managed across the Group. The framework is designed to support the identification, assessment, monitoring and control of risks that are significant to the Group's business objectives. The policies for each category of

risk are reviewed and approved annually by the Board. This is essential to ensure the Group remains compliant and profitable. Group Risk Management has overall responsibility for reporting to the Board in relation to setting and controlling risk exposures. It drafts the Group risk policies for the Board's approval. It also supports and monitors the effective implementation of the policies at Group and business unit levels and supports the Risk Committees. Risk functions have also been established in each business unit. The role of these functions is to implement the Group policies as appropriate to each business unit.

The members of the Audit Committee are all independent non-executive directors. The Audit Committee's remit is to consider any matter relating to the financial affairs of the Group, its internal and external audit arrangements and its internal control and compliance arrangements. The Audit Committee meets at least four times a year, and will meet more frequently whenever required. At least once a year, it meets with the external and internal auditors without management being present. This is essential to enable the Audit Committee to discharge its fiduciary responsibility without interference from the management. However, the Audit Committee meetings are also attended by the Group Chief Executive, Group Finance Director and other members of senior management as appropriate. This provides an opportunity for both parties to clarify and justify any grey area that emerged during the audit process. The Audit Committee reports its activities and makes recommendations to the Board.

The Audit Committee reviews the financial statements of the Group, the Company's regulatory returns and any formal statements relating to the financial performance of the Group and group Companies. This incorporates consideration of significant accounting policies, estimates and judgements applied, changes made to these during the period, and the view of external auditors. It considers the effectiveness of the Groups' internal audit function and monitors the external auditor's independence and objectivity, and the effectiveness of the external audit process.

The Audit Committee also receives regular updates from the Group Operational Risk Committee and Group Technical Risk Committee. It also reviews the arrangements by which staff of the Group may, in confidence, raise concerns about possible impropriety in matters of financial reporting and other matters under the Committee's remit. Any

concerns are independently investigated and the Committee ensures that appropriate follow up action is taken. In undertaking its duties, the Committee is authorised by the Board to obtain any information it requires from any director or employee of the Group. The Committee is also authorised to seek, at the expense of the Group, appropriate professional advice inside and outside the Group whenever it considers this necessary.

The directors have overall responsibility for the group's system of internal control and for the ongoing review of its effectiveness. The system is designed to manage rather than eliminate the risk of failure to meet business objectives. It can only provide reasonable, not absolute, assurance against material misstatement or loss. The effectiveness of internal controls is reviewed regularly by the Group Internal Audit and Group Compliance, which report their findings to the Audit Committee and the Board. The review is in accordance with the Combined Code[8] and the Turnbull Report[9]. It is based on reports provided by Group Internal Audit, Group Compliance and Group Risk Management.

It also includes reviewing the results of the process of direct self-certification where directors and senior managers across the Group confirm their compliance with the relevant elements of the Group's internal control framework, including policies and minimum standards. The review covers material internal controls, including financial, operational and compliance risk controls. Where material control weaknesses are identified, corrective action plans are put in place and monitored regularly. This is to ensure the Group is complaint with all relevant regulations before the external auditors conduct their assessment. Further more, it is more cost effective as a corrective plan can be drawn out whilst any problem is at an early stage.

---

[8] *The Combined Code on Corporate Governance* (July 2003), by the Financial Services Authority, is a complete guidance for good corporate governance for public listed companies. It details out the role of companies including the board of directors, chief executives, audit committees and also the role of shareholders. Further information available at: http://www.fsa.gov.uk/pubs/ukla/lr_comcode2003.pdf (9 November 2006).

[9] Turnbull Report is the popular name given to the guidance '*Internal Control: Guidance for Directors on the Combined Code*' issued by the London Stock Exchange (LSE) in the UK. The aim of the guidance is to ensure that all companies trading on the LSE have in place an adequate system of internal control in order to facilitate the management of business risk. Further information available at: http://www.globalcontinuity.com/thought_leadership/what_is_the_turnbull_report (13 November 2006).

4.3.5 Records Management in Standard Life

Managing capital is a highly risky business, particularly after the catastrophic terrorist attacks. Financial institutions must be able to provide evidence for investigations whenever required by legal process. The FSA admits good record keeping makes a positive contribution to the fight against crime and terror by providing an audit trail of financial records of those involved (Robinson, 2005). KYC forms provide vital evidence of customer relations. Effective management of on-going KYCs needs more robust and timely information management. It is not uncommon for a financial firm to hold KYCs for up to 40 or 50 years as life insurance business is a long-term commitment. The Group needs to be certain that the necessary records of identity verification and transactions are retained and readily retrievable.

The absence of adequate and reliable records management systems may expose the Standard Life Group to risk from various quarters. Standard Life now has a well established business as usual records management framework. It all started with a pilot project. A comprehensive records management project was launched in 2001, which the Group appointed Mrs Kate Knight, as the Group Records Management Manager to lead[10]. Mrs Knight was previously a Systems Manager. The initial project took 18 months to accomplish and tellingly was sponsored by two members of the Senior Executive – the then General Manager, Compliance and the General Manager, Facilities.

In an interview on 16 February 2006, Mrs Knight explained that during its peak, the records management unit had 8 members of staff including herself[11]. At present, there are only four staff left, partly as result of downsizing in conjunction with the Group's demutualization plan. Although the number is small, the staff come from different academic backgrounds, including one with a legal experience. It is important to note that managing records exposes the Group to legal risk, for example, if records are destroyed earlier than stipulated by legal or other requirements. As manager, Mrs

[10] Unfortunately this project does not cover electronic records and e-mails instead it only covers business records, which are mainly in physical form.

[11] It is essential to note that the interview was conducted whilst the organisation was amid of preparation for demutualisation. Therefore, the confidentiality of information was tightened. As a consequence, the interviewee was not provided with paper documents which could lead to the leaking of information.

Knight is also responsible for providing on-going trainings for the career development of the unit's staff[12].

The Group Records Management unit adopts a holistic approach by integrating the records management function into Standard Life's risk management framework. The current strong backing from the Director, Group Operations, is important for the unit, and particularly the manager, who is also responsible for promoting the benefit of good records management to the senior management and managers of business units. Mrs Knight explained that collaboration with senior managers of business operations, support functions such as information systems, and risk management units including audit, compliance, legal, information security and physical security are elements that contribute to the establishment of consistent records management practices.

This collaboration is also essential in the development of robust records retention schedules. Standard Life has a suite of retention schedules created using Designing and Implementing RecordKeeping System (DIRKS) methodology. A top-down analysis is followed up by bottom-up analysis. The schedules are designed to reflect business functions and there is a hierarchy of schedules. At the top level, a schedule documents records that the Group must have. Another level lists those relevant to the specific businesses of companies within the Group, such as Investments and Healthcare. Then, there is a suite of schedules for non line-of business records, such as Human Resources. Table 4.3.5 attempts to illustrate the integrated records management approach used by the division across the Group.

Item	Types of records	Reason for keeping	Retention period	Disposal requirements

Table 4.3.5: An example of a record retention schedule in Standard Life.

[12] At the time the interview was conducted, one of Mrs Knight's staff was pursuing tertiary education in records management in England.

Standard Life's retention schedules are designed to show what records it needs to keep, the precise reasons why, how long it needs to keep them and disposal requirements. The requirements are rigorously researched, with specific citations of legal and regulatory authority, so that the company can rely on them to make decisions. In contrast, traditional records retention schedules are less convincing as they only tend to detail the length of time records need to be kept. Business managers are interested not only to know how long they need to keep records, but more importantly because they need to know why they have to and what are the repercussions if they failed to keep or destroy records, precisely because they need to manage costs.

Records-related operational risk management is one of Group records management activities, but is not encapsulated in the retention schedule only. It is done via means of policy compliance reporting, reviews of records management practices, gap analysis and action planning, working together with the business units. Business units provide bottom-up analysis once the Group Records Management unit has completed the top-bottom analysis. It is a collaborative process and means that the business units do not have to invest significant resource in research of legal and regulatory requirements. Indeed, it is a win-win situation for the Group Records Management division, the Group Operational Risk Committee, the Group Technical Risk Committee as their individual contributions are enhanced. The Group as a whole certainly gains more benefits from an integrated records management and risk management approach.

A good working relationship between the Group Records Management division and these committees enables the development of the policy, processes and tools, such as retention schedules. It is not individual units, but the whole organisation that should benefit from such an integrated records management approach. It is worth noting that inputs from the legal division as well as the risk management committees are all vital in composing the retention schedule.

According to Mrs Knight, it is a time consuming process to produce such authoritative records retention schedules. Although senior management support was said to be excellent, it was the responsibility of the Group Records Management unit to champion the process. Understandably, the decision to demutualise means the Group had to ensure it had a comprehensive records management framework to support demanding

markets, policy holders, stakeholders as well as the FSA. In order to get their participation, Mrs Knight had to develop a good rapport across the group, particularly with business managers, as they are the owners of business processes. Mrs Knight found that working with business managers was always one of the most enjoyable aspects of the job.

It was invariably possible to find something in her brief that would really benefit their business operation. It was very rare to find a business manager who did not understand the value of records management practices. The only issue for most was finding the resource to commit to initiatives in the way they would have liked. However, it does need enthusiasm as records management is not always first on the list of people's priorities. It needs a champion to head the project, and Mrs Knight had what it took to lead the project. With experience as a systems manager, she knows the needs for good record management to underpin business process. This made it easier for her to understand the need to integrate a sound records management framework with existing business information systems.

Inputs from business managers are the key ingredients of the records retention schedules as they are well-versed with the nature of their business and the needs of regulations and compliance. In this context, the Group Records Management unit functions to compile inputs from various business units and to suit them with the level and types of risk identified by the Group Risk Management unit. Mrs Knight went on to say that the comprehensiveness of the retention schedules was very helpful to business managers in monitoring their performance against operational risk scorecards as well as ensuring that their respective business units manage records according to the retention schedules and records management guidelines.

The Group Records Management unit is responsible for the creation and implementation of Standard Life Group Records Management Policy, which covers all records formats, including digital, paper and audio-visual. The unit monitors and reports on policy compliance. The Group has a huge number of physical records, which means that sooner or later it will be faced with storage problems. As a solution, the Group launched a digitisation project to digitise physical records to save storage

space and facilitate document retrieval and access. However, the project is not under the remit of the Group Records Management unit, instead the Group IT unit.

Although the FSA (2003) perceived electronic methods of storage using scanning technology may offer a better longer-term alternative, there is not as yet a single one-for-all solution to ensure the sustainability of electronic copies over longer period. The Group has to be certain about digital longevity to avoid loss of records across time, particularly the growing number of records created electronically. In this context, collaboration with the Group Records Management unit is desirable and would be useful in order to ensure electronic copies retain their authenticity, whilst at the same time improving retrievability and accessibility.

Since the Board of Directors is accountable for the governance and performance of the Group, it was their decision that the Group should adopt a risk-based approach in achieving its strategic objectives. This led subsequently to the adoption of an integrated records and risk management approach. As a result, the Group Records Management division produced a series of comprehensive records retention schedules for the use of the whole Group. It is up to individual business managers to implement the policy provisions, as it is their personal responsibility to ensure that their individual business units function within the organisational–wide risk management framework.

4.3.6 Discussion of Research Objectives in Standard Life

Following is discussion on the case study in Standard Life, in line with the research objectives.

4.3.6.1 Records management and the governance of Standard Life

Standard Life operates under a volume of regulations such as the Combined Code on Corporate Governance and Basel II. These regulations demand accountability and transparency of business operations. In addition, the demutualization of the Group's shares also means better performance is expected to meet the expectation of shareholders and stakeholders. Performance is measured in term of profit which can only be retained when negative impacts can be avoided and costs can be reduced. Standard Life believes that companies that can demonstrate good governance and commitment to environment and social responsibility are likely to enjoy comparative advantage in the long term. It is evident that the strength of Standard Life is its ability to transform this belief into practice. Its clear governance structure facilitates the delegation of responsibility, which in turn leads to its sustainability for over nearly two centuries.

Arguably, the demand of regulations and the expectation of shareholders and stakeholders were the driving force behind good governance in Standard Life. The Group believes in delivering performance and acting with integrity by ensuring each and every employee does the right thing in order to achieve operational excellence. The efficiency of the Group is mainly contributed by the effectiveness of the Board of Directors, which meets on a monthly basis. Furthermore, with only 13 members the Board can often reach an agreement without lengthy discussion. Strategic decision-making is more efficient. This enables Standard Life to remain competitive in the financial and insurance industry. The Board of Directors is well aware of the importance of compliance and the ability to grasp business opportunities.

The sustainability of Standard Life relies not only on its compliance with regulations but equally importantly is its ability to grasp and expand business opportunities. This stance is consistent with the principles of corporate governance advocated by the OECD (2004) which states that to remain competitive in the changing world,

corporations must innovate and adapt their corporate governance practices so that they can meet new demands and grasp new opportunities. In other words, good governance is not only about ensuring compliance with regulations, but also about grasping new opportunities. Being in such a competitive industry, Standard Life has to ensure the availability of records as well as its operational efficiency in order to gain an edge over competitors. Thus, monthly board meeting is important to ensure the Group does not miss business opportunities.

Standard Life's senior management is aware of the importance of having sound information management and keeping of accurate and complete records is one of the cornerstones of effective governance. This is proven by the contribution of its two senior level risk management committees namely, the Group Asset and Liability Committee (ALCO) and Group Operational Risk Committee. Their involvement and support facilitated the incorporation of risk management into business processes. The efficiency of business processes and decision making is further enhanced by the establishment of an integrated records management system. This was instigated by two members of Senior Executive, the then General Manager, Compliance, and the General Manager, Facilities. It was their relentless support that fostered the cultivation of the importance of good record keeping across Standard Life. It evident that the awareness and commitment among senior management of the importance of good record keeping in underpinning good governance is central to transparency and accountability of Standard Life.

4.3.6.2 The Role of Records in the Accountability Processes in Standard Life

Accountability is an evidence based process that occurs after activities have been taken executed or decisions have been made. Records and the evidence that they contain are the instruments by which organisations can promote a climate of trust and overall commitment to good governance. Accountability of governance can only be demonstrated when the availability of adequate and reliable evidence is ensured through effective and efficient record keeping systems. It is essential for an organisation to demonstrate accountability not only to its shareholders and stakeholders, but also to the public as part evidence of social responsibility.

In the context of financial institutions, including Standard Life, demonstrating accountability is paramount for the same reasons. However, this is easier said than done as there is a pre-requisite to demonstrate accountability that is by ensuring transparency in business processes, which in turn requires reliable information and records management. Compliance with regulations cannot be proven in the absence of reliable records. This means business processes must be properly documented to provide reliable evidence of those processes. Willis (2005), a lawyer, advocates sound information and records management enables accountability. His view has credence as all organisations need to keep their records of business decisions and transactions to meet the demands of corporate accountability. Good record keeping practice has been nurtured in Standard Life particularly since the development of an integrated records and risk management in 2001 as explained by Mrs Knight, the then Records Manager. The effort and commitment from senior management was pertinent as only the availability of reliable records can ensure the accountability of the Group.

4.3.6.3 The Relationship between Risk Management and Managing Records in Standard Life

Theoretically, risk management and records management complement each other. The former uses records that are made available by records managers and produces records that will be systematically managed by them. Both risk management and records management are tools that enable an organisation to achieve organisational goals such as meeting shareholders value, stakeholders' expectation, good quality of service, efficiency, transparency and accountability. There must be a clear understanding that risk management is not about minimising risk but about understanding and managing risk.

Risk management is a cyclical process, whereby records produced must be kept for future assessment to determine whether recommended risk mitigation has been followed by relevant business process owners. The latter, meanwhile, prioritises the types of records according to the level of impact and the likelihood of risk to occur based on information made available in risk scorecards by the former. It is evident that Standard Life has expanded the notion of risk management. In their context, risk management is no longer confined to compliance with pertinent regulations *per se*, instead it embraces almost every aspect of the organisation from day-to-day activity

and operation to strategic decision making and even risk of managing records and information. It is vital to remind records management professionals that managing records is not about keeping everything because organisations can not afford that as the cost would be excessive. For example, annual surveys by Financial Executive International (FEI), a leading professional organisation serving Chief Financial Officers and other senior financial executives, revealed the costs of compliance with SOX since 2004 were too high, though they are decreasing in the second year of the law being in force[13].

Arguably, the cost of compliance will remain high despite the slight declination disclosed by the surveys. Advocating the need to practice and the benefit of good record keeping is meaningless if records managers themselves do not understand the applicability of records management in an organisation. In such situation, McDonald's suggestion that records managers must understand business processes in order to understand how records should be managed is perfectly relevant. Otherwise, records managers will marginalise themselves. Although senior managers are clearly concerned about adhering to the requirements of the law and established compliance standards, they are also charged with growing the organisations and generating profits for their shareholders (Sharon, 2006b). Hence, records managers must be in the same thinking territory to be relevant to the organisation.

To this end, Standard Life has developed a pragmatic approach by integrating risk and records management that enables its sustainability. Prioritising risk eventually followed by actions in managing records. Mrs. Knight asserts that the records management system in Standard Life was developed using DIRKS methodology. This is to say that risk assessment was involved in identifying record keeping requirements. It was assumed that a combination of the outcome of risk management and a system developed with associated risk taken into account, the management of records would be more economic. It is about merging risk scorecards (Figure 4.3.3) and records retention schedules (Figure 4.3.5).

[13] The surveys involved public companies with large market capitalization ranges from $75 million and above. Further information on details of the surveys are available at http://www.financialexecutives.org

Standard Life's records retention schedules illustrate not only the length of retention period but more importantly the reason for keeping records which indicates specific citation of legal and regulatory requirements as well as the repercussion if they failed to keep or destroy records. This is essential as business managers are busy enough managing operational tasks, and they need to be informed about the risk of failure to keep or destroy records. Hence, it is not a surprise that Mrs. Knight is benefiting from effective collaboration with most of business managers. The benefit certainly is not limited to the Group Records Management division and Risk Management Committees only, but Standard Life as a whole. Integrated risk and records management improves not only the performance but also ascertains risk expose to the organisation.

Mrs Knight admits although the process of producing an authoritative records retention schedule is time consuming and challenging, rigorous research and collaboration with Risk Management Committees and consultation with business managers facilitated the task. She further admits that it was the comprehensiveness of the retention schedules that attracts business managers to be more concerned about managing their business records. Any adversity resulted from their failure to manage records would be solely their responsibility as the requirements are made available to them. Fortunately, to date their respond and cooperation is encouraging, thus delighting Mrs Knight and her staff as their task in managing records becomes more efficient and effective and appreciated.

Arguably, the efficiency of records management in Standard Life is partly contributed by the adoption of DIRKS methodology in developing its records management system. DIRKS employs risk assessment approach in developing a record keeping system. Risk was comprehensively considered even in the conceptual stage of the development of the system *(Please refer Section 4.3.5 Records Management in Standard Life)*. This proves that the notion of risk management in Standard Life is not limited to compliance, but embraces every aspect of its operations as the sustainability of Standard Life relies not only on compliance but ability to satisfy shareholders' and stakeholders' expectation by continuously making profit and delivering corporate social responsibility.

4.4 The European Investment Bank, Luxembourg

4.4.1 Background

The European Investment Bank (EIB), the financing institution of the European Union (EU) was established in 1958 in accordance with the Treaty of Rome. The members of the EIB are the Member States of the EU, who have all subscribed to the Bank's capital. Being a continent-wide institution, the EIB enjoys its own legal personality and financial autonomy within the Community system. The EIB's mission is to further the objectives of the EU by providing long-term finance for specific capita projects in keeping with strict banking practice. It also contributes towards building a closer-knit Europe, particularly in terms of economic integration and greater economic and social cohesion.

As an institution of the EU, the EIB continuously adapts its activity to developments in Community policies. As a bank, the EIB works in close collaboration with the banking community both when borrowing on the capital markets and when financing capital projects. The EIB grants loans mainly from the proceeds of its borrowings, which, together with 'own funds' (paid-in capital and reserves), constitute its 'own resources'. Outside the EU, EIB financing operations are conducted principally from the Bank's own resources but also, under mandate, from EU or Member States' budgetary resources.

The EIB, together with the European Investment Fund formed the EIB Group. The European Investment Fund (EIF) which was established in 1994, provides venture capital and guarantees for small and medium enterprises (SME). In June 2000, the EIF's Statutes were reconstructed and its shareholding structure was modified (with the EIB becoming a majority shareholder[14]) so as to endorse the role of the EIF as the exclusive vehicle for the venture capital of the EIB.

4.4.2 Governance of the EIB

As the EU's financing institution, the EIB tailors its borrowing and lending activities to the Union's economic policies. As it funds its operations by borrowing on the capital

[14] The EIB owns 62 percent shares. Other shareholders are the European Commission (30%) and some twenty EU private banking institutions (85). Further information available at: http://www.eif.org (20 November 2006).

markets rather than by drawing on the Community budget, the Bank enjoys decision-making independence within the Community's institutional system, in accordance with its Statute[15]. The EIB's management and control structures reflect the independence and allow it to take lending and borrowing decisions solely on the basis of a projects' merits and the best opportunities available on the financial markets. The shareholders of the EIB are the 25 Member States of the EU. Each Member State's share in the Bank's capital is calculated in accordance with its economic weight within the European Union at the time of its accession[16]. In total, the Bank's subscribed capital amounts to more than €163.6 billion. The EU Member States are fully eligible for Bank financing operations, without any geographical or sectoral quotas being applied. Under its Statute, the Bank may have maximum loans outstanding equivalent to two and half times its capital.

The EIB is governed by four bodies, namely:

i. Board of Governors

The Board of Governors consists of Ministers designated by each of the 25 Member States, usually Finance Ministers. It lays down credit policy guidelines, approves the annual accounts and balance sheet, and decides on the Bank's participation in financing operations outside the EU as well as on capital increases. It appoints the members of the Board of Directors, the Management Committee and the Audit Committee.[17]

ii. Board of Directors

The Board of Directors has sole power to take decisions in respect of loans, guarantees and borrowings. The Board of Directors is also responsible for ensuring that the Bank is managed in line with the Treaty and the Statute and with the general directives laid down by the Governors. Members of the Board of Directors are appointed by the Governors for a renewable period of five years following nomination by the Member States and are responsible solely to the Bank. The Board of Directors consists of 26 Directors, with one Director nominated by each Member State and one by the European Commission.

[15] http://www.eib.org/cms/htm/en/eib.org/attachments/general/statute/eib_statute_2007_en.pdf (21 June 2007).
[16] http://www.eib.org/about/index.asp?dep=108 (20 November 2006).
[17] http://www.eib.org/about/structure/dep_gov.asp (20 November 2006).

There are 16 Alternates, meaning that some of these positions will be shared by groupings of States. Furthermore, in order to broaden the Board of Directors' professional expertise in certain fields, the Board is able to co-opt a maximum of 6 experts (3 Directors and 3 Alternates), who participate in the Board meetings in an advisory capacity, without voting rights. Since 1 May 2004, decisions have been taken by a majority consisting of at least one third of members entitled to vote and representing at least 50 percent of the subscribed capital. As the Board of Directors is non-resident, members do not receive remuneration from the Bank. For each meeting day of the Board (normally ten per year) in which they participate, Members and Alternates of the Board of Directors receive an indemnity of €600. In addition, the Bank pays a per diem of €200 as a lump-sum reimbursement for hotel and related expenses to be covered by individual Board Members and reimburses travel expenses.[18]

iii. Management Committee

The Management Committee is the Bank's permanent collegiate executive body. It has nine members. Under the authority of the President and the supervision of the Board of Directors, it oversees day-to-day running of the EIB, prepares decisions for Directors and ensures that these are implemented. The President chairs the meetings of the Board of Directors. The members of the Management Committee are responsible solely to the Bank. They are appointed by the Board of Governors, on a proposal from the Board of Directors, for a renewable period of six years.[19]

iv. Audit Committee

The Audit Committee is an independent body answerable directly to the Board of Governors[20] and responsible for verifying that the operations of the Bank have been conducted and its books kept in a proper manner. Further discussion on Audit Committee is available in *Section 4.4.4 Audit Committee of the EIB.*

[18] http://www.eib.org/about/structure/dep_dir.asp (1 May 2006).
[19] http://www.eib.org/about/structure/dep_mc.asp (1 May 2006).
[20] The Board of Governors consists of Ministers nominated by each of the Member States, usually Ministers of Finance, Economic Affairs or the Treasury. They represent the Bank's shareholders Member States.

As both a Community body and a financial institution, the Bank cooperates with other independent control bodies including the European Court of Auditors, European Anti-Fraud Office and the European Ombudsman.

On the date of study, there are 12 Directorates and Departments in the EIB, namely[21]:

i. General Secretariat and Legal Affairs
ii. Directorate for Lending Operations in Europe
iii. Directorate for Lending Operations outside Europe
iv. Finance Directorate
v. Projects Directorate
vi. Risk Management Directorate
vii. Human Resources
viii. Information Technology
ix. Inspectorate General
x. EIB Group Compliance Office
xi. Management Committee Advisor
xii. Representation of Board of Directors of European Bank for Reconstruction and Development

The responsibility of these departments and directorates are:

- To evaluate, appraise and finance projects
- To raise resources on the capital markets and manage the treasury
- To assess and manage risks attaching to EIB operations
- To carry out necessary economic or financial background studies

Working together in multidisciplinary teams, these directorates and departments prepare and implement the decisions of the Bank's management. The EIB and its staff are covered by a Code of Conduct that sets out the rules and standards for professional behaviour. Members of staff are expected to commit themselves to the Bank, act loyally, honestly and impartially, and subscribe to a high standard of personal

[21] These have since changed. A new Strategy and Corporate Centre Department was established, of which Building, Logistic and Documentation Division, of which Documentation and Records Management Unit is located. Further information available at: http://www.eib.org/about/index.asp?dep=107 (1 March 2007).

and professional ethics. In order to ensure compliance, the Bank established a Compliance Office in 2004 that functions to identify, assess, advice on, monitor and report on the compliance risk of the Bank.

Transparency and accountability constitute one of the two pillars of the Bank's strategy, the other being value-added[22]. It is the strategy of the Bank to implement EU policy, generate more value-added, take more risks, and generate more surplus. As a publicly owned bank with the mission of furthering and supporting EU advancement, the Bank is committed to attaining a high level of transparency of its activities, thereby showing the value of its operational performance. Corporate governance of the Bank has been reinforced by a number of measures endorsed by the Board of Governors, agreed by the Board of Directors and developed and put into practice by the Management Committee on an on-going basis. The Bank's policies and the measures taken in the areas of defining and formulating strategies, ways and means of implementation and transparency towards civil society are summarised in the Corporate Operational Plan, Corporate Governance Statement and Public Disclosure Policy (EIB, 2006a).

By the end of 2005, over 85 percent of the transparency policy's action plan to boost disclosure of information had been achieved, including:

- The stock of documents disclosed through the EIB's website had increased by 50 percent since the publication of the transparency policy. Many of the new documents published dealt with issues of corporate governance, policies and strategies. Two key documents were the Statement on Corporate Social Responsibility' and 'Statement on Governance at the EIB (EIB, 2006b).

Indeed, several actions were taken in 2005/2006 that proved the commitment of the Bank to increasing transparency and accountability including:

- A first public Statement on Corporate Social Responsibility in May 2005, which complements a number of other corporate governance measures including the Transparency Policy and the annual Statement on Governance at the EIB.

[22] Further information of the EIB Transparency Policy available at http://www.eib.org/cms/htm/en/eib.org/attachments/strategies/transparency_en.pdf (21 June 2007).

- The Bank's Public Disclosure Policy was drawn up following the Bank's first public consultation procedure on Bank policy. The Policy is founded on a presumption of disclosure but necessarily takes into account the fact that the Bank can only operate efficiently as a credit institution if banking relationships are managed appropriately, in line with EU legislation, those of the EU Member States and internationally accepted practices. The Management Committee therefore considers that it has to strike a balance between attaining full disclosure to interested third parties and the clear duty of the Bank to protect the legitimate business interests and confidentiality requirements of its clients, particularly those from the private sector.
- A new Document and Records Management Policy and a set of common principles to ensure the reliability of the Bank's documents and records were approved by the Management Committee in March 2006, underlining the evidential value of authentic, reliable and usable records as proof of business activities.
- Greater clarity in the disclosures made in the *curriculum vitae* of the members of the Board of Directors and systematic publication of individual declarations of conflicts of interest in relation to projects.
- Publication of the *curriculum vitae* of the Directors General of the Bank[23].

The Bank aims to continuously increase the level of transparency and compliance whilst remaining efficient in supporting the objectives of the EU.

4.4.3 Risk management in the EIB

The Bank aligns its risk management systems to changing economic conditions and evolving regulatory standards. It adapts on an ongoing basis as 'best market' practice develops. Systems are in place to control and report on the main risks inherent to its operations, particularly credit, market and operational risks. It is essential for the Bank to apply best market practice in order to analyse and manage risks so as to obtain the strongest protection for its assets, financial results, and consequently its capital. Although the Bank is not subject to regulation, it aims to comply in substance with the relevant EU banking directives and recommendations of the banking supervisors of the

[23] See no. 21.

EU Member States, EU legislation and the competent supranational bodies, such as Basel Committee on Banking Supervision (BCBS).

The management of risk is under the remit of Risk Management Directorate[24] (RMD), which is independent from the organisation's front offices. The RMD has, since November 2003, been structured around two departments namely, the Credit Risk Department (CRD) and Asset and Liability Management (ALM), Derivatives, Financial and Operational Risks (FRD) Department – and a Coordination Division (Figure 4.4.3). RMD independently identifies, assesses, monitors and reports the credit, market and operational risks to which the Bank is exposed in a comprehensive and consistent way and under a common approach. The Director General of RMD reports, for credit risks to the President of the Bank, and for market and operational risks to the designated Vice-President. The President and designated Vice-President meet regularly with the Audit Committee to discuss topics relating to credit, market and operational risks. They are also responsible for overseeing risk reporting to the Management Committee and the Board of Directors.

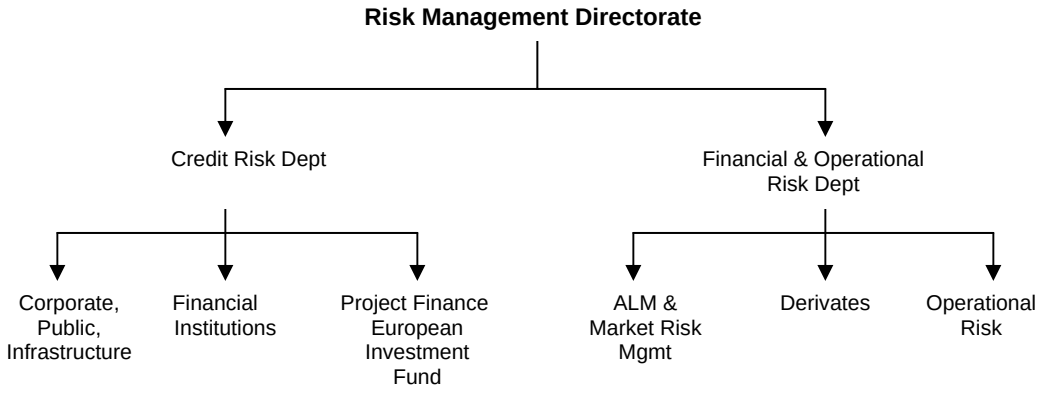

Figure 4.4.3: Risk Management Directorate of the EIB (4 May 2006).

It is important to note that the mission of the Bank is to further the objectives of the EU by providing long-term finance for specific capital projects in keeping with strict banking practice. The Bank processes approximately 30 loan applications per month. According to the head of the Operational Risk Division, although the number of

[24] Further details available at http://www.eib.org/about/index.asp?dep=143 (4 May 2006).

transactions is small in comparison to commercial banks which could reach hundreds, the value of money involved in the Bank's individual deals is much higher[25]. There is no room for any tolerance as a mistake could trigger a huge loss. A comprehensive assessment is required to determine whether or not the projects funded by the Bank have the potential to succeed. In addition, it also needs to be balanced against the Bank's strategy of taking more risk. The Operational Risk Division ensures that the decision made to fund a project must be a justifiable one as it will prolong the accountability and reputation of the Bank.

Fortunately, the smaller number of transactions means the Operational Risk Division has adequate time to assess risk associated with each potentially funded project. Mr Iglesias, who used to be an Internal Auditor for the Bank, was adamant that an effective record keeping system is essential to facilitate decision-making by his division as any delay in processing loan applications would subsequently delay the project. In the long term, this may retard the objective of the EU, particularly for much needed development in member states. Based on first hand experience, the head of the Operational Risk Division asserted that there should be no duplication of keeping records and records should not be re-created to meet the needs of various departments but the bank as a whole. In the EIB offices[26] records are stored in individual departments making sharing difficult and time consuming. The Bank, however, maintains a policy of centralised record keeping. It was anticipated that the implementation of *Gestion Électronic de Documents* / Electronic Document Management (GED) would resolve the problems of accessing records, not only for business purposes but also for risk assessment, audit and compliance in various EIB offices.

The RMD is continuously striving to improve its performance by introducing a number of changes to internal document management and additional risk management procedures including, in 2005, Credit Risk Policy updates in respect of project finance and the risk pricing and internal grading with respect to lending operations under the Investment Facility, Facility for Euro-Mediterranean Investment and Partnership

[25] During an interview on Wednesday, 26 April 2006 in Mr Antonio Roca Iglesias's office in the EIB, Hamm, Luxembourg.
[26] There are existing two buildings located in Kirchberg (headquarters) and Hamm separated approximately 18 kilometres apart. There is now a third building at Findel and multiple offices around the world.

(FEMIP) and Asia and Latin America (ALA) mandates. The Bank also created a manual, known as Financial Risk Procedure and Methodologies (FRPM), to complement the new Financial Risk and Asset and Liability Management (ALM) Policy Guidelines (FRPG) which were issued in December 2004. In conjunction with the commitment to increase transparency and compliance with relevant EU banking regulations and market 'best practices', the Bank is developing a methodology and associated guidelines to implement the Basel II Internal Rating Based (IRB) Advanced Approach for calculating the EIB's Regulatory Capital Requirements.

Apart from the RMD, the implementation of the Bank's risk policies is also supported by two risk-oriented committees. Firstly, the Credit Risk Assessment Group (CRAG) is a high-level forum for discussing relevant credit risk issues arising in the course of the Bank's activities and for advising the Management Committee on these. Its members are the Directors General of the Operations, Projects, Risk Management, Finance and Legal Affairs Directorates. The CRAG is intended to complement, and does not replace, the existing case-by-case review of lending operations, which remains central to the loan approval process.

The second committee is an ALM Committee (ALCO), which is made up of the Directors General of the Operations, Finance and Risk Management Directorates, and provides a high-level forum for debating the Bank's ALM policy and for making proposal in this field to the Management Committee. ALCO promotes and facilitates the dialogue among the Directorates represented on it, while providing a wider perspective on, and enhancing their understanding of, the main financial risks. With high commitment and orchestrated comprehensive efforts to mitigate risks, it is perceived that the Bank's aim to increase the level of transparency and compliance is within reach, though compliance and regulations are dynamic.

4.4.4 Audit Committee of the EIB

The Audit Committee is an independent body answerable directly to the Board of Governors and responsible for verifying that the operations of the Bank have been conducted and its books kept in an appropriate manner. This includes the balance sheet and profit and loss account. It reports to the Board of Governors and, at the time of approval by the Governors of the Annual Report of the Board of Directors, issues a

statement on the audits carried out. The Audit Committee is composed of three members and three observers, appointed by the Governors for a term of office of three years.[27]. The Audit Committee fulfils its role by:

- Overseeing the work performed by the external auditors and coordinating such work with that of the internal auditors
- Safeguarding the independence and integrity of the audit function and the follow-up of audit recommendations, and
- Understanding and monitoring how Management is assessing the adequacy and effectiveness of internal control systems, risk management and internal administration (EIB, 2006a).

These are done through a 'listen, ask, assess and challenge' approach without infringing the management responsibility. The approach ensures the Audit Committee functions independently and effectively whilst maintaining good working relationships with all directorates and departments. It is essential, indeed, to follow-up the implementation of recommendations made by the Audit Committee, as audit does not end when the Audit Committee report is produced. Like a risk management process, audit is also a cyclical process, which means that only the implementation of the recommendations in the due time will improve the present situation. Otherwise, it is just a waste of money and other resources used in conducting risk management processes[28]. Generally, it is the responsibility of the Management Committee to ensure the implementation of the recommendations by respective directorates or departments.

The Audit Committee is assisted by a group of internal auditors and a firm of external auditors in carrying out its task. The Audit Committee, the Management Committee and external auditors and internal auditors have mutually constructive relationships. It is the responsibility of the Management Committee to ensure that staff and resources are available, so that the Audit Committee and external auditors can be provided with any explanation requested regarding the Bank's activities and its systems and controls. The Management Committee also ensures that the Internal Audit, which is a division of the Inspectorate General, reviews all major business areas within a suitably frequent

[27] Further information available at http://www.eib.org/about/structure/dep_audit.asp (6 May 2006).
[28] Further discussion on risk management is available in *Section 2.7 Risk Management and Managing Records*.

time period (based on independent risk assessments) by the RMD. However, the Management Committee usually consults the Audit Committee before deciding the Internal Audit's forward programme. The Internal Audit produces independent reports on its findings and also follows up the implementation of agreed action (to matters raised during both the internal and external audit processes). All its reports go to the Audit Committee at the same time as they go to EIB management.

The efficiency and effectiveness of the Audit Committee is partly complimented by the Inspectorate General, the Chief of Compliance Office and the RMD, through regular meetings. The Inspectorate General was established in 2005, is an autonomous department that combines Internal Audit and Operations Evaluation, the two main independent *ex post* control functions. The Internal Audit and Operations Evaluation continue to function independently, but the new structure makes it possible to exploit synergies and to develop a more coordinated approach to their respective work programmes. This reflects a comprehensive effort of evaluation activities to the attainment of the Bank's strategic objectives and their impact on operational performance, accountability and transparency. The Internal Audit keeps a constant eye on internal control systems and the procedures involved. Meanwhile, the Operational Evaluation carries out *ex post* evaluations of a representative sample of the completed projects and programmes financed by the Bank.

Internal Audit relies heavily on the availability and reliability of documents and records in both electronic and physical forms. In an interview with one of the internal auditors admits that good record keeping systems, particularly after the implementation of the Integrated Strategic Information System (ISIS), facilitates internal auditors' tasks as they do not need to be personally present in the department to perform their auditing tasks[29]. Information is gathered online, which means assessment can be conducted in their office, and visits to relevant departments only made when necessary. So far, the internal auditor has not experienced any serious obstacles in finding records for audit purposes. The implementation of GED is very much appreciated as it helps internal auditors to do their job.

[29] An interview was conducted on Thursday, 27 April 2006, in Mr Lemak's office, the EIB, Kirchberg. He has now left the Bank.

It is essential to note that in line with the commitment of the Bank to increase the level of transparency and compliance, the role of audit is no longer limited to all directorates and departments only, but has been extended to the functioning of the Bank's Governing Bodies, which was initiated by the President of the Bank in 2002. This is certainly welcome by many as high profile corporate failures, such as Enron and WorldCom, have shown that the collapse was caused by irresponsible and unethical gatekeepers, particularly the external auditor and the board of directors. It is unimaginable for such a huge public financial institution as the EIB to collapse as a result of similar irregularities, as the consequences would be catastrophic for the EU and its financial institutions. Hence, to prevent is better than to cure.

4.4.5 Records Management in the EIB

Managing records and archives of the EIB falls under the remit of the Buildings, Logistic and Documentation Department, Documentation and Records Management Division (DRM)[30]. There are two subdivisions in the DRM namely, the Records and Management Unit (RMU), and the Library. *Gestion Électronic de Documents* / Electronic Document Management (GED) Unit, is now belongs to another division[31]. Since the implementation of ISIS, GED has had a major role in providing a reliable document management system to users across the Bank.

4.4.5.1 Records Management Unit

The RMU is responsible for managing archives and conventional records. Murdock (2006b) explains that the Archives Services of the EIB comprise almost 9 linear kilometres of records, representing the Bank's operational and administrative history since 1958. It includes details of almost 13,000 lending projects many of which have 30 year project life-cycles. Almost 55,000 documents related to active projects arrive each year with the operational archive teams. In addition, approximately 400LM of semi-active records arrive for 'records management' storage. There are twelve people in the RMU ensuring smooth operations. The responsibility of the RMU does not end there as it also involved in the GED project, which is an enterprise-wide document management project.

[30] There have been dramatic changes of governance structure since the visit on 26-27 April 2006. Managing records and archives used to be under the remit of Communication and Information Department (CID), headed by Mr Eric van der Elst. He has now left the Bank.
[31] GED and RMU used to be sub-division of CID.

4.4.5.2 GED Unit

It is essential to note that the experience of the GED project team in developing the system may provide guidelines for developing future integrated document or records management systems. The GED project is not only about document management systems, but it also about the governance of the project. The history of GED began in December 2002, when the EIB management committee approved a huge IT re-engineering programme to replace all legacy systems, some of which were installed more than fifteen years ago, with an integrated EIB-wide system with a reduced number of applications and interfaces.

The programme called Integrated Strategic Information System (ISIS) with three-year implementation plan, with the majority of ISIS projects drawing to close in 2004 and overall completion scheduled in mid-2005 (ERPANET[32], 2004). ISIS covers the entire information structure at the EIB except e-mail, including the bank's processes with records of borrowing, lending and administration. There are four application systems in the ISIS namely, GED, which was meant to be the back bone of the ISIS; RE – a system for borrowing, treasury and back-office loans; *Système Efficace et Rapide d'Accèss aux Prêts et Informations de Support*[33] (SERAPIS) – a system for front office loans and; OSIRIS – an administration system[34] *(Figure 4.4.5.2: The ISIS programme)*.

Since GED is a transversal project, therefore, it must be able to integrate with the three other systems (RE, SERAPIS and OSIRIS). It was developed to serve both the ISIS and the Bank. The GED means all important documents in the Bank created, modified, signed, stored, indexed and available in structured folders. This is not an easy task considering the size of the Bank, the complexity of the business and the relatively limited time frame allocated for the project to accomplish. The GED was developed based on analysis of record keeping models and standards namely DIRKS, MoReq, ISO 15489, Dublin Core and thesaurus, which were locally developed. Within the ISIS, the GED should be able to:

- Perform all document management tasks

[32] Electronic Resource Preservation and Access Network (ERPANET). Further information available at http://www.erpanet.org
[33] English equivalent: Access system for loans and background information.
[34] Other applications namely PIC (reference database), LDAP and EAI are not parts of ISIS.

- Provide flexibility to ISIS by managing exceptions to workflows
- Enforce single classification throughout ISIS and the Bank.

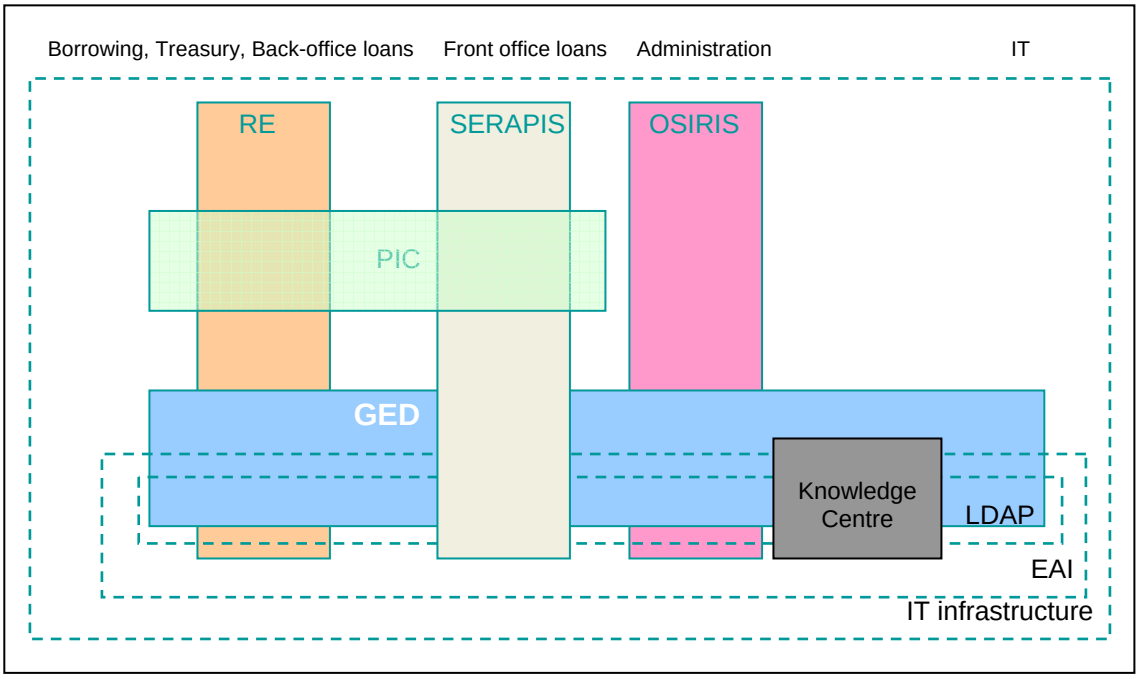

Figure 4.4.5.2: The ISIS programme

In the Bank context, the GED should be able to:

- In the short term, replace document circulation (paper or e-mail) by direct access to electronic information – has been successfully implemented.
- In the medium term, reinforce sound record-keeping practice by securing authentic records – in its infancy stage as few changes are being made to suit demanding users needs.
- In the long term, create and structure the Bank's experience as a key component of EIB added value – in its infancy stage.

The GED has three workspaces namely:

- Working area – is a collaborative workspace where people can alter documents according to their privileges. Unfortunately, after being implemented it is under utilised. The contributing factor was users are reluctant to share information

although they have been made aware that every document or record is not their personal property. Documents created will be saved in a designated unit or a divisional working area, and made available for other staff members within the unit or division. Users are allowed to access and modify documents, including documents created by others. There is an issue of the safety of documents as accidental or deliberate modification or deletion of documents can occur, which in turn may affect the efficiency of the Bank as a whole. To this end, it is important to note that the management of the Bank is very concerned that the Staff Code of Conduct ensures every member of the Bank acts responsibly.

- Knowledge Centre – was intended as a referral centre for all EIB staff. Complete documents from working areas will be transferred into the Knowledge Centre for permanent storage. In this stage, documents are accessible but no longer editable.
- Institutional workspace – was intended for administrative documents, restricted to organisational structure. Shared drives were migrated into these areas.

A GED project committee was formed to undertake the development of the GED system. The project committee or team comprised representatives from few departments including the IT Department, Information and Communication Department and Library and Information Department. It was headed by a representative from Library and Information Department [35]. When the GED project was officially closed in April 2004, the project team was also disbandoned. To this end, the responsibility was transferred to DRM Division, GED Functional Unit. Other team members returned to their respective departments. The GED system was initially promoted as very beneficial enterprise-wide project for all. Unfortunately, when the ISIS project was accomplished, the GED failed to impress all members of the Bank. All the interviewees admitted that probably excessive promotion of the GED system led to high expectation from users. They were also in agreement that they were overjoyed that eventually they were given a massive opportunity to develop a comprehensive tailor-made document and records management system.

[35] It was unfortunate that the Project Head was forced to take an early retirement due to health condition. Unplanned departure of project leader resulted in disruption of project timescales.

Indeed, as the Audit Committee (2006) noted the Bank experienced a number of problems during the implementation of a new ISIS application (for borrowings - RE) in July 2005. A recent external audit requested by the Audit Committee on ISIS has been very favourable to GED. As a consequence, the implementation of RE and another system, OSIRIS, has been delayed. Arguably, it was an ambitious project considering the scale of the ISIS and the time frame allocated within two to two and half years. The GED project started in May 2002 and was officially accomplished in April 2004. There were four phases within this period, namely:

- Design and Procurement (IT and Classification): May 2002 – December 2002
- Configuration: December 2002 – September 2003
- Connecting and training users: September 2003 – January 2004
- Legacy migration and populating with documents: January 2004 – April 2004

Records management tasks started in the middle of the first phase until the end of the project. Backlog scanning started in the third phase until the end of the project. Ms Hoffmann (2006) admits that the integration of the GED with SERAPIS was far more complicated than expected by the project team phase 2. The GED is a brand new system using Livelink software as its platform meanwhile, SERAPIS is an upgraded version of existing in-house system. Apart from that, the integration was made whilst both systems were being developed and re-developed. As a result, the process of bridging the GED and SERAPIS did not go on as scheduled.

Another contributing factor was the governance of the GED project. The project demonstrated the importance of managing and directing consultants successfully as a key component of project management. With hindsight, several consultants came in and out without delivering meaningful progress to the project. These wasted the already limited time frame given to accomplish the project. There were situations where consultants asked the GED project team for suggestions rather than themselves provide to the team. Mr Murdock asserts that the GED project team must be certain about what they want from a consultant, which in turn should provide solutions to the team.

Despite its official termination there is another phase yet to be completed in the GED project life cycle. Post implementation review is a stage after the completion of a

project which functions to highlight issues faced and provide recommendations for downstream corrections and to serve as a learning tool for the future (ISACA, 2003). At the moment, the GED system is undergoing a fine tuning stage including the modification of folder structures and file naming conventions to suit ever expanding and demanding user's needs across the Bank. The file name structure and naming conventions were initially developed based on business functions, through collaboration with all individual business units within the Bank. Ironically, it was discovered that users are not satisfied with the implementation. To this end, post-implementation modification is inevitable.

Apart from existing templates for workgroups, the new approach provides a more flexible naming convention according to business activities and it also allows the creation of new folders depending on the needs (*See appendix 1*). Johnston (2006) asserts that a functional system is not easy to build, but it is possible. He went on that a functional scheme cannot be imposed on or built for an organisation, instead it can only be built within an organisation. In other words, it means that naming convention must be based on functions that people recognise; words that are meaningful to people; and vocabulary that people understand. Then users will use the classification scheme as they have been involved in its creation and it makes sense to them. Ownerships and meaningfulness are great levers to use in change management.

Consistent with the findings of the Electronic Records Management Project by Humanities Advanced Technology and Information Institute (HATII) (Currall *et al*, 2002), the GED Functional Unit also discovered that it is difficult to attain commitment from records creators to fulfil required record keeping metadata in templates provided. Many of them sent their electronic documents to the GED Unit to complete remaining required metadata fields. To this end, automatic metadata capturing is desirable to facilitate subsequent record keeping activities. However, this seems to be unrealistic as the cost is prohibitive. The problem can gradually be resolved by providing continuous training to secretarial staff of each business unit as they are heavily involved in the creation and filing of records. Furthermore, they are gate keepers who ensure incoming and outgoing records and documents possess adequate metadata.

The GED system will also be equipped with records retention schedules to enhance the management of electronic records. The idea of integrating risk and records management has attracted the Inspector General, as he believes that managing records is not about keeping everything[36]. Keeping and destroying records must be based on risk analysis to ensure the Bank operates within anticipated risk boundaries. Decisions and actions must be justifiable as the call for transparency is constantly high. At the moment, records retention schedules are being developed, however, they are not so far integrated as when the task started the RMD was yet to be established. Responsibility for retention schedules remains with RMU and not RMD. The RMD was only established in November 2003, when the GED system was in the third phase. Hence, it was not possible for the GED project team to adopt input from the RMD. It would have been very beneficial for the project team in particular and the Bank in general, if the RMD had been established much earlier as it would provide reliable inputs for the RMU for developing records retention schedules.

Integrating records retention schedules requires considerable effort for the development of retention schedules and supporting technologies. Assigning retention periods requires detailed information on various aspects including business needs, legal and compliance requirements as well as historical value. It is certainly beyond the capability of the RMU to decide for how long a particular record should be kept. Therefore inputs from the RMD, Legal Department and the Compliance Office are vital for the RMU for developing functional retention schedules. In the first case study, at Standard Life Assurance Group Plc, it was discovered that an integrated records retention schedule is more convincing and reputable as it specifically identifies the types and level of risk, the departmental current position, and provides recommendations to mitigate risks for every business department.

The Bank will enjoy further benefits if integrated records retention schedules can be embedded with the GED, hence ensuring the consistency and efficiency of the GED operation. The GED system can be enhanced by including digital preservation features for the purpose of ensuring the longevity of digital records. Despite awareness of the importance of digital preservations, the GED Unit has to focus on improving key

[36] During a lunch meeting also attended by Mr Murdock and later joined by Mr Eric van der Elst, Head of Division, DRM and Mr Ciaran Hollywood, Head Internal Auditors.

features of the system to meet user's expectations and business needs, which they failed to achieve when the GED was officially completed. Currently, there is no systemic effort taken to preserve digital records. The notion of digital preservation may not be of similar meaning and importance to IT professionals as opposed to archive and records management professionals. The former is more concerned with ensuring availability and accessibility, whilst the later is more concerned with maintaining authenticity and integrity of digital records. An interview with a member of IT Department staff reflects the difference[37]. Records have to retain their original elements to be reliable evidence as they were initially created and used. The integrity of a record refers to its wholeness and soundness: a record has integrity when it is complete and uncorrupted in all of its essential respects. This does not mean that the record must be precisely the same as it was when first created for its integrity to exist and be demonstrated (InterPARES, 2001). These issues were discussed in *Section 2.8.4 Authenticity and Integrity of Records*.

Constrained by limited human resources in comparison to the development stage of the system, it is understandable that the GED is concentrating on improving existing applications whilst digital preservation remains as an area of high priority. Considering the hard working of the GED Unit and existing good relationships with the RMD, Inspectorate General and the Compliance Office it is perceived the GED system will reach stability in the near future. Indeed, the GED system has reached stability when this thesis was about to accomplish.

4.4.6 Discussion on Research Objectives in the EIB

Following is discussion on the case study in the EIB, in line with the research objectives.

4.4.6.1 Records Management and the Governance of the EIB

Despite its European Union public organisation status with legal immunity, the President of the Bank believes the Bank has to increase the level of transparency and

[37] Although Mr Patrick heavily involves at operational level, his views on digital preservation was consistent with general assumption that IT professionals are more concerned with the accessibility, but less concerned with the integrity of digital records. To this end, a working collaboration between the two professions is vital to ensure the needs of record keeping can be fulfilled by technologies.

accountability in order to sustain its reputation in a risky and competitive financial services sector. The President decided the Bank has to comply with Basel II convention in order to demonstrate accountability of governance and be transparent to its shareholders and stakeholders. It is hard to demonstrate accountability and transparency if there is no benchmark. Hence, conforming to Basel II convention facilitates the Bank in identifying specific requirements that enable transparency and accountability of governance.

Although the Bank is governed by four bodies namely, the Board of Governors, Board of Directors, Management Committee and Audit Committee, it continues to operate efficiently and effectively. This is mainly a consequence of its clear governance structure and delegation of responsibility to these bodies and seamlessly to their subordinates. The President of the Bank was certainly aware that having an effective record keeping system is fundamental for the operation of the Bank as it also ensures the evidence of the Bank operations will be managed systematically. In any organisation, there is no better person other than the head of the organisation itself to show concern about records management condition in the organisation.

It was therefore not a surprise when he allocated a huge fund to develop an organisational-wide integrated strategic information system or ISIS, of which records management functions or GED is a key component. From the records management perspective, the President of the Bank was a true records management champion. A direct consequence of his commitment was the development of ISIS and particularly the GED, did not encounter managerial interference. This proves that involvement of senior management is crucial for the success of a records management initiative. Records managers in other organisations may not be so fortunate enough in securing commitment from senior management.

Making the GED the key components of the organisational-wide integrated information system endorses the key role of documents and records in underpinning the governance of the Bank. Arguably, this should not be limited to financial institutions but applied in all types of organisations as managing documents and records is also managing the evidence that is a pre-requisite for good governance.

4.4.6.2 The Role of Records in the Accountability Processes in the EIB

Accountability and transparency constitute one of two pillars of the Bank's strategy. The other is value-added. The Bank believes that in order to generate more surplus, it has to generate more value-added and take more risk. As a publicly owned bank, it has to attain a high level of transparency, thereby showing value of its operational performance. Accountability can only be achieved with the presence of authentic, accurate and up-to-date records or evidence. The accountability of the Bank operations is ensured by its Audit Committee and Compliance Office.

The Audit Committee is an independent body that is directly answerable to the Board of Governors. The Audit Committee verifies that the operations of the Bank have been conducted and its books are kept in an appropriate manner, which includes the balance sheet and profit and loss account. Meanwhile, the Compliance Office ensures the compliance risk of the Bank. In the EIB context, accountability is not limited to financial management but embraces non-financial management as well. There were regular meetings between the Audit Committee, Compliance Office and RMD to streamline information for transparency and accountability purposes.

Although the Documentation and Records Management Division was not directly involved in the meeting, its critical role in ensuring the availability of records of and for the three entities cannot be denied. Notwithstanding that the ISIS and GED are in place, together with a new Document and Records Management policy approved by the Management Committee in 2006, the trustworthiness and evidential value of authentic, reliable and usable records as proof of business activities is assured. Since accountability embraces every aspect of the Bank operations, the development of the organisation-wide ISIS says everything about the Bank commitment to increase the level of transparency and accountability of its performance. This helps the Bank to gain trust from its shareholders, stakeholders as well as members of the public. Arguably the decision by the President of Bank was a wise one as having sound information and records management systems enables accountability (Willis, 2005).

With three workspaces namely, Working Area, Knowledge Centre and Institutional Workspace, the GED plays a vital role in ensuring the trustworthiness and authenticity of documents and records. Initially, the GED was under utilised due to a less functional

newly introduced folder structure and naming convention despite consultation with users. The unexpected outcome forced the Records Management Unit to conduct post implementation review to find a solution, so that the GED would not be a white elephant project. As a result a more flexible naming convention according to business needs was established. This led to a better acceptance and utilisation of the GED by users. Indeed the experience of developing and implementing the GED presents a lesson to learn. The governance of an automated record keeping system is not easy but challenging enough particularly, to meet user's needs that are changeable from time to time.

The authenticity and trustworthiness of records which is central to accountability is protected as documents were transferred from Working Area into the Knowledge Centre. Control mechanisms are embedded in the system, therefore the authenticity of records is guaranteed. Authentic and reliable records provide an unambiguous link between contextual information that serve as evidence to identify abuse, non-compliance and mal-administration. Audit trails provide a reliable source of information whenever an investigation is necessary. Obviously, the Bank has all it needs to implement an effective and efficient record keeping system. They are the new document and records management policy, the new organisational-wide strategic records and information system and critically the full support from the President of the Bank. With these elements in place, it is perceived that the Bank can increase the level of transparency and accountability as expected because the core requirement that is sound record keeping system.

4.4.6.3 The Relationship between Risk Management and Managing Records in the EIB

At present, the collaboration between the RMD and RMU is not explicit. Apparently risk management and records management are two separate functions that do not communicate effectively between each other. Perhaps this is partly caused by the specific function of the RMD that is to identify, assess, monitor and report the credit, market and operational risks. Meanwhile, the RMU functions to manage archives and conventional records. Although the RMD and RMU are geographically separated about 18 kilometres apart it should not be a constraint on the potential integration of risk and records management because it is borderless in an electronic environment.

Since the ISIS and GED already are being used, in-depth analysis is required to integrate risk and records management. This is because modifying existing systems is more difficult than developing new ones. Although the GED was developed using DIRKS, which considers risks in designing the system, it is inadequate to enable immediate integration of risk management into the existing system. Input from a reliable source, in this instance the RMD, is crucial to add-value to the existing ISIS. The process of integrating the two areas is perceived not complicated and costly due to the flexibility of the GED and the requirements that need to be embedded into the system are not complicated. What is needed is input, such as the types, likelihood and impact of risks, from the RMD to be attached to pertinent record categories. This will enable a more systematic identification of risk exposed to different type records and in turn to the Bank.

It is worth noting that this is not about minimising risk but about enabling the Bank to take opportunities while being certain about associated risk. Arguably, this can also change the perception that the management of records is not costly as many might suggest. While the role of the RMD is crucial as it provides information on both financial and operational risk, the importance of the Compliance Office and the Audit Committee to the existence of the RMU can not be neglected. Indeed, it is a symbiotic relationship between all the entities that would benefit the Bank as a whole.

The Inspectorate General was convinced about the benefit of integrating risk and records management. It is hoped that his concern and influence would enable and facilitate the integration of the two areas. As the first case study in the Standard Life proved the organisation is enjoying the benefit of the integration of risk and records management, it is perceived that the Bank will adopt a similar approach in the future. Notwithstanding the existing organisational-wide ISIS, of which the GED is the backbone, the initiative to implement the integrated approach would not take long to implement. This would help achieving the aim of the President of the Bank to increase the level of transparency and accountability of the organisation.

4.5 NHS Greater Glasgow and Clyde Board

4.5.1 Background

The UK's National Health Service was set up in 1948. It is now the largest organisation in Europe and recognised as one of the best health services in the world by the World Health Organisation[38]. The role of the NHS is to make sure that every one who is entitled to treatment has access to services and treatments that will help them avoid, survive or cope with ill-health and to promote healthy behaviour. The NHS in Scotland is a large and complex organisation but is essentially organised into two tiers. Scottish Ministers through the Scottish Executive Health Department (SEHD) are responsible for national policy, direction and funding of all NHS Boards across Scotland. In the meantime, NHS Boards are responsible for local health planning and improvement and for the delivery of hospital, community and primary care services consistent with the national framework and policy.

There were 15 NHS Boards, however, Argyll and Clyde Health Board was dissolved on 31 March 2006 and split into two, leaving only 14 NHS Boards including the newly re-drawn NHS Greater Glasgow and Clyde Health Board and NHS Highland[39]. The NHS Argyll and Clyde consistently overspent and was dissolved by Scottish Ministers. In order to strengthen healthcare services Community Health Partnerships[40] (CHPs) have been set up play a central role in reshaping local community and primary care health services across Scotland. CHPs are expected to operate within NHS Boards' policy, planning and performance management arrangements, standing financial orders, audit and risk management systems, and ensure actual expenditure is monitored against budget, and corrective action taken if necessary. There are also eight Special Health

[38] http://www.nhsgg.org.uk/content/default.asp?page=s779 (22 June 2007).

[39] NHS Argyll and Clyde was dissolved and merged with two other Health Boards namely, NHS Highland and NHS Greater Glasgow. Other NHS Boards are Ayrshire & Arran, Borders, Dumfries & Galloway, Fife, Forth Valley, Grampian, Highland, Lanarkshire, Lothian, Orkney, Shetland, Tayside and Western Isles. At the end of 2005/06, NHS Argyll and Clyde received £82.3 million form the SEHD to write off its £81.7 million cumulative deficit (Audit Scotland, 2006).

[40] CHPs, also known as Community Healthcare Partnerships (CHCPs), were proposed in Partnership for Care and introduced on a statutory basis by The National Health Service Reform (Scotland) Act 2004. They are not independent statutory bodies, but are committees or sub-committees of a health board. The original implementation date for CHPs was from April 2005, although some were operating in shadow form prior to that date. More information about CHPs and their schemes can be found at: http://www.show.scot.nhs.uk/sehd/chp/ (18 September 2006).

Boards that provide services on a national basis[41]. The SEHD is headed by the Chief Executive of NHS Scotland, who is directly accountable to the Scottish Parliament for financial propriety and regularity, and for achieving best value from the resources allocated to SEHD and NHS Scotland[42].

An NHS Board is a body corporate consisting of a Chair appointed by the Scottish Ministers and such numbers of other appointed members as the Scottish Ministers think fit. NHS Boards manage their day-to-day affairs without detailed oversight from Ministers and SEHD but they are accountable to Ministers and SEHD for the financial and operational performance of the local NHS system. NHS Boards are primarily responsible for the protection and improvement of the health of their population; the delivery of hospital, community and primary care services; for developing a local health plan which addresses the health priorities and health care needs of the population; for allocating resources to address local priorities in accordance with a Board's strategic objectives and the performance management of the local health system.

The establishment of CHPs requires NHS Boards to devolve key areas of responsibility and large amount of resources to their CHPs. Critical to this is the need for sound governance arrangements to be in place to support CHPs in doing the job expected of them, and to ensure that they use their resources properly and to good effect[43]. Putting governance arrangements in place is not easy as it needs to be clear who is responsible for what, and all partners need to be signed up to this. The absence of sound governance arrangements will subsequently lead to the danger of poor record keeping, confusion and weak accountability.

Audit Scotland foresees joint working between NHS Boards and local authorities as possibly difficult to manage because working across organisational boundaries is complex and can involve significant risks. This suggests that the implementation of a

[41] Special Health Boards are NHS Quality Improvement Scotland, NHS Health Scotland, NHS Education for Scotland, Common Services Agency, Golden Jubilee National Hospital, Scottish Ambulance Service, State Hospital and NHS 24.
[42] NHS Greater Glasgow Freedom of Information (Scotland) Act 2002: Publication Scheme. Available at: http://www.nhsgg.org.uk/foi/publicationscheme (25 January 2006).
[43] How the NHS Works: Governance in Community Health Partnerships – Self Assessment Tool. Audit Scotland, May 2006. Available at: http://www.audit-scotland.gov.uk/publications/pdf/2006/HNHSWorks_Governance.pdf (21 September 2006).

single system can only succeed if there are clear accountability lines supported by consistent record keeping systems. In the case of the NHSGGC, this is far from easy particularly when it involves joint partnerships with Glasgow City Council Social Work Department (SWD) and East Renfrewshire Council Social Work Department. These have been established as CHPs and they are organisations brought together from two legal entities to deliver local health and social care to their population set against a joint accountability framework.

The NHSGGC Archivist and Records Manager, Mr. Alistair Tough, asserts that it is very difficult to have a single record keeping system as there is a fundamental conflict between the two sectors. Mr. Tough went on to say that the NHS has a long-established policy of retaining and re-purposing key data elements from patient record keeping systems whilst social workers are not accustomed to this. The NHS also uses a centralised Information Services Division to receive and process summary data in respect of all hospital in-patient episodes. The data elements retained include the patients' names, addresses and NHS numbers, so record linkage is possible.

Data has been gathered in this way since the late 1950s, and no retention or disposal schedule applies. On the contrary, the SWD does not retain summary data, whereby once a client file is due to be disposed of, according to approved retention schedules, the file is destroyed and no pre-designed summary of its content is left. This is done to protect the confidentiality of clients and has the effect of preventing litigation[44]. Consequently, however, when there is a necessity, the NHSGGC cannot compile comprehensive information about a patient that is crucial in facilitating health care services.

4.5.2 Governance of the NHSGGC

The newly re-constituted NHSGGC is the largest NHS Board in Scotland employing over 44,000 staff and the largest public sector employer in Scotland (NHSGGC, 2006a). The general health of the people of the West of Scotland is the poorest in Scotland and therefore the workforce of NHSGGC, while delivering services to patients, has to concentrate on tackling health inequalities and health improvement. In order to ensure efficient healthcare service to the public, the NHSGGC work together with

[44] In a discussion on 19 December 2006, in HATII, University of Glasgow.

partners, local authorities and other agencies, public, private and voluntary to provide a full range of healthcare to 1,196,335 people living in:

i. The City of Glasgow
ii. East Dunbartonshire (Milngavie, Bishopbriggs, Kirkintilloch)
iii. West Dunbartonshire (Clydebank and Dumbarton)
iv. Inverclyde
v. North Lanarkshire - part (Stepps - Moodiesburn corridor)
vi. South Lanarkshire - part (Rutherglen and Cambuslang)
vii. Renfrewshire
viii. East Renfrewshire (Eastwood)

Previously known as NHSGG, it had four divisions, namely North Glasgow University Hospitals Division, South Glasgow University Hospitals Division, Primary Care Division and Yorkhill Division (which replicated the four former NHS Trusts which were dissolved in 2004). However, the move into a Single System Organisation in accordance with the 'Partnership for Care: Scotland's Health White Paper' has involved the dissolution of individual Divisions, the creation of one Greater Glasgow wide Acute Division and the formation of ten CHCPs and a Mental Health Partnership.

The external auditors for the NHSGGC, PricewaterhouseCoopers, state that the reorganisation was not only about major structural change – shifting from four NHS divisions and sixteen Local Health Care Co-operatives[45] (LHCCs) into a single acute division and partnership arrangements for mental health, primary care and community services – but also about transforming ways of working, including the integration of health and social care services, breaking down barriers between primary and secondary care, delivering services across Greater Glasgow and putting health improvement at the centre of the NHS.

The restructuring process is being driven forward directly as a result of 'Partnership for Care' which clearly directs the Health Board to:

[45] In Scotland, Local Health Care Co-operatives are voluntary groupings of GPs and other local healthcare professionals intended to strengthen and support the primary health care team in delivering local care.

- Make better use of resources to improve services for patients
- Devolve decision-making to a local level
- Increase consistency and equity of access
- Reduce duplication

Given the size of the NHSGGC, there is, however, a huge potential of incompatibility between devolving decision-making to a local level and increasing consistency and equity of access, unless there is good governance across the Board. Governance is about making sure decisions are made in a clear and appropriate way to assure the Scottish Executive and the communities served that public money is properly accounted for and that the care being delivered is to nationally set or locally agreed standards.

The current models of care are not delivering the improvements in healthcare services and have failed to match the public expectations[46]. The Board believes that restructuring will radically change the approach and decentralise healthcare in the broadest possible terms and create new CHPs that are bigger organisations with greater responsibilities and influence to drive forward local priorities and develop stronger links with a new single acute hospital operational unit. The Board is attempting to turn the rhetoric of patient-centred care into reality by putting an end to the old style of working where people had to fit into the services rather than the services fitting around them.

The governance of NHSGGC Board is headed by a Chairman. The Board are accountable to SEHD. Currently the NHSGGC Board also comprises a Chief Executive Officer, 4 executive directors and 26 non-executive directors[47]. Non-executive directors should constructively challenge and contribute to the development of strategy and should satisfy themselves that financial information is accurate and that financial controls and systems of risk management are robust and defensible. Effective boards need to display high levels of trust and challenge (Higgs, 2003). The large number of members of the Board raises concern about their collective efficiency and roles,

[46] Information of the reorganisation of the NHS in Greater Glasgow available at: http://www.nhsgg.org.uk/content/default.asp?page=home_reorganisation (1 February 2006).
[47] http://www.nhsgg.org.uk/content/default.asp?page=s108 (15 September 2006).

particularly of non-executive directors contrary to the recommendation of the Higgs Report. Board meetings are normally held bi-monthly on 3rd Tuesday of the month. The Board members are bound to the Ethical Standard in Public Life etc. (Scotland) Act 2000, which provides a new Code of Conduct for local authority councillors and members of relevant public bodies. Members are responsible for ensuring that they are familiar with, and that their actions comply with, the provision of this Code of Conduct. The NHSGGC Board are responsible for setting the strategic direction for health improvement/care against a governance framework which is designed to ensure probity and transparency for the decision making process.

The following are categories of responsibilities of the Board, namely:

I. Strategy for Health Improvement
   i. Improving the health of population
   ii. Strategic development and direction
   iii. Development and implementation of the Local Health Plan
   iv. Performance management of NHSGGC through Performance Assessment Framework (including areas like monitoring waiting time targets and handling of complaints).
   v. Accountability review process
   vi. Public involvement

II. Governance
   i. Resource allocation and financial monitoring (for both capital and revenue resource allocation)
   ii. Approval of annual accounts
   iii. Scrutiny of public private partnership
   iv. Appointment of directors
   v. NHS statutory approvals
   vi. Corporate governance framework including
      - Standing orders
      - Establishment, remit and reporting arrangements of all Board Committees and Subcommittees
      - Standing financial instructions and scheme of delegation

There are 19 Standing Committees in the NHSGGC Board, namely:

i. Public Involvement Committee
ii. Family Health Service (FHS) Disciplinary Committees
iii. Staff Governance
iv. Clinical Governance
v. Audit
vi. Research Ethics Governance
vii. Service Redesign
viii. Area Clinical Forum
ix. Performance Review Group
x. Pharmacy Practice Committee
xi. Community Health (Care) Partnerships - 10
xii. Mental Health Partnership

Each Standing Committee is headed by board member or a Councillor.

It is essential to note that the research focuses mainly on the operation of the Board Headquarters of the NHSGGC located in the Glasgow City Centre. Two visits were conducted to the Southern General Hospital and one visit to the Gartnavel Royal Hospital to meet relevant officials. As a result of the initial move to a single system in April 2004, the four Glasgow NHS Trusts transferred their functions, staff and assets to new operating Divisions of the NHSGG Board (PricewaterhouseCoopers, 2006). The Board aimed to accomplish the process within two years, however it was considered ambitious by the NHS Quality Improvement Scotland (NHS QIS, 2005b) given the size and complexity of the Board.

Indeed, the inclusion of Clyde into NHSGG in April 2006, has affected the re-structuring of governance and strategies in establishing a single system working. As a result of the integration, the Board foresees, among other issues, significant financial consequences resulting from redeployment and possible redundancies, significant costs of integration, including information technology, legal and other related costs, issues in relation to the impact of the new Mental Health Act which will enable patients to mount legal

challenges, and a number of key primary care premises developments have additional revenue costs not fully covered in the financial plan.

The NHSGGC annual review for its financial year ended 31 March 2006 indicates that all financial targets were delivered, as well as securing balanced investment across main programmes (NHSGGC, 2006a). Being the biggest public organisation in Scotland, the governance of NHSGGC requires detailed planning, control and monitoring to ensure its strategic direction falls within the parameters laid down by the SEHD's policies, providing leadership, setting the tone for the whole organisation, overseeing the control of the Board's work and reporting activities and progress to stakeholders. NHSGGC board members are, therefore, collectively responsible for the success of the organisation. The main acts governing the NHS in Scotland are currently:

i. The National Health Service (Scotland) Act 1947
ii. The National Health Service (Scotland) Act 1972
iii. The National Health Service (Scotland) Act 1978
iv. The National Health Service and Community Care Act 1990
v. The National Health Service (Primary Care) Act 1997
vi. The Health Act 1999
vii. The Community Care and Health (Scotland) Act 2002
viii. The Mental Health Care (Care and Treatment) (Scotland) Act 2003
ix. The National Health Service Reform (Scotland) Act 2004. (Mackie, 2005)

Apart from these healthcare specific acts, NHSGGC like other public organisations also operates under Data Protection Act (1998) and Freedom of Information (Scotland) Act 2002.

Governance within the NHSGGC can be considered under 4 main headings (Table 4.5.2), namely:

Financial and Performance Governance	The proper management of resources and a sound financial standing will enable the organisation to achieve its aims and objectives to meet its obligations as and when they fall due.
Clinical Governance	The Board should have an established clinical governance framework which supports and monitors standards for care, creates an environment for the continuous improvement of services, supports strategic planning and facilitates service delivery.
Risk Management	Responsibility is placed on the Board and primarily the Accountable Officer in the Statement of Internal Control to maintain a sound system of internal control and comply with all applicable laws and regulations.
Staff Governance	NHSGGC as employers are expected to have a system in place to identify areas that require improvement and to develop action plans that describe how improvements will be made. The underlying principle is that NHSGGC Board should recognise that investing in staff will allow them to deliver services to the best of their ability in modern healthcare settings (NHSGGC, 2006a).

Table 4.5.2: The governance structure of the NHSGGC.

Understandably, the aim of establishing a single system was to remove organisational barriers and to establish shared aims and lines of accountability across NHS board areas (Audit Scotland, 2006). In its Audit 2005/06 report, PricewaterhouseCoopers states that given the scale and the complexity of the governance and management arrangements that existed before 1 April 2004, it was recognised that attaining a single system solution would be difficult to achieve. This is consistent with the Audit

Scotland's view that foresees the potential problems of having a single system of working. As a consequence, the Board decided to adopt a two-year staged approach to single system working that included the operation of transitional governance arrangements prior to full implementation. The restructuring of NHSGG and integration of part of the former NHS Argyll and Clyde has direct consequences for the existing committee structure, particularly the main governance Committees – Audit, Clinical and Staff Governance Committees. For example, apart from financial reports, the Audit Committee will also receive and consider reports which cover strategic issues and recognised areas of risk. Discussion of audit committees is provided in the subsequent section and also in *Section 2.8.3 Audit and Internal Controls*.

Financial and performance governance requires effective financial planning and strategy, financial control, and through maximising value for money to achieve high standards of financial stewardship. The financial position of the NHS in Scotland has moved from overall overspend of £32 million in 2004/05 to an overall under spend of £70.6 million against the health budget for 2005/06, saved by under spend of capital (Audit Scotland, 2006). The situation is worse in England, when a study by a Select Committee of Members of Parliament found mismanagement at all levels of the NHS in England has led to current multimillion pound deficit[48]. These include the most basic errors, such as inadequate monitoring and an absence of financial control.

A good financial and performance governance framework should enable Board members to make formal decisions about every conceivable financial impact with knowledge and confidence. The management of the NHSGGC has established a Finance Transitional Overview Group, chaired by the Director of Finance, and supported by three sub-groups representing Corporate (the Board), Partnerships and Acute Services. The objectives of these sub-groups was to convert the current geographically based financial reporting and monitoring structure to a new functional divisional basis to match the revised NHSGGC structure on the 1 April 2006 (PricewaterhouseCoopers, 2005). The remit of the Clinical Governance Committee has

[48] Health Select Committee is appointed by the House of Commons to examine the expenditure, administration and policy of the Department of Health and its associated bodies. Further information available at: http://www.parliament.uk/parliamentary_committees/health_committee/health_committee_remit.cfm (8 February 2007).

been reviewed and redrafted to reflect single system working, the integration of Clyde and the formation of a Clinical Governance Implementation Group (CGIG). The Committees provide oversight and assurance rather than delivering clinical governance. Currently, work is ongoing to draft a new Clinical Governance Strategy taking account of the reorganisation of the Board.

The governance of the NHSGGC requires efficient and effective record keeping practices. In addition, the accountability review process and strategic development and direction of the organisation rely hugely on the availability of accurate and up-to-date records. Corporate governance is concerned with structures and processes for decision-making, accountability, control and behaviour at the upper levels of the organisation. Three fundamental principles of corporate governance that apply equally to all bodies are openness, integrity and accountability (PricewaterhouseCoopers, 2005). The success of single system working relies on the strength of the governance and clear accountability, which in turn, relies on good record keeping supporting the smooth operation of the system. Equally importantly there should be a clear distinction between the role of the back office and the front office particularly in processes that require accurate documentation such as decisions to award contracts.

4.5.3 Risk Management in the NHSGGC Board

Risk management proactively reduces identified risks to an acceptable level by creating a culture founded upon assessment and prevention, rather that reaction and remedy. It plays a vital role supporting and informing decision-making in providing a safe and secure environment for patients, carers and staff (NHS QIS, 2005a). Arguably, this is a very limited definition. Risk management should be seen from a wider perspective if the full benefit is to be achieved by NHS Boards. The NHSGGC Board is corporately responsible for ensuring that significant risks are adequately controlled. The Board believes that a robust and effective framework for the management of risk that is proactive in understanding risk and integral to decision making, planning, performance reporting and delivery processes, is essential in order to provide a high quality and safe healthcare services to the public.

At the time of writing, the Risk Management Steering Group (RMSG) was established as a sub-group of the Corporate Management Team[49] (CMT). It comprised a sponsor director from the CMT, a risk management head from each division and is jointly chaired by the Medical Director (as Executive lead for clinical risk) and Director of Human Resources (as Executive lead for non-clinical risk). The RMSG met for the first time in October 2004. A working group of the RMSG was established consisting of the risk managers from each division supported by a representative from PricewaterhouseCoopers, the NHSGG Board's external auditors. The prime function of the working group was to prepare a draft of risk Management Strategy and to develop the processes to create and sustain a corporate risk register[50].

The RMSG believed that the provision of high standards of health, safety and welfare within a risk management framework is fundamental to the provision of a high standard of health care services. The strategy was predicated on the belief that risk management is:

- An important activity to ensure the health / well being of patients, staff and visitors.
- An inclusive and integrative process covering all risks, set against a common set of principles.
- Best implemented where good practice is acknowledged and built upon.
- A major corporate responsibility requiring strong leadership and regular review.

The RMSG had identified several approaches to achieve high standards of health care services, including ensuring adequate processes to facilitate systematic recording and

[49] A Corporate Management Team (CMT) was established during 2003/04 and consists of the NHS Board Chief Executive, Director of Public Health, Director of Finance, Director of Planning and Community Care, Medical Director, Nursing Director, Employee Director and the Trust/Divisional Chief Executives. The CMT is the most senior officer led committee within NHSGG, oversees the operational implementation and delivery of approved strategies and developments. The work of the CMT was augmented by the Trust Management Teams (and from 1 April 2004, Divisional Management Teams. NHS Greater Glasgow (2004, July). *Statement of Internal Control 2003/04.* Available at: http://library.nhsgg.org.uk/mediaAssets/Board%20Papers/04-35(1).pdf (21 December 2006).

[50] Risk register is a database of risks that is always changing to reflect dynamic nature of risk and its management. Its function is to help managers to prioritise available resources to minimise risk to best effect and provide assurances that progress is being made. NHS Greater Glasgow. (2005). *Risk Management Strategy*. Board Paper No. 05/25. Available at http://library.nhsgg.org.uk/mediaAssets/Board%20Papers/nhsgg_board_paper_05-25.pdf (15 December 2006).

reporting of incidents and 'near misses[51]' to minimise the risk of occurrence, covering clinical and non-clinical incidents. Arguably, the success of risk management relied to a great degree on the availability of adequate and reliable records particularly to underpin risk assessment. In other words, the Board was not only exposed to the risk of clinical negligence but also the risk of failure to keep or destroy information and records, particularly since the FOISA came into force. To support the Board, a number of committees with interest in various aspects of risk management in NHSGGC have been developed namely Performance Review Group, Audit Committee, Staff Governance Committee and Clinical Governance Committee.

Whilst the Chief Executive had overall accountability for risk management across NHSGG, the Corporate Management Team, together with the Divisional Management Teams were tasked with the unambiguous lead role to co-ordinate, integrate, oversee and support the risk management agenda and provide assurances to the Board that all significant risks were adequately managed and the risk management principles are embedded across NHSGGC. The RMSG produced a model of risk governance (Figure 4.5.3) for the Board, however it was constructed before the inclusion of Clyde into the Board. Previously, it was the responsibility of each Divisional Management Team to implement local arrangements which accord with the principles and objectives set out in the Board's risk management strategy.

Divisional Management Teams managed risk in a way that best suits their existing style and arrangements should be able to demonstrate that they were managing risk in a consistent manner through the adoption of the guiding principles and general approach described in the Risk Management Strategy. Divisional Management Team individuals could also be nominated to lead and coordinate particular elements of the risk management process and to work with colleagues and the local risk management advisors to develop and implement agreed actions.

[51] NHSGGC Risk Management Strategy defines 'Near misses' as an undesirable incident that by chance or design did not result in harm or loss.

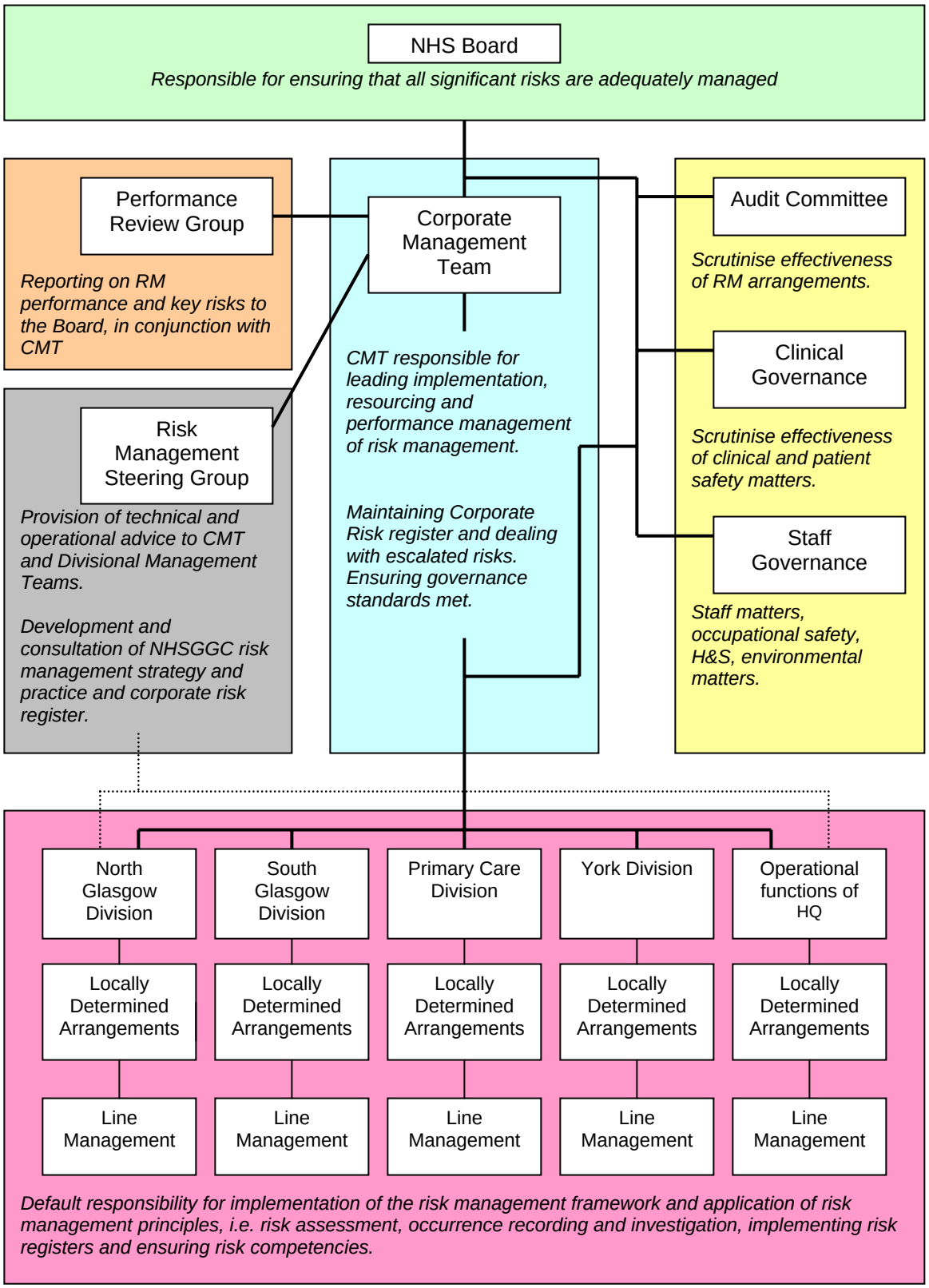

Figure 4.5.3: The governance of risk management of the NHSGGC.

The Risk Management Strategy outlined that NHSGG aimed to minimise the likelihood and severity of risk events by the recording of all occurrences or near misses through Occurrence Recording systems implemented within each division. It was the responsibility of management within each division to encourage staff to report occurrences that could pose a hazard or threat to people or the provision of services and this enable improvements to be identified, prioritised and implemented. Recording and analysis processes were made available to support local data entry, with the overall aim of shared learning across the NHSGGC.

In addition to risk identified through integrated reporting systems the Divisional Management Teams were also be required to regularly 'horizon scan' to identify risks by looking forward to tomorrow's threat as part of the development of the Divisional Risk Register. It was the responsibility of each Divisional Management Team to maintain its own Divisional Risk Register. Each risk was allocated a risk owner(s) for taking appropriate action to minimise its impact. The Divisional Management Teams regularly reviewed and updated their risk registers. It is hoped that the new governance structure of the NHSGGC Board is not a stumbling block in implementing effective risk management and new arrangements and processes are currently being considered by the Audit Committee to re-shape the risk management arrangements for the new organisation.

Meanwhile, the CMT was responsible for maintaining the Corporate Risk Register, which records and reports on action taken to manage the strategic risks facing the NHSGGC. To assist the Board in meeting its governance requirements in respect of the management of risk, the Divisional Management Forums independently challenges the effectiveness of the risk management processes at a divisional level and provides a mechanism for assuring governance to the NHSGG Audit, Staff and Clinical Governance Committees and the Board. The CMT and Performance Review Group evaluated assurances for the most significant and widespread risks contained within the NHSGGC corporate risk register and regularly reported their findings to the Board. This included a view on NHSGG's ability to meet its objectives. This ensured that risk management became firmly embedded as a Board responsibility and that assurances were provided both at a divisional and corporate level on the overall effectiveness of the risk management processes across NHSGGC.

The NHS QIS (2005b) noted that there must be numerous challenges associated with managing risk across the constituent of the NHSGGC. Although risk management strategy has been introduced, its implementation is perceived to be challenging as there are enormous disparities at the operational level. NHS QIS (2005b) identified three fundamental challenges, namely:

- Attention to document control (e.g. ensuring that strategies, plans and committee minutes are clear, specific and up-to-date) might have a positive impact on the Board's ability to oversee activity and assure governance, and allow it to better evidence its current position and performance internally, and to wider stakeholders.
- Ensuring effective continuity of risk management, while the design of arrangements for the management of risk is re-engineered to take account of whole-system working.
- Re-establishing the function of the clinical governance committee at the NHS Board level, and full implementation of clinical governance arrangements and frameworks across the system.

Since these suggestions came from an authorised body, there is clear evidence of the desirability of good record keeping across the Board for better clinical and non-clinical governance and risk management. Ironically, the state of record keeping in NHSGGC is not in line with the aim of the Board. As this research does not focus on clinical records, it is not justifiable to comment on the management of these records. However, for non-clinical records, based on interviews conducted and the findings of a records survey conducted by the Board's Archivist and Records Manager, Mr Alistair Tough, there is significant evidence that the state of non-clinical record keeping in the Board does not support effective risk management. Indeed, the risk management model will only function effectively when there is commitment from the senior management. Otherwise, the model remains ineffective and NHSGGC continues to be exposed to unprecedented risks and failure to capitalize on opportunities. Further discussion on record keeping is available in *Section 4.5.5 Records Management in the NHSGGC.*

A report by the external auditor, PricewaterhouseCoopers, states that progress continues to be made with the implementation of the Risk Management Strategy.

Consideration has been given to the implications for the strategy as a result of the restructuring within Glasgow and the transfer of services from the former NHS Argyll and Clyde Board. A recent Statement on Internal Control states that the RMSG membership, its remit and working relationship are currently being reviewed by the Chief Executive and designated executives to ensure that leadership and accountability arrangements fit with a new single system structure and also to reflect the incorporation of the functions transferred from the former Argyll and Clyde Health Board (NHSGGC, 2006c).

A consistent protocol that will apply across the single system is being developed to facilitate risk identification and assessment. The Board's external auditors, PricewaterhouseCoopers have identified the need to update and refresh the corporate risk register consistently, whilst recognising the restructuring has impacted on the development of the corporate risk register (PricewaterhouseCoopers, 2006). In response to the recommendation, the Board established a central Corporate Risk Register, a one-point entry for complaints instead of previously five risk registers across the Board. However, it is doubtful that the Corporate Risk Register can meet the expectation in the absence of good record keeping systems across the NHSGGC. In this context, a knee-jerk response is less useful without a strategic approach to ensure the availability of authentic and reliable records to feed information to the Corporate Risk Register.

4.5.4 Audit Committee of the NHSGGC Board

The NHS Scotland Audit Committee Handbook sets out that an audit committee should be composed of, as a minimum three non-executive directors, with a quorum of two and in particular the duties and experience of the work of audit committees. The handbook states:

> *At least one non-executive director of the Committee should have significant, recent and relevant financial experience, for example as an auditor or finance director. All members of the committee, what ever their background should have an understanding of Board objectives and significant issues, Board structure and culture, relevant legislation and rules, major initiatives and accountability. The Committee as a whole should have*

> *knowledge/skills/experience in accounting, risk management and audit. (Pricewaterhouse Coopers, 2006:26).*

The NHSGGC Board fulfil this requirement and has nine non-executive members.

An audit committee must contribute independently to the board's overall process for maintaining efficient and effective internal control and risk management (Audit Commission, 2006). The audit committee has a pivotal role in supporting continuous improvement as audit process is essentially risk based and provides an independent and objective examination of the financial affairs of the NHSGGC. The audit process is not only about holding audited bodies to account but also aims to support continuous improvement by making recommendations in management reports and final audit reports, and monitoring progress against agreed action plans. Since audit is a cyclical process recommendations accepted by the management must be followed up with action for the betterment of the organisation. This in turn, will be assessed by auditors in the subsequent financial year.

In the NHSGGC, the Audit Committee is gaining momentum as a result of the restructuring of the Board. It has been given greater responsibility by establishing two Audit Support Groups covering the Acute Division and the Partnerships/Corporate function. Operational issues and risks would be reported to the relevant Audit Support Group with the Groups providing assurance to the Audit Committee that they had addressed and actioned all necessary matters raised. These groups will also ensure that any issues which had or were liable to increase in importance were brought to the attention of the Audit Committee in regular reports. In the statement of assurance in respect of the system of internal control within the NHSGG, the Audit Committee concluded that risk management and internal control are considered by the Board and the Audit Committee and are incorporated into the planning and decision making processes of the Board.

As the accountable officer, the Chief Executive of the Board is responsible to the Scottish Executive for maintaining a sound system of internal control and he is required

to sign a Statement on Internal Control (SIC) as part of the annual accounts[52]. The SIC describes the effectiveness of the system of internal control; it is not restricted to internal financial controls and considers all aspects of the organisation's system of internal control including clinical governance, staff governance and risk management. If any significant aspect of the system of internal control is found to be unsatisfactory, this should be disclosed in the SIC (NHSGGC, 2006c). The SIC also states that the Board is responsible for reviewing the effectiveness of internal control having regard to the assurances obtained from the Audit Committee and any other standing committee of the Board whose remit includes aspects of the internal controls.

4.5.5 Records Management in the NHSGGC Board

Public organisations in the UK are bound to Public Records Act 1958 that is the main legislation for governing public records. NHS Boards across Scotland are bound to Public Records (Scotland) Act 1937 and Code of Practice on Records Management issued under Section 61(6) of the Freedom of Information (Scotland) Act 2002 (FOISA)[53]. FOISA requires public organisations to be able to respond to requests made by the public. Compliance with FOISA depends greatly on the effectiveness and efficiency of a record keeping system to support their operation. This, in turn, requires a significant change of mindset and culture of the staff in the Board. Despite the fact that FOISA contains Section 61 Code of Practice on Records Management, which provides guidance for managing both physical and electronic records, there is no obligation for public organisations to comply, particularly as long as they are able to respond to public requests. Organisations cannot be forced to adopt Section 61 Code. This does not in any case guarantee the status of records management.

Since the case study was conducted in the NHSGGC Board, it is essential to note it only involves administrative records as the Board does not possess clinical records. Administrative records are those relating to the management and administration of healthcare organisations, and do not include the personal health records of individual patients. Indeed, the research focuses on the strategic management of records,

[52] When the Scottish Executive issued HDL (2002) 11 – 'Corporate Governance: Statement on Internal Control', in March 2002, that requires Chief Executives to be officially responsible.
[53] NHS HDL (2006) 28 circular guidance updates NHS Boards and special Health Boards with guidance on retention and disposal of administrative records (it does not include the personal health records of individual patients) replaces guidance previously issued in Scottish Health Memorandum 60 of 1958 (SHM 58/60).

regardless of their types and forms and there was no access to records involved. In line with the FOISA, the NHSGGC is committed to increase openness and transparency in the provision of information to the public. Until 1 January 2005, members of the public were entitled to request information about NHS Greater Glasgow under the Code of Practice on Openness in the NHS in Scotland. If some or all of the information could not be provided, then the NHS Greater Glasgow Board has to explain why the information cannot be disclosed.

From 1 January 2005, under the FOI legislation members of the public are entitled to a general right of access to information, in any form, held by the NHS Greater Glasgow. However, the right to access this information is subject to certain exemptions listed in the FOI Act that the NHS Greater Glasgow has to take into consideration before deciding what information can be supplied. Information may be withheld under several circumstances such as if the Board considers that disclosure may seriously prejudice legal proceedings, regulatory or enforcement activities, or where disclosure is prohibited by law. The Board may also withhold information which may seriously prejudice the commercial interests of any person or organisation, and personal information under the Data Protection Act 1998.

Most of the requests for information came from journalists, and very few from individual members of the public. Some of the requests by journalists required complex data analysis. However, only relevant raw data can be provided, as it is beyond the capability of the Board to perform data analysis. Dr Burns (2005), currently Chief Medical Officer of Scotland, believes that the Board can respond to those requests promptly provided that they have an effective record keeping system, not only at the Board level but also across the NHSGGC areas[54]. In order to respond to those requests, the Board has to gather information from divisions involved. This can only be done in a sound and timely manner if records are readily available.

The implementation of the new single system, with CHPs being at the fore front of delivering health services, poses more problems to the NHSGGC. Apart from sound governance arrangements to support CHPs in doing the job expected of them, and to

[54] Interviewed on 16 August 2005, Tuesday, 10.00 a.m. at NHSGGC Board, Dalian House, St Vincent Street, Glasgow.

ensure that they use resources properly and to good effect, the need for an effective record keeping system is imperative as it underpins smooth operations and supports audit process.

The Head of Board Administration, Mr John C. Hamilton, heavily relies on effective record keeping as he is responsible for ensuring the availability of information for the needs of Board members and in responding to external requests. Mr Hamilton admits that currently, the Board does not have an effective and organisation-wide record keeping system[55]. This in turn leads to longer time required in finding records to fulfil those requirements. His claim is consistent with the findings of a records survey conducted by the NHSGGC Archivist and Records Manager, Mr Alistair Tough, which discovered inconsistencies of record keeping practices among various levels of administrative staff in the head office Dalian House[56].

Actually, administrative staff are provided with shared drives to facilitate sharing and access of documents and records. Unfortunately, the infrastructure does not meet their needs as more than half of respondents stated that the electronic record keeping system does not represent an adequate intellectual relationship with existing manual record keeping system. This led to users' resistance as many of them continued to use personal space in the shared drives for storing records. This is not a surprise as the GED Unit in the EIB encountered the same problem when systems developed did not satisfy users' need, though users were consulted during the development phase. Business processes did not determine the suitability of the technology to be adopted instead it was the technology that drove business processes.

It was also discovered that users were not aware of procedures for the disposal of non-current records and non-record information resources which lead to the storing of irrelevant information over time which eventually will result in the Board being flooded with unnecessary electronic documents and records. As a consequence, the Board may not be aware that it continues keeping irrelevant records or accidentally destroys

[55] Interviewed on 28 October 2005, Friday, 10.00 a.m. at NHSGGC Board, Dalian House, St Vincent Street, Glasgow.
[56] Researcher was so grateful to be given permission by Mr Tough to benefit from his records survey though it is yet published. The record survey covered the NHSGGC Board, North Glasgow University Hospitals Division and South Glasgow University Hospitals Division and Primary Care Trust.

important records, which in turn exposes itself to unquantifiable risks. Although educating and training users is essential to increase participation in a system, this is not the case for the Board at the moment, as the existing system has regularly failed to meet users' needs. Educating and training users would be a waste of resources. If a new record keeping system is to be established, a thorough feasibility study is required to ensure that the Board can operate efficiently and economically.

An integrated records management approach combining risk management, such as the one being implemented in the Standard Life Group Plc, is perhaps the best approach to adopt as it balances the cost of operations and risks exposed. There must be someone to champion the initiative, such as the Standard Life Finance director, as the governance of the project is vital to ensure the future system can satisfy users' needs. The person to lead the project must develop a working relationship with relevant divisions or committees particularly the risk management committee, the audit committee, the legal department and the IT department. The implementation of the system should be followed by training and educating users to enable them fully to utilise the future system.

Mr Tough reckons that the Board has missed the greatest opportunity to implement such system as nowadays senior management is less concerned about the impact of the FOISA in comparison to pre- and initial stage of its implementation. The Scottish Information Commissioner (2006) reported that there were 2450 enquiries against public authorities in 2005, the first year that the FOISA came into force. There were 571 appeals of which only 240 or 42 percent of cases were completed and 331 or 58 percent cases brought forward to 2006[57]. The Commissioner stated that too often public authorities failed to respond to request for information, a trend known as mute or deemed refusals. They only released the requested information after being contacted by the Commissioner, but that was months after the original request was made.

Hence, it is not a surprise that there is not yet a single case concluded in a court of law, reflecting the complexity of the process of retrieving information and records from public

[57] For further information read the Scottish Information Commissioner Annual Report 2005, available at: http://www.itspublicknowledge.info/aboutus/annualreport2005.htm (20 December 2006).

authorities[58]. This cannot be allowed to continue if the government is committed to improve the accountability and transparency of the public sector. The Scottish Information Commission will only be respected if they managed to determine the outcome of those enquires. This in turn, relies heavily on the efficiency and effectiveness of public authorities in responding to those enquiries. Arguably, the FOI legislation will only succeed when good record keeping is practiced in the public sector.

An updated guidance on the retention and disposal of administrative records to be used by NHS Boards and special Health Boards across Scotland eventually came into force in April 2006. This guidance replaces the previous guidance which was introduced almost half-a-century ago[59]. But it is essential to note that NHS Boards are not obliged to adopt the guidance. Mr Tough (2007), who was also a member of a committee that produced the guidelines, believes that the guidelines may not cover the latest technology used in the creation of records as it took about fifteen years to accomplish[60]. This was mainly a result of changes of senior officers or senior executives involved, which subsequently hampered the development of the guidelines. There were repetitions of processes as new officials need to be briefed about the draft of the new retention schedules. Eventually, it was simply too late when it came into force. Arguably, this is one of the reasons why the public sector is usually too slow in responding to changes and current needs.

The updated guidance provides comprehensive records retention schedules that encompass different types of records. However, consistent with the tradition of public organisations, the schedule only indicates the types of records, minimum retention period and brief notes for certain types of records. Apparently, the schedules suggest that the NHS Boards comply with the guidance without explaining the reasons why they should do so or identifying the risk of not doing so. These contrast with the ones that

[58] In coming to decisions on appeals the process of investigations is thorough but often time consuming. The Commissioner is obliged to come to a decision on every appeal unless it is abandoned or withdrawn. Establishing the validity of an appeal is not always straightforward as investigators to look at the request and the replies from the authority. They will look at the information which has been withheld – which may run into hundreds of pages of documents. They will ask the authority to make a submission in response to the appeal and often have to go back for supplementary (Scottish Information Commissioner, 2006).

[59] The guidance replaces the previous version issued in Scottish Health Memorandum 60 of 1958 (SHM 58/60).

[60] During a discussion on 5th January 2007, Friday, in HATII, University of Glasgow.

are being used in the Standard Life Plc which include the types and levels of risks, their current status and recommendations to improve the situation. Perhaps, it is the time for the public sector to adopt such an integrated approach combining records and risk management, which has been increasingly implemented in the private sector, to improve governance and performance.

4.5.6 Discussion on the Research Objectives in the NHSGGC Board

Following is discussion on the case study in the NHSGGC in line with the research objectives.

4.5.6.1 Records management and the governance of the NHSGGC Board

The NHSGGC is governed by a board comprises 18 non-executives directors and 11 executive directors. The NHSGGC Board has a greater responsibility than any other health board in Scotland because it is the largest NHS Board and the largest public sector employer in Scotland with over 44,000 employees to serve more than 1 million community members. In addition, the West of Scotland has the poorest health condition in Scotland. It is worth noting that the Board only deals with administration records, and there is no medical record at all. The Board is primarily responsible for the protection and improvement of health services of Greater Glasgow and Clyde region; the delivery of hospital, community and primary care services; for developing a local health plan which addresses the health priorities and health care needs of the population; for allocating resources to address local priorities in accordance with the Board's strategic objectives and the performance management of the local health system.

These prompt the Board to be effective and efficient in governing and providing health care services to the public. Being a public organisation, the nature and culture of the Board is very different from those found in Standard Life and the EIB. A recent restructuring and the implementation of a Single System Organisation aim at improving the efficiency of the Board by making better use of resources, devolving decision-making to a local level, increasing consistency and equity of access and reducing duplication. It is perceived a better option than the previous four divisions governance structure that have seen barriers that had dampen the delivery of efficient health care services to the public. The external auditor for the Board, PricewaterhouseCoopers,

believes this would enable a better delivery of healthcare services to the public as there will be no more barriers such as during the four-division governance structure. However, the new governance structure can only succeed whenever effective records management is implemented alongside clear regulations and functional procedures as well as effective control mechanisms and risk management.

Devolving decision-making to a local level requires good governance and good record keeping in ensuring consistency. Otherwise it may expose the Board to inconsistencies as similar situation may result in a variety of decisions in different quarters. Understandably devolving decision-making would speed up processes, however by the same token it may back fire on the Board if patients or the public are not satisfied and find inconsistencies of decisions or actions. This in turn may affect its accountability and reputation. To this end, effective records management is crucial to ensure consistency of decisions across the Board by making available records of precedent cases for reference. Unfortunately, there is no good record keeping practice in the Board. Also, none of the Board members is that concerned and committed to improve record keeping since the departure of Dr. Burns. This situation is obviously different to the Standard Life and the EIB, where the senior management are concerned about improving records management that is a pre-requisite for increasing the level of transparency and accountability of governance.

Arguably, being a public organisation with professional practice monitored by a self-regulated GMC, there is less urgency to improve transparency and accountability of governance of the Board in comparison to Standard Life and the EIB. As a consequence, there is no urgency to improve records management too. All NHS Boards are in some degree under the surveillance of the GMC, which is a self-regulated body itself. Based on the present situation, the effectiveness of the GMC is not something to be proud of, as most of its members are from medical background. Many argue that the GMC should employ more experts from other background to improve its governance and role in monitoring the NHS across the UK. Then only can the administration of NHS Boards across the UK be effectively monitored.

Perhaps, the lack of availability of funds from the government and the less than effective role of the GMC has partly contributed to the complacency amongst NHS

Boards. The Board is the heart of healthcare services across the NHSGGC region. The better the performance of the Board means the better the healthcare services to the public. It is worth stating that the management of many quarters within the NHSGGC would not be effective if the headquarters itself is not effective. The record keeping practice in the Board, which is the centre of the administration, must be improved in order to stimulate good record keeping across the NHSGGC region. Given the huge number of the Board members, it is suggested that it would be beneficial to review the participation and contribution of all members as such a huge Board cannot perform effectively. An effective board should not be so large as to become unwieldy. It should be of sufficient size that the balance of skills and experience is appropriate for the requirements of the business and that changes in the board's composition can be managed without undue disruption (Higgs, 2003).

However, it is not fair to blame NHS Boards alone for their poor governance or performance without mentioning other contributing factors that are beyond their control that have drained their resources significantly. For example, the influx of Eastern Europeans[61] and increasing operational cost (Audit Scotland, 2006), have direct financial consequences to the NHS Boards. As a result, more resources are allocated for healthcare services, leaving fewer resources for improving record keeping in the Boards. It is crucial for the Board to improve its record keeping practice if clinical governance and clinical risk management is to reach its full potential. The need to have a records management champion in the Board is imperative in order to ensure the effectiveness of the new single working system.

4.5.6.2 The Role of Records in Accountability Processes in the NHSGGC Board

Accountability is a global agenda that has become priority in both public and private organisations. Arguably, public organisations should be more concerned about increasing the level of accountability and transparency because their existence relies on taxpayers' money. Hence, being transparent and accountable for their performance is crucial in retaining public trust. Whenever failure or maladministration occurs, public organisations must be able to provide evidence and records to facilitate investigations.

[61] John Reid, the then Home Secretary, admitted the unprecedented influx of 600,000 eastern Europeans led to enormous burden on schools, hospitals, transport and social services. Further information available at http://www.dailymail.co.uk/news/article-419370/I-dont-know-coping-eastern-European-influx-Reid-admits.html (9 Sept 2009)

Such a situation must be resolved efficiently and the culprit must be identified and punished according to pertinent laws and regulations. Only then will public trust be maintained in the organisation and the government, though its reputation may have been tarnished. Providing quality healthcare services, which is a key public service, is central to the government.

Today, in the name freedom of information and in the interest of the public, the media can reveal information that may damage the reputation of the Board. In the event, the Board must be able to respond by providing reasonable reasons supported by evidence and records. Given the huge responsibility of the Board in providing quality healthcare services, managing financial and other resources as well as strategic issues, the potential of the Board to be the focus of public attention is certainly high. Records have a crucial role in providing reliable evidence that can be used by an organisation to inform the public about the actual situation or to defend itself against any accusation. The Head of Board Administration, Mr Hamilton, admitted that the Board is desperate to have a sound record keeping system to facilitate the accountability processes.

There are instances where he almost failed to find records to respond to the media. Such situations jeopardised the accountability of the Board and public confidence. There are cases where the lack of appropriate records had led to an out of court settlement for undisclosed compensation to plaintiffs because of the NHSGGC's apparent failure to provide appropriate healthcare services. It would be even more damaging, if the Board failed to defend itself in accountability cases such as accusation of mismanagement or maladministration, due to unavailability of authentic and up-to-date records. The Head of the Board certainly knows that good record keeping is what exactly needed to function more effectively, not only because of the pressure from the media and the public, but for better operation of the Board itself. Unfortunately, his concern is not given adequate attention by the Board. Perhaps, the demand for transparency and accountability is less pressing in that case, in comparison to the Standard Life and the EIB.

Implementing a good record keeping initiative should be a high priority. The longer the delay, the more the cost incurred for unnecessary things such as waste of man hours as experienced by Mr Hamilton and his staff in the process of looking for records to

respond to the media. This situation should not be allowed to continue because it affects the efficiency and effectiveness of the Board not only in responding to media scrutiny, but in its daily operation as well. The current state of record keeping in the Board as discovered by the Archivist and Records Manager, Mr Tough, through his records survey needs immediate attention from the Board. There are inconsistencies of record keeping practices among various levels of administrative staff in the Board despite having shared drives to facilitate record keeping activities.

Accountability processes will become more efficient when records are managed effectively and systematically. Evidence can be made available within a reasonable response time and decision making will be more efficient. Good record keeping can be implemented in the Board without much cost and over-engineering because the basic infrastructure is already there. Administration staff are provided with shared drives, that are meant for sharing of documents and records. Further more, there are only administration records in the Board, no medical records at all. So it will be less complicated. What is needed now is a driving force from an influential individual among the Board members to lead a records management initiative. Ideally it should be the chairman of the Board himself, just like the President of the EIB. Otherwise he could appoint any influential Board members to become a records management champion.

4.5.6.3 The Relationship between Risk Management and Managing Records in the NHSGGC Board

The Board believes that a robust and effective framework for the management of risk that is proactive in understanding risk and integral to decision making, planning, performance reporting and delivery processes is essential to provide high quality and safe healthcare services to the public. However, this belief should not remain as a fine rhetoric given the present situation of the Board that it is still long way for risk management to reach its goals.

The establishment of RMST that functions to manage clinical and non-clinical risk would not reach its targets if there is no holistic approach taken by the Board, particularly with the restructuring and the implementation of the Single System Organisation. Effective risk management helps the Board to balance its cost and benefit as well as achieving it strategic goals. However, it is essential to note that risk

management should not be seen as an agent of identifying threats to organisations, but it has to be viewed as an enabler and a driver of change that moves organisations towards achieving its strategic goals (Currall, 2006b). Therefore, taking risk into consideration would be useful for the Board to function effectively and economically.

Managing the Board should not be too much different from managing other organisations because it mainly deals with strategic issues. It would be easier to implement risk management at the Board level rather than across the NHSGGC mainly due to the size and the focus of the Board. Unfortunately, during the time of the study there was no clear evidence of the implementation of risk management in the Board. The study also reveals there is no evidence of a relationship or an integration of risk management and managing records in the Board. Given the inconsistencies in record keeping practice, it is likely that risk management requires considerable time to reach maturity.

Arguably, good record keeping is a pre-requisite to risk management as it ensures the availability of records for risk assessment purposes. It is suggested that in order to be effective, the Board must view the benefit of risk management from a broader perspective. Together with records management, an integrated approach can be adopted, similar to the one in Standard Life. Maybe, the demand to adopt such approach is not as great as in the latter. Risk management must be embedded in all activities so that it can become part of the daily routine and responsibility of every staff. This applies to records management too. These two management areas embrace all activities within an organisation because all management is risk management. Meanwhile, records are a by-product of business activities that need to be managed appropriately. It is to be hoped that the Board will pay adequate attention to integrating risk and records management as the benefit is not limited to these two areas only, but the Board as a whole will improve its performance as well as the level of transparency and accountability.

CHAPTER 5
DISCUSSION AND CONCLUSIONS

5.0 DISCUSSION AND CONCLUSIONS

5.1 Introduction

This chapter attempts to integrate and compare the cases of poor governance outlined in Chapter 3 with the case studies with reference to the research objectives. Despite a belief that records have a crucial role in underpinning effective and efficient operations and the accountability of governance, the contribution of the records management community was not widely acknowledged either internally or externally in the chosen organisations (Meijer, 2001). To this end, it is worth noting from the cases of poor governance and the case studies of ways to improve the contribution of records management to the accountability of governance. This chapter discusses the findings of the research and provides recommendations to improve the role of records management in underpinning the accountability of governance. The findings and recommendation should enhance the records management profession in both the public and private sectors.

5.2 Discussion

In a democratic society, the government is expected to be more accountable and transparent than in the private sector. However, the trend revealed by this study is the other way around for various reasons. The cases of poor governance and the case studies were deliberately chosen involving both public and private organisations to identify the best records management practice that can be adopted elsewhere. Having investigated the cases of poor governance and conducted the case studies in Standard Life, the EIB and the NHSGGC, it became clear that records management is central to good governance in both public and private organisations.

5.2.1 The essence of records management for good governance

The board of directors or the governing body of an organisation is responsible for the direction, leadership and accountability of the organisation. These obligations can be achieved through having appropriate systems and processes. Transparency and accountability is underpinned by good governance, which in turn leads to good management, good performance, good stewardship of public money, good public engagement and, ultimately, good outcomes (The Independent Commission on Good Governance in Public Services, 2004).

Good governance relies on ethical values and commitment from employees in performing their responsibilities. There are seven principles of good governance, namely: selflessness, integrity, objectivity, accountability, openness, honesty and leadership (Committee of Standard in Public Life[1], 2006). These principles can only be established with the presence of evidence, in form of records. Therefore, managing records, regardless of their form, is vital to providing evidence of good governance. Although not all principles, for example selflessness, can be apparently demonstrated in records, the availability of adequate metadata and contextual information can prove the existence of this ethical value. Therefore, the comprehensiveness of documentation process must be properly considered to ensure the adequacy of metadata for the authenticity and integrity of records.

It is evident that poor record keeping attracts corruption like flies to a carcass is perfectly pictured in the mismanagement and corruption in the Australian government in the 1980s and 1990s. Ironically, good record keeping also cannot prevent mismanagement and deceptions, most notably in the collapse of Enron. This is to say that in the absence of good ethical values and integrity, a situation can be manipulated to fulfil individual interests and greed. It is evident too that good record keeping cannot guarantee jobs are performed responsibly. For instance, the massive killings by Shipman were discovered by assessing available records. Though the triggering point was merely amateur, the subsequent investigations discovered the actual scale of the crime.

In other words, good record keeping without adequate or effective control mechanisms together with the absence of good ethical values could impede the accountability of governance. Arguably, implementing control mechanisms must consider the economic return as well as the likelihood and the impact of the risk of failure to comply with any particular regulations. This issue is further discussed in *Section 5.2.3 The Relationship between Risk and Records Management*.

[1] This committee was known as the Nolan Committee, which was asked to investigate standards in public life, is an independent committee, set up in response to concerns that conduct by some politicians was unethical – for example, allegations of taking cash for putting down parliamentary questions. Further information available at: http://www.parliament.uk/works/standards.cfm (24 September 2006).

Among all cases of poor governance, the Hutton Inquiry and the Butler Inquiry were the ones that gained most public attention in the UK as the government was directly involved. The tragic death of Dr. Kelly, one of the chief weapons inspectors in Iraq, had shocked the UK and consequently put the Labour government under massive pressure to justify its decision to go into war in Iraq. Although both the Hutton and the Butler inquiries were regarded as a government white wash for not identifying the culprit, they disclosed a worrying record keeping practice in government that is less effective than it used to be. It was also discovered that decision-making was more informal, and that Cabinet agendas were not distributed in advance, thus plainly preventing Cabinet members from preparing properly for discussion of such important issues (Committee of Privy Counsellors, 2004). This in turn, reduces the scope for informed collective political judgement, which in a way enabled the Labour government to go to war in Iraq without going through heated debates in the Cabinet.

Unfortunately for the Labour government, the situation became worse when the effort to be transparent through the Hutton and the Butler inquiries failed to convince the public. Understandably, the unconvincing evidence used, for example only two drafts of the dossier were presented to the Hutton Enquiry as pointed out by the Times editor. The editor was also concerned about how the Cabinet office could become in effect an electronic office without good record keeping practices.

In other words, the government failed to convince the public because its transparency failed to shed light on government practices due to the absence of reliable, relevant and timely information (Kondo, 2002). The claim by the Labour government that Iraq possessed WMD was eventually proved completely wrong in a report by US Chief Weapons Searcher, Charles Duelfer, released in July 2004. To this end, being transparent alone does not guarantee a higher level of trust, because it is evident that transparency also can encourage people to be less honest, increase deception and by so doing reduce trust, particularly those, who know that everything they say or write will be made public (O'Neill, 2002).

It is evident from the cases of poor governance that good record keeping is essential for good governance. The presence of integrity and good ethical values enhance the

significance and contribution of records management to the accountability of governance of organisations. The three case studies were conducted in order to investigate the essence of records management for good governance in both the private and public sectors. Apparently, in Standard Life and the EIB records management was given higher priority by the management. Standard Life is a private organisation, whereas the EIB is an EU public body. Arguably, it was not the status of the organisation that matters, but the nature of business that triggered them to engage good record keeping practice. By contrast, the NHSGGC, also a public organisation, does not possess good record keeping practice despite providing healthcare services, one of the core public services, in the West of Scotland.

Standard Life has no option except to comply with the FSA requirements as well as Basel II convention in operating its business. The EIB, although it possesses legal immunity, chose to comply with Basel II convention for the purpose of transparency and accountability. It is essential for financial institutions to demonstrate a high level of transparency and accountability, particularly in an era where corporate crime and terrorism is deemed a threat to the global economic stability and safety. Being a completely private organisation, Standard Life has to achieve a considerable level of transparency and accountability of its performance in order to gain trust and confidence particularly among its shareholders and stakeholders. Without trust and confidence, the company may collapse. In other words, Standard Life does not only need to comply with the FSA and Basel II requirements, but equally important is the need to satisfy the expectation of its policy holders, shareholders and stakeholders that profit must be delivered continuously year in, year out.

The seven principles of good governance advocated by the Committee of Standard in Public Life (2006) are applicable to both public and private organisations. The decisions, actions and performance of an organisation must reflect the fact that its employees have been imbued with these principles. The management of Standard Life, aware that operating in a tight regulation environment, requires them to be certain about the accuracy of their records in order to operate at a high level of certainty, in terms of decision-making, business strategies as well as strategic planning. Rightfully, Willis (2005), a lawyer by profession, advocates that good record keeping underpins six key requirements for good corporate governance, namely: transparency, accountability,

due process, compliance, meeting statutory and common law requirements, and security of personal and corporate information. This is to say that there is nothing more important than ensuring the availability of the evidence or records, which is a key substance of all business activities. Failure to capture and manage records may expose the organisations to considerable uncertainty or risk.

Because the benefit of good record keeping is not limited to transparency and accountability purpose only, the EIB implemented an organisational wide integrated strategic information system, of which an electronic records and document management or GED is the backbone. An interesting point about the EIB is that the management was highly committed to developing the infrastructure that is key to the implementation of an organisational-wide record keeping system. The GED is equipped with effective control mechanisms that ensure the integrity and authenticity of records. Therefore, the EIB can be certain about its performance, compliance, higher level of transparency and accountability as well as its sustainability.

The management of Standard Life convinced that what was needed is good record keeping practice in order to provide evidence of their performance and business activities. Good record keeping has been nurtured and embedded in its business activities across the company. More interestingly, Standard Life adopted an integrated risk and records management approach, which is scarcely seen in other organisations. The case study in Standard Life was a revelatory one, indeed. The integration of risk and records management is further discussed in *Section 5.2.3 The Relationship between Risk and Records Management*.

Understandably, the responsibility of the public sector is different from that of the private sector. The governors of public organisations, including the NHSGGC Board, face a difficult task as they are responsible for governance – the leadership, direction and control of the organisation they serve. Their responsibility is to ensure that they address the purpose and objectives of the organisation and that they work in the public interest. However, there should not be much difference in terms of practicing good governance that enables efficient, effective and economic operation. Executive and non-executive directors must be clear about their responsibilities and need to make

sure that those responsibilities are carried out. The Independent Commission on Good Governance in Public Services (2004) states the role of non-executive directors is to:

- Contribute to strategy by delivering a range of perspectives to strategy development and decision making,
- Make sure that effective management arrangements and an effective team are in place at the top level of the organisation,
- Delegate: non-executives help to clarify which decisions are reserved for the governing body, and then clearly delegate the rest,
- Hold the executive to account: the governing body delegates responsibilities to executives. Non-executives have a vital role in holding the executive to account for its performance in fulfilling those responsibilities, including through purposeful challenge and scrutiny,
- Be extremely discriminating about getting involved in matters of operational details for which responsibility is delegated to the executive.

Mutual understanding is essential in order to allow a meaningful relationship between a chairman, who is a non-executive director, and the chief executive officer. Their responsibility will be jointly supported by other board members. It is, therefore, essential to appoint non-executives directors with adequate competencies to ensure that they are capable to perform their responsibilities. Currently, the NHSGGC Board comprises 18 non-executive directors and 11 executive directors. Perhaps, it would be beneficial to review the participation and contribution of all members of the Board, as such a huge group can not perform effectively. An effective board should not be so large as to become unwieldy; it should be of sufficient size that the balance of skills and experience is appropriate for the requirement of the business and that changes in the board's composition can be managed without undue disruption (Higgs, 2003).

Ironically, despite of the massive size of the EIB's senior management team which includes the Board of Governors, the Board of Directors and the Management Committee, the Bank continues to function efficiently and effectively. It is the responsibility of the Management Committee to ensure the Bank's operations are conducted according to relevant procedures, regulations and standards adopted. In the case of NHSGGC Board, the role of the CMT should be expanded to ease the role of the Board. This would be hard to implement as the Board has a different culture,

particularly if members of the CMT are not from a medical background. Changes to the present governance structure are required if the Board is committed to operate efficiently, effectively and more importantly economically. The remits of the Board and the CMT have to be reviewed to delegate more power to the CMT for making decision, whilst the Board remains the most authoritative and accountable body within the NHSGGC. All these reforms have to be seen from a wider risk management perspective with an aim to strike a balance between costs and benefits of operating the NHSGGC. Indeed, the Board can gain even more benefits if good records management, alongside risk management, can be cultivated and embedded in all its operations.

However, it is not an easy task to implement a sound records management across an organisation as it requires commitment at the most senior management level, be it an individual or the rest of the management. Arguably, the success of integrated record keeping systems in the Standard Life and the EIB was a direct result of the commitment from the senior management. At one time, the NHSGGC Board was on the right track to improve record keeping practice when Mr Tough managed to gain the support of Dr Burns, the then Public Health Director. Unfortunately, the effort came to a halt with the departure of Dr Burns, when he was appointed Chief Medical Officer for Scotland in June 2005. In the EIB, it was the President of the Bank who instigated the compliance effort, which in turn led to the implementation of the GED and the ISIS.

This, however, is not the case in the NHSGGC as there is now no one at the most senior management level to champion records management. Perhaps, a move by the government, with its coercive power, is the best solution to improve record keeping practice in the public sector. Only then, will adequate funds be made available for public organisations, including NHS Boards to review or redevelop record keeping. However, hoping for this to happen will not improve matters. A change of culture is desperately needed if the NHSGGC Board is to become committed to improve performance and accountability. It is essential to note that the benefit of good record keeping does not appear immediately, but will gradually surface when the number of records increases steadily, whilst the retrieval of records and information becomes more efficient and effective in responding to internal users, media and the general public.

5.2.2 The Role of Records in the Accountability Processes

Accountability is the process of being called 'to account' to some authority for one's action, and to be 'accountable' is to 'answerable' (Jones, 1992). Accountability is also described as an informative concept that requires provision of answers, such as reporting or more obviously 'giving an account' to authority (Quirk, 1997). The demand for transparency and accountability, either political or managerial, is greater than ever as a society became more complex and global. Without reliable and authentic documentary evidence, an organisation cannot demonstrate to its shareholders, stakeholders and the public that it has used resources responsibly and it has fulfilled its mandate. Relatively, the public sector has to demonstrate a greater transparency and accountability than the private sector because resources mainly come from taxpayers' money. The private sector mostly needs to satisfy their shareholders and stakeholders (Moss, 2006a).

Nevertheless, organisations need to avoid the trigger of accountability processes by being transparent. However, transparency does not guarantee a high level of trust as the truth may be massaged by irresponsible individuals as we have seen (O'Neill, 2002). To this end, accountability processes such as audit and ombudsmen have a critical role in demonstrating the transparency of audit processes as well as the transparency of audit findings (Hollingworth, 1999). These activities use and produce records that are vital for the accountability of organisations. Arguably, transparency enables accountability by providing reliable, relevant and timely information about the organisation's activities to the authority or public. In the context of the public service, the notion of accountability has been extended to the sense of individual responsibility, both professionally and personally, and concern for the public interest expected from public servants (Mulgan, 2000).

Cases of poor governance proved wherever corruption and a failure of accountability are found, an associated failure in record keeping is, almost, invariably, identified as part of the cause. For example, the investigation by the Auditor-General of Victoria on the Victoria Metropolitan Ambulance Service *(See Section 3.2.1.2 Victoria Metropolitan Ambulance Service)* discovered corruption and crime of breach of trust involving the chief executive of the MAS himself, an established audit firm and three consultancy

companies (Victoria Government, 1997). Although, transparency and accountability was not a key agenda during the time, the failure to deliver efficient emergency services to the public triggered the accountability process.

The corruption eventually failed to hide records and other evidence of their corruption, though on few occasion records were deliberately not created for the purpose of hiding wrong doing. As a result of the investigation, the corrupt management team was replaced by a new management team which progressively implemented a new records management system as part of initiatives to improve the process and integrity of contract management (Victoria Government, 1997). Arguably, the absence of good record keeping in the MAS allowed greedy individuals with poor ethical standards to be so corrupt that they damaged the accountability of the organisation as well the Victorian government. It is evident that records play an essential role in the accountability process as the Auditor-General of Victoria who eventually disclosed the culprits testified.

The accountability process in the Heiner Affair was more complicated because of the involvement of political masters. Premature destruction of public records under the directive of the Goss cabinet and subsequently approved by the then State Archivist raised concerned about the accountability of the government and the record keeper as an agent of accountability. The destruction of the records was regarded by Hurley (1999a) as the real corruption and the root cause of child abuse because they permitted and nurtured the cover up that allowed systemic child abuse to occur. The act of the then State Archivist allowing premature destruction of public records, presumably was mainly caused by the absent of legal protection, that left her with no option except to comply with the directive from her political masters.

It took fifteen years and considerable cost of investigation to convict only one person, Pastor Douglas Ensbey, whereas others, including senior government officials and politicians despite their roles in the premature destruction of records and mismanagement, escaped scot-free. What was the key contributing factor to the lengthy investigation or accountability process? Arguably, it was the premature destruction of records at various levels, from the ministry to the operational, in an attempt to cover up the abuse at the JOYC. Such mismanagement can be avoided if

those involved particularly politicians, possess a high level of integrity and accountability.

The collapse of Enron and other corporate giants in the US, in the early stage of the millennium shook the corporate world around the globe. The fall of Enron disclosed the horrific scale of irregularities in its practices, including the involvement of one of the most trusted audit firm, Arthur Andersen, which was caught red handed shredding supporting documents and the actual accounts of Enron in an attempt to cover up improprieties (Healy & Palepu, 2003). It was proved that two sets of records were consistently updated to demonstrate fake accountability and to hide improprieties. The catastrophe also disclosed the failure of the internal accountability process under the remit of its audit committee. Had the internal auditors and the audit committee acted responsibly, such a crime of breach of trust could have been prevented much earlier.

Surprisingly, even with the presence of prominent figures in the Enron audit committee, they failed to perform check and balance functions as expected. This raised questions about the reliability and performance of audit committees and inspectors, that are themselves subject to audit too as argued by Power (1994) more than a decade ago. This suggests that having another third party to monitor the performance of audit committees and external auditors may provide a solution. This, however, could be too costly and as a consequence, organisations may be reluctant to adopt such approach as it would be difficult for them to attain economic efficiency and sustainability. Perhaps, the financial or other authorities should perform this task without involving too much cost. Understandably, transparency and accountability is attainable when the cost is reasonable for organisations to sustain and continue making profit.

The Shipman case provides evidence that procedures alone cannot stand by themselves as irresponsible individuals might choose to override them. Accountability processes become negotiable whenever the level of trust is high. That was exactly Dr Shipman's intention. He developed a warm and professional relationship with individuals related to his role as a general practitioner. Once trust has developed, he betrayed them without the suspicion of those individuals. During his 23 years of malpractice and murder, records were created as required, but the authenticity and integrity was never challenged, until the accountability process known as the Bichard

Inquiry was set up. The ombudsman proved that legislation and regulations are meaningless in the absence of effective monitoring and controls, even if adequate records are available to detect a wrong doing. From another perspective, this case proved that the benefit of good record keeping is enormous. Even after 23 years, the evidence was still readily available to facilitate the accountability. To this end, good record keeping proved to be vital for the accountability process.

The case studies discovered different levels of authority and importance of audit committees. Audit committees in Standard Life and the EIB, are given a greater authority in comparison with the audit committee in the NHSGGC. The key factors certainly are the private sector status and the nature of business of Standard Life and the EIB that require both organisations to be certain about the availability of records of their business transactions. Understandably, records have a crucial role in attaining a high level of transparency and accountability that is vital for the sustainability of these organisations. Both Standard Life and the EIB must have learned from the failure of the audit committee that partly contributed to the collapse of Enron. Furthermore, the catastrophic failure of corporate firms and high profile accounting scandals in the US, has led to the establishment of the SOX that demands higher accountability from audit committees. This has opened the eyes of the senior management of Standard Life and the EIB to strengthen the role of audit committees, though there is yet no SOX-like legislation in the UK and on the Continent.

The fact is that by improving the performance of audit and internal controls, an organisation will be more certain about its performance as well as compliance with regulations. The Standard Life Audit, Risk and Compliance Committee is responsible, among others, to oversee financial reporting, internal controls and risk management, whistle blowing, as well as internal and external audit. The audit committee receives report from Group Risk Management and Compliance, Internal Auditors and External Auditors.

Arguably, this is a perfect blend as audit, risk and compliance are inter-related areas that require a holistic approach not only for handling audit, risk and compliance matters but also identifying appropriate strategies for the efficiency of conducting audit, risk and compliance-related activities. This in turn, facilitates the decision making and

accountability processes as being a hub of audit, risk and compliance activities. The information is held by the committee's members. To this end, Standard Life as a whole has attained an economic efficiency that ensures its sustainability. Interestingly, these activities are incorporated into records management, thus makes the whole processes within the organisation systematically organised.

In this context, next to Standard Life is the EIB. Although the governance structure of the EIB is slightly different from that in Standard Life, the role of the audit committee is still the same in that is to ensure that the operations of the Bank have been conducted and its books are kept in an appropriate manner. Similar to the situation in Standard Life, the efficiency and the effectiveness of the audit committee is partly complimented by other entities namely, the Inspectorate General, the Compliance Office and RMD. Despite the name that is yet to include risk and compliance terms of reference, the audit committee actually is also responsible for assessing the adequacy and effectiveness of internal control, risk management and compliance of the operations within the legal and regulatory framework.

It is evident from the case studies in Standard Life and the EIB, that the process of ensuring accountability would be more economically implemented by integrating audit, risk and compliance tasks. It is also evident that the strength of such approach, particularly in Standard Life, is underpinned by effective records management, which integrates risk into records management framework. The integration of risk and records management is further discussed in the subsequent *Section 5.2.3 The Relationship between Risk Management and Managing Records*. Like Standard Life, the EIB also has upgraded its information and records management systems by developing an organisational-wide ISIS and the GED. These systems facilitate the management of information and records that are the key ingredients for the Inspectorate General, the Compliance Office and the RMD. This is to say that the management of Standard Life and the EIB believe that records management is vital for the performance, accountability and sustainability of the organisations.

The third case study in the NHSGGC revealed that the organisation does not possess comprehensive accountability measures as at the Standard Life and the EIB. Arguably, its public organisation status and the nature of its business make accountability less

important to the Board despite increasing public interest in the transparency and accountability of the public sector. This indicates that the impact from public demand is less effective than that of regulatory requirements.

The role of the audit committee of the Board was merely to oversee financial aspects. However, following the restructuring of the Board recently, the audit committee has been given greater responsibility that now embraces operational and risk management. Perhaps, this is an early indicator that the Board is moving towards increasing the level of transparency and accountability. The restructuring also led to a move into a single system for healthcare services across the NHSGGC region. This means there is an increasing reliance on the integrity and authenticity of records in providing evidence for not only daily operation, but also the accountability review process and strategic direction of the Board.

Unfortunately, the Board is yet to be convinced of the essence of good record keeping and the need to improve existing record keeping system despite the frustrations experienced by the Head of the Board Administrator, Mr Hamilton. With hindsight, the departure of the then Public Health Director halted the effort to improve record keeping practice in the Board. Hence, it would be better to expose the Board members to the integrated approach such as implemented in Standard Life and the EIB. The contrast of the nature of business should not be an impediment as the objective is to increase the level of transparency, accountability and the sustainability of the Board by adopting an integrated, holistic and strategic approach. By so doing, hopefully the perspective of the Board members will change significantly. The departure of any Board members would not be a hindrance to the process of improving record keeping practice anymore, as the benefits will be understood by all members of the Board.

Having scrutinised and analysed the cases of poor governance and the case studies, it is undeniable that good record keeping is essential for accountability processes, be it internal controls and audit or public inquiries. Indeed, the case studies in Standard Life and particularly the EIB, proved the benefit of good record keeping is huge. It is not limited to the purpose of transparency and accountability solely, but more significantly enables attaining higher profits and above all the sustainability of the organisation itself. Neither regulations nor audit and control mechanisms nor records management can

individually significantly contribute to the accountability and sustainability of the organisation. An orchestrated effort is required to nurture the culture of good governance amongst accountability actors including employers and employees, as well public servants and ministers. But one thing is for certain, reliable and authentic records, and the evidence that they contain, are instruments by which organisations can promote a climate of trust and overall commitment to accountability and good governance.

From the records management perspective, the accountability of records managers and archivists is of utmost importance because they are the keepers of evidence and national heritage. Unfortunately, public records centres and archives have no power to attest to the veracity of records, particularly their content, as the responsibility lies within the operational or business process owners. Without legal protection, it would be illusory for records managers and archivists to be accountable in performing their jobs as record keepers, particularly under political influence, except for those with brave hearts. To this end, the gravity of being accountable but against the instructions of superiors could be intense, as experienced by the famous tobacco whistle-blower Dr Jeffrey Wigand for disclosing vital information in a court of law. Indeed, the repercussion was deeply painful not only for a whistle blower but his or her family too. (*Discussed in Section 3.3.3 Authority of Records Managers and Archivists).*

In a truly democratic society, records centres and particularly national archives should be given full authority under the rule of law to decide whether or not to retain a record. There should not be political interference, particularly by the government, in deciding which records be kept or destroyed, as evidence of governance has to be kept for future research and posterity. Be it as evidence of good or poor governance, only time will tell.

5.2.3 Relationship between Risk Management and Managing Records

For board of directors and senior management, there is nothing more important than the sustainability of the organisation, which relies heavily on the profitability and cost efficiency of operations. All these, however, have to be attained in a climate where transparency and accountability is paramount. To this end, organisations must be able to adopt a pragmatic and holistic approach that balances sustainability and the demand

for transparency and accountability. Apart from adopting the principles of good corporate governance, the case study in Standard Life discovered an integrated risk and records management approach, which ensures the sustainability, transparency and accountability of the organisation. Indeed, this is the key finding of the research.

With hindsight the notion of risk management, since its emergence in 1960s, has expanded from its traditional role of controlling loss and financial status of an organisation (Mehr and Hedges, 1974) to the harm that may be suffered by any type of facility or activity because of unforeseen (or indeed predicted) events, in response to tightening controls and external pressures (Thompson, 2003). Increasing regulations and compliance as well as global demand for transparency and accountability of governance are requirements, expectations and pressures that seek strategic solutions rather than knee-jerk actions from the management. It is essential for the management to understand that confining risk management to compliance is dangerous as risk management is about clarity and the ability to not only identify the correct opportunities but also to maintain discipline in pursuing them (Sharon, 2005a). To this end, the integrated approach adopted by Standard Life is certainly a strategic solution that enhances the sustainability of the organisation.

Understandably, risk management is a key element of corporate governance, and records and information management supports the attainment of both effective risk management and corporate governance (Lemieux, 2006). At the same time, however, increasing public demand for good governance has given rise to a compliance culture that has both spawned a rise in the number of records and information-related risks and created a situation where total compliance is virtually impossible, if not undesirable, due to conflicting regulations and objectives and the cost of implementation. In such an environment, risk management is the best, if not the only way to strike an appropriate balance. Risk management should not only be seen as an agent of identifying threats to organisations, but it has to be viewed as an enabler and a driver of change that moves organisations towards achieving strategic advancement (Currall, 2006b). The strategic and integrated risk and records management approach adopted by Standard Life proved that having a concerted effort involving the Audit, Risk and Compliance Committee and the Group Records Management Division is worthwhile.

The formation of the Audit, Risk and Compliance Committee proves the commitment of the Board of Directors and the senior management of Standard Life towards to improving the performance as well as increasing the level of transparency and accountability of governance that satisfies its policy holders and stakeholders. Centralising audit, risk and compliance activities facilitates the coordination and arrangement of internal controls. Resources will be more organised and monitoring of control mechanisms will be more efficient and effective. As a consequence, the board of directors and the management are more certain about performance levels and exposure to risk.

The model of risk management process by AIRMIC, ALARM and IRM (*See Section 2.7.2 Elements of Risk Management*) and understanding the role of records management lead to an assumption that there is a symbiotic relationship between the two and also the audit and compliance elements. At this point in time, it is no longer an assumption as the relationship has become a reality as proven by Standard Life. An integrated approach completely overturns the perception that records management does not contribute to the performance of an organisation, instead has a vital role in underpinning the performance of the organisation provided a pragmatic and strategic approach is adopted. As a consequence, the management of records in Standard Life became more efficient, partly because the destruction of unnecessary records is now more reliable as a result of authoritative input from the Risk, Audit and Compliance Committee.

Under an integrated approach, the task of identifying risk associated with a particular record becomes part of the remit of the Audit, Risk and Compliance Committee. With reliable input from such an authoritative source, the task of producing records retention schedules becomes more efficient, reliable and accountable. In Standard Life, the driving force behind the effective collaboration between the Group Records Management Unit and the Audit, Risk and Compliance Committee was the relentless support from the Board of Directors and senior management. In fact within this framework, the Records Management Unit worked closely with other divisions as well, including IT Infrastructure and Application Development, Business Resilience, Physical Security and Business Unit stakeholders, thus creating a virtual team addressing issues of risk.

This to say, in order to be effective and significant to the organisation, records managers have to be proactive and collaborative. They need to change their mindset and come to understand that managing records has to be aligned with the organisation's business goals. Perception that business managers are not interested in practising good record keeping should not be in their mind at all because it brings nothing except the isolation of the records management profession itself. The case study in Standard Life proved that good record keeping can be successfully embedded in business activities and become a culture in the organisation.

It was the awareness of the board of directors and senior management that good governance is not compliance driven but sustainability and performance driven. The stakes of Standard Life are high. Thus, records management systems can not go wrong as financial crime such as money laundering and fraud may go undetected or remain unproven. The impact can be immediate and disastrous, at best share prices plummet or at worst the organisation collapse. Arguably, the needs for sustainability is greater than the needs for compliance as meeting the latter's requirements could be too costly and can severely limit surpluses available to stakeholders hence affecting sustainability. On the other hand, ensuring the sustainability allows a greater flexibility in mitigating risk that enables greater surplus whilst being certain about risk associated.

It is essential to note that during the writing of the thesis, the manager for the Group Records Management Unit has left Standard Life to join another financial services institution as Head of Information Management Governance. Certainly her experience in developing such a pragmatic and economic integrated risk and records management approach is an invaluable asset that is highly marketable. The experience as a system manager was a key element that led Mrs Knight to the successful collaboration with other professionals in implementing the organisation-wide integrated risk and records management system. Her enthusiasm, knowledge and experience enabled a seamless networking that interweaves the needs of records management, business requirements as well technology capabilities towards the organisational goals. These are the qualities that that can resurrect the records management profession. To meet this goal, higher learning institutions and professional bodies have a crucial role in educating and training future records manager.

In the context of the EIB, the essence of records management for the sustainability of organisations has been given high priority by the senior management. Although, there is as yet no integration of risk and records management, the infrastructure to enable such a process has already been established with the successful implementation of the ISIS and the GED across the Bank. Besides that, the Inspector General, the head of Operational Risk Division and the Chief Compliance Office acknowledge the importance of good records management for accountability of governance. They also showed a great interest in the idea of integrating risk and records management as it is beneficial not only for their divisions but more importantly for the Bank as a whole. In addition, there is already an excellent working relationship between the RMU and those divisions that provides a firm foundation for an integrated approach. On top of this, the commitment of the President of the Bank to increase the level of transparency and accountability offers the best opportunity for the implementation should a proposal for an integration of risk and records management be put forward.

The efficiency of the Inspectorate General, the Risk Management Directorate and the Compliance Office rely heavily on the accuracy and authenticity of records. Their decisions and actions must be justifiable as the call for transparency and accountability is constantly high. The Bank cannot be flooded by unnecessary records as it affects not only the efficiency but also expose the Bank to unnecessary risk. To be efficient and certain about risk exposure, there must be a consistent appraisal and destruction of unnecessary records, including records of tolerable risks. Record retention schedules must be systemically determined based on risk analysis in order to ensure the availability of records of the Bank's operations, which is within anticipated risk boundaries.

In other words, a symbiotic relationship between the Risk Management Directorate and the RMU ensures the continuity of the information produced by the former is benefiting the latter. This reciprocity means reliable and authentic records of risk management, audit, compliance and other business purposes is readily available through effective records management. It is worth noting that risk management is an iterative process, hence, both Risk Management Directorate and the RMU are interdependent and beneficial to each other. In a broader perspective, the EIB as a whole will attain

effective and efficiency of operations. Nevertheless, given the established infrastructure and the commitment from the senior management, particularly the President of the Bank, the integration of risk and records management is within reach.

The case studies in the Standard Life and the EIB revealed that both organisations have adopted a collaborative approach by enhancing the role of audit committees and establishing risk management and compliance divisions in line with best corporate governance practice. These divisions, in turn, enable the organisations to strike a balance between the cost of operations and risk exposed. In Standard Life, the Audit Committee is responsible for reviewing the adequacy and effectiveness of internal control and risk management systems, which is the responsibility of the director responsible for the Group Risk Management and Compliance division. The importance of risk management became more paramount when the Group became a public listed company in the middle of 2006. As a consequence, increasing expectations and demands from its shareholders and stakeholders obliged the Group to be much more certain about its operations and the exposure to risk.

The case study in the NHSGGC revealed a different situation than that in Standard Life and the EIB. Arguably, both risk management and records management are given inadequate priority by the Board of Directors. Records management has long been a function in the Board, but it has never been given much attention for improvement. Although risk management is relatively new to the Board, it has recently gained more attention from the members of the Board. This is understandable as healthcare services are exposed to considerable risk from many quarters. However, in this context the contention of this research is not about comparing which management area should get higher attention from the management but to find a strategic, pragmatic and holistic approach that could lead to better performance and higher level of transparency and accountability of governance. Having discovered such approach in Standard Life, the task at the Board is now to look into customising an integrated approach to meet its needs.

Recent restructuring of the Board has resulted in the expansion of the role of the Audit Committee with the inclusion of risk management under its remit. It was a very good decision, indeed, as the notion of risk management has expanded to embrace almost

every aspect of operation. This was followed by the establishment of a central Corporate Risk Register, which is a one-point entry for complaints to replace existing five risk registers across the Board. However, it is doubtful that the Corporate Risk Register can meet the expectation in the absence of good record keeping practice across the Board. This is no more than a knee-jerk action as there was no strategic approach in ensuring the accuracy and authenticity of records that feed information to the Corporate Risk Register.

It is evident that Standard Life's records management system improved to support the risk management, audit, compliance and other business functions. The EIB even developed an organisation-wide strategic information system namely ISIS, and an electronic records management system namely GED, merely to ensure the accuracy and authenticity of records for the purpose of audit, compliance, risk management and other business functions. In this context, the NHSGGC Board apparently needs a more comprehensive and strategic approach to succeed in implementing its organisational-wide risk management system. What is absent in the Board is the awareness of the importance of good record keeping practice for its sustainability. Arguably, it is partly caused by its public organisation status, which means their existence and operations is funded by the government. This is perceived as the key reason to less demand for good governance and compliance in the Board than that either Standard Life or the EIB.

For Standard Life, its rise and fall is in the hands of the Board of Directors and its senior management. In the context of the EIB, despite its EU public organisation status which means surety should the Bank face a financial crisis, the commitment and enthusiasm of the President of the Bank to demonstrate a high level of transparency and accountability of governance paved the way for the development of the ISIS and the GED. Indeed, such commitment should not be limited to private or financial organisations only, as the benefit goes beyond compliance, transparency and accountability; but as importantly is the sustainability of the organisation.

The NHSGGC Board should have such enthusiasm, commitment and strategy to improve its performance as well as increasing the level of transparency and accountability. An integrated risk and records management is a new strategic approach that is helpful to balance cost and benefit of operation. For the NHSGGC Board to

implement the approach, there are three elements that have to be considered namely, people, process and technology (Knight, 2007). Unfortunately, at present none of the Board members is willing to champion records management.

Undeniably, the awareness of all Board members is best for ensuring efficient implementation of good record keeping practice across the organisation as the change of any Board members, such as the departure of the Public Health Director (*See Section 4.5.5 Records Management in the NHSGGC*), may halt the good record keeping initiative as other Board members do understand its significance and benefit. It is certainly difficult for the Archivist and Records Manager to persuade the Board as he has no direct access to the Board.

Perhaps, the Chief Executive Officer, who is also a member of the Board, should play an active role in promoting the benefit of good record keeping. This is mainly due to his responsibility to ensure efficient administration of the Board. Therefore he should be well-versed with the importance of good record keeping, particularly for underpinning the efficiency of the newly established Corporate Risk Register. The task of persuading other members of the Board, however, is perceived to be challenging because many of them are qualified medical practitioners whose interests are more on improving medical services, and not back office functions. A better option is if the chairman of the Board, with a persuasive power, can be encouraged to adopt the idea of improving record keeping practice at the same time as the risk register is being built to underpin the performance, transparency and accountability of the Board. Then, there would be a greater impact such as in the EIB.

The second element that has to be considered in implementing an integrated risk and records management approach is understanding business processes in the Board. Both risk and records management activities must be embedded in all business processes, then only will records creators and users, that is all the employees, acknowledge the essence of appropriate documentation for the efficiency of their business operations and the organisation as a whole. The benefit of good record keeping must be made apparent to employees and its requirements must be made seamless possible to employees' activities. This would facilitate the cultivation of good record keeping culture, which is essential for the performance of the Board. Once a

good record keeping culture has developed, compliance will be synonymously fulfilled should its regulatory and procedural requirements were considered in designing the integrated risk and records management system.

The third element that has to be considered is choosing the right technology for the efficiency and effectiveness of the integration of risk and records management in the Board. The application and functional requirements of the integrated approach should not be driven by technology; instead the latter should driven by the former. Hence, getting the right people to champion the effort and understanding business processes are pre-requisite for selecting the right technology as the platform for operating the integrated approach. In other words, automating an inefficient system would not produce a better system as the underlying business processes are not streamlined. In addition, an automated system, be it information, records or other applications, does not belongs to information technology professionals alone but all the stakeholders, that are the owners of the business processes. To this end, the technologies have to be fine-tuned to meet specific business process requirements and not the other way round.

The Board had previously installed shared drives for the use of administrative staff to facilitate sharing and access of documents and records, but unfortunately the facility was under utilised as discovered by the Archivist and Records Manager, through a record survey (*See Section 4.5.5 Records Management in the NHSGGC*). To this end, the acquisition of technology should meet users' requirements and add value to what they do. Even, in the case of the EIB where user's requirements were considered in the development of the GED, the system turn out to be under utilised at the initial stage of the implementation because it crucially failed to meet the added value test. Hence, post-implementation review was conducted to identify the actual reasons for under utilisation. This confirmed that technology cannot be the driving force as it is merely a tool that should fit the needs of business processes. The first two elements, people and process, are much more important in implementing an integrated risk and records management approach that ensures the sustainability of the organisation.

It is evident from all the case studies conducted that risk management has become a part of the responsibility of audit committees, besides its traditional responsibility of attesting to the veracity of financial statements. From the literature examined, however,

there was no apparent evidence to relate the cases of poor governance with risk management. With hindsight, the case of corruption of MAS in Victoria, and the Heiner Affair in Queensland, that occurred in the 1980s and 1990s, the notion of risk management was confined solely to attesting to financial statements. Furthermore, good record keeping was not a main agenda item for the then government[2].

Notwithstanding the absence of awareness of transparency and accountability of governance, the crime of breach of trust and mismanagement occurred on a huge a scale. The discussion in the literature was mainly on the loop holes in poor record keeping and the absence of integrity among those involved. Given the current state of records management in Australia and active participation of its records management society at the international level, particularly in producing ISO 15489, it is evident that the Australian government has now prioritised the essential role of record keeping for good governance. Arguably, managing records is like other management fields is essentially about managing risk, which is a tool for achieving organisational goals.

From another perspective, the cases of poor governance particularly, the collapse of Enron, was mainly a result of deliberate and systemic mismanagement due to the absence of good ethical values. In this context, transparency was not a problem. Telling the truth was. Where there can be a link between transparency and accountability, the latter is no guarantee of the former. Arguably, there is no management system in the world that is not exposed to manipulation by its actors, let alone by professionals. This is consistent with the exploitation of expertise by monks, who were traditional experts in writing, but were also the greatest forgers in the twelfth and thirteen century (Clanchy, 1979). In today's electronic environment context, a concerted and systemic mismanagement would be much more difficult to detect due to the very nature of electronic records. Thus, presents a challenge to records management professionals to ensure the documentation of business processes and managing records should not be driven by the technology, but the authenticity and integrity of the evidence in the form of records.

In the case of the killing of 218 elderly patients by Shipman which shocked the world, the weaknesses of the record keeping system that failed to safeguard patients were

[2] Further information is available at http://www.heineraffair.info/site_pages/governor.html

disclosed (Shipman Inquiry, 2005). Shipman's evil crime lasted for 23 years mainly because there was no effective check on the information that he recorded on cremation certificates. He also managed to escape attention through the confidence he established with patients and their families and the respect he earned from professional colleagues, which eventually charmed them mistakenly into placing their trust in him. Above all, was the absence of an integrated record keeping system for monitoring the number of death certificates signed by a given doctor, so no one noticed the large number signed by Shipman.

During the period of the crime, it would have been very costly to scrutinize every single medical record for no reasonable cause. If the victims were younger age patients, the crime would have been detected much earlier as the level of suspicion would have been considerably higher. To this end, having an integrated risk and record keeping system would have enabled the crime to be easily detected providing it was designed with appropriate control and security measures. Such a system certainly will alert the authorities or GMC should a huge number of unexplained deaths by a single doctor be detected again. Perhaps, to make the system more reliable associated risk for every type of treatment or diagnosis can be attached. Therefore, any peculiar trend or results of treatment can be detected more easily. This is to say that having a central risk register as being planned by the NHSGGC is vital in order to provide reliable and trusted healthcare services to the public.

The Hutton and the Butler inquiries disclosed the weaknesses in the administration of the Labour government. The information used by the government that led to the controversial decision was not well documented, despite massive repercussions in the event of it going wrong. Arguably, the political agenda of certain individuals in the governing party overwhelmed the responsibility of the government in ensuring transparency and accountability of governance. It is highly questionable that at such high level no one was given a clear mandate to ensure the accuracy, integrity and secrecy of highly confidential records that are essential for the stability and future of the nation. With hindsight, managing records in the public sector in the UK used to be the responsibility of the Cabinet Secretary, the Head of the Civil Service and through him the other permanent secretaries.

Such an approach needs to be revived if good record keeping is to be effectively practiced in the public sector, and those officials, like chief executives in the private sector, must take responsibility or else should lose their jobs if there is evidence of systemic failure (Moss, 2005). Certainly, the future of a nation should not be jeopardised by poor documentation of governance activities as those appointed by the people of the country must demonstrate transparency and accountability to the governed. Documentation of their actions and decisions must be consistent and according to procedures and regulatory requirements in order to ensure the integrity and reliability of records, which is essential to proof their accountability.

5.3 Conclusions

Three case studies were conducted and five cases of poor governance were analysed in the process of investigating the relationship between records management and accountability of governance. The conclusions of the research are drawn together to match the research objectives, namely:

I. To identify the underlying cause of records management not being regarded as essential for good governance.

From the analysis of case studies and cases of poor governance, two key factors that contributed to the fact that records management is not being regarded as essential for good governance have been identified:

A. Lack of awareness and commitment among senior management of the importance of good record keeping

The essence of record management for good governance relies heavily on the awareness among senior management of the benefit of practising good record keeping. Senior management are often more concerned with business processes rather than documenting those processes. Even, when mismanagement or maladministration was detected, their main focus is to identify the weaknesses or loopholes in their business processes and less attention is given to strengthen the documentation of those processes. Indeed, there must be a champion particularly among the senior management to initiate an effective records management programme. The case studies conducted proved that the level of awareness and commitment from senior management has a significant impact on the status of

records management within the organisation. Apparently, organisations with higher levels of awareness and commitment from senior management possess better records management than organisations with lower level of awareness and commitment from senior management.

The case studies in Standard Life and the EIB showed, perhaps unsurprisingly, that high level of awareness and commitment from senior management facilitates efficient records management initiatives. This in turn improved the efficiency and better performance of the organisation. In the EIB, it was the President of the Bank himself who pledged to increase the level of transparency and accountability of the Bank. Despite being a central bank with legal immunity, the President believes that the bank has to be compliant with Basel II convention in order to demonstrate accountability and be transparent to its shareholders and stakeholders. A huge amount of resource was allocated to establish a bank-wide integrated strategic information system or ISIS, of which an electronic document management system or GED is the backbone. This is an excellent example of a strategic application of a records management system. Arguably, all these were triggered by the presence of awareness among senior management that good record keeping can contribute in achieving transparency and accountability.

Standard Life also possesses a high level of awareness among senior management about the importance of records management to good governance and improving performance. There were two senior management officials who championed records management initiative namely, the then General Manager, Compliance, and the General Manager, Facilities of Standard Life. It was their support and commitment that facilitated the development of a functionally integrated record keeping system by the then records manager, Mrs Knight. The impact of senior management involvement was apparent as most business managers gave their full co-operation to the records manager in the process of developing an integrated risk and records management system.

Operating under tight regulations and compliance regimes is demanding enough, notwithstanding the demutualization of the business, the senior management of Standard Life knew that having an effective and efficient record keeping system is

imperative. Having an integrated risk and records management system is certainly a bonus to the organisation as it not only ensures records are well-managed but they are managed economically. This helps Standard Life to balance its cost and benefit, which in turn ensures its sustainability.

Understandably, it was the purpose, nature of business and culture of the organisation that alerted senior management of the EIB and Standard Life to the need to establish organisational-wide good record keeping practice. Senior management of both organisations are aware that the benefits of good record keeping is not limited just to compliance, transparency and accountability; but as importantly it facilitates the achievement of strategic objectives and sustainability. Indeed, the impact of support and commitment from senior management is paramount to the implementation of organisational-wide good record keeping practice.

Ironically, there was a different tale of records management in the NHSGGC Board. At the time of writing, none of the Board members is willing to champion a records management initiative. Previously, the then Public Health Director was the only senior management officer who was concerned about poor record keeping practice in the Board. However, his departure has brought a halt to the good record keeping initiative planned by the Archivist and Records Manager, Mr. Tough. Although the Head of Board Administration, Mr Hamilton realised that the Board really needed an effective record keeping system particularly to respond to external inquiries, his commitment is not enough to persuade members of the Board to commit themselves to improve the present record keeping situation.

It is perceived that nothing much will change as long as the awareness and commitment of the senior management is absent and there is no external pressure for change. Perhaps, the absence of tight regulations contributes to the lack of awareness of the importance of good record keeping among the members of the Board. Members of the Board should understand that managing records is not about keeping records *per se*, but it is also about destroying records. And they should also be informed that managing records does not necessarily increase cost but can decrease cost by adopting a strategic records management approach.

Arguably, persuading senior management is the biggest obstacle in implementing good record keeping practice. This is mainly because the benefits of good record keeping will not surface immediately and they come in both tangible and intangible forms. It ensures not only compliance with regulations, such as Basel II and FOI legislation, but more importantly the efficiency and effectiveness of business operations. This in turn, enables the organisation to achieve its business objectives and goals.

The Board may be at risk of wasting public money for allocating huge funds to improve its record keeping system as the benefits cannot be seen immediately. What is paramount to the Board is providing quality health care services to the public and ensuring the accuracy of medical records. Therefore, it is perceived that there is still a long way to go for the Archivist and Records Manager of the Board to put into practice his good record keeping initiative across the organisation. Perhaps, adopting a new strategy by integrating risk and records management would attain the attention and commitment of the senior management to implement such an economic and pragmatic approach in the Board.

B. Records management is not embedded in businesses processes

Understanding records means understanding business processes (McDonald, 2002). Records management remains a separate function when records managers fail to understand business process and business managers fail to understand the importance of records management. In these circumstances records management cannot be embedded in business processes which must be aligned with good governance requirements. The case studies proved that the essence of good governance varies between private and public organisations. Private organisations such as financial institutions including Standard Life and the EIB demonstrated higher commitment to implementing an effective and efficient records management system than the public sector. This is mainly a consequence of tight regulations and compliance regimes that require them to demonstrate the accountability and transparency of their business activities.

The role of record keeping in the financial sector is paramount especially after the implementation of SOX in the US that requires financial institutions and business organisations to be certain about the availability and reliability of their records. This confirmed that record keeping is essential for good governance, although it may require considerable effort and resources at the beginning to ensure compliance with Section 302 and Section 404 which require massive documentation of business processes. Complaints by senior management about time and cost required, however, gradually disappeared as companies discovered many fringe benefits of having a controlled environment (Wagner and Dittmar, 2006). This, however, may not be the case for many organisations as the cost of better governance is expensive and therefore will inevitably reduce returns to shareholders. To this end, adopting an integrated risk and records management approach as implemented at Standard Life, perhaps, is the best option as it can provide a balance between meeting regulatory requirements and ensuring sustainability.

On the contrary, public organisations demonstrated less commitment to accountability and transparency. Understandably this is mainly because they are not bound so tightly to regulations and compliance such as the ones faced by financial institutions. Perhaps, the availability of funds and other resources lead to complacency among senior management of public organisations. Relatively, the repercussion of mismanagement is less fatal to the sustainability of public organisations than private organisations.

In addition, non-profit making status partly discourages the management of public organisations from adopting a rigorous effort to improve the governance of organisations. This finding is consistent with Meijer's (2000) finding that public organisations that are bound to a high degree of control through legal regulations and hierarchical procedures demonstrate better accountability of governance than for public organisations with a low degree of control. Good governance can only be achieved with the availability of reliable and authentic records to facilitate business processes and decision making. Lack of commitment to good governance means lack of commitment to improve records management. As a consequence, records management remains unimportant and marginalised from their business operations.

It is evident from the case studies conducted that one of the key reasons why records management is not considered essential for good governance is because good record keeping practice is not embedded in business processes. In the case of Standard Life, good record keeping practice has been nurtured and embedded in its business processes, particularly since 2001 when the management planned for demutualization. This ensures that business evidence is captured in order to achieve efficiency and effectiveness of operations as well as meeting shareholders' and stakeholders' expectations.

To this end, Standard Life and its auditors must be certain that necessary records are retained and are readily retrievable. In the EIB, the implementation of the Bank-wide electronic document management system or GED is evidence that records management is embedded in business processes across the Bank. The process of identifying working documents and records is more efficient because there are designated workspaces. Working documents are made available in a workspace known as working area, which is a collaborative workspace where people can alter documents according to their privileges. Meanwhile completed documents are permanently stored in a workspace known as knowledge centre which is a referral centre for all EIB staff, where completed documents are accessible but not editable. To this end, consistency can be assured through control mechanisms embedded in the GED system.

II. To identify the role of records in the accountability of governance

Accountability is an evidence based process that occurs after activities have been executed or decisions have been taken. Records, and the evidence that they contain, are the instruments by which organisations can promote a climate of trust and overall commitment to good governance. Accountability of governance can only be demonstrated when adequate evidence is garnered through effective and efficient record keeping systems. It is important for an organisation to demonstrate accountability not only to its shareholders and stakeholders, but also to the public as part evidence of social responsibility.

The case studies showed that organisations with higher commitment to demonstrate accountability, such as the EIB and Standard Life, possess better record keeping

practice. It was the commitment of the President of the Bank to increase transparency to demonstrate accountability that led to the establishment of the Bank-wide integrated strategic information system, of which GED is the back bone. For Standard Life, demonstrating accountability is vital, not only to meet compliance and regulatory requirements but equally importantly its shareholders and stakeholders. Thus, the development of an integrated risk and records management approach was a major effort to establish an essential tool to underpin efficient operations, transparency and accountability.

On the contrary, the NHSGGC Board does not practice good record keeping partly because it is not bound to such stringent regulations as the former. Although the governance of the Board is attested by internal and external auditors, the case study discovered considerable room for improving record keeping practice, which in turn could increase the efficiency and efficacy of the Board. The inefficiency of record keeping was mainly felt by the Head of Board Administrator, Mr Hamilton, who sometimes struggled to find relevant information to respond to media inquires raising questions of the accountability of the Board.

There were cases against the Board, which were eventually settled out of court for undisclosed amount of compensation. Although the amount is thought to be judged tolerable by the Board, public money has to be spent wisely. It is certainly wasteful if compensation were paid just because of the unavailability of relevant records for the Board to defend itself. This should not be allowed to continue if the Board is committed to demonstrate its accountability as a string of failures eventually will damage reputation and decrease trust among the public. Hence, it is easy to understand why Mr. Hamilton insisted that an organisational-wide good record keeping system is desperately needed to improve the efficiency, transparency and accountability of the Board.

It is evident that records can also demonstrate fake accountability such as in the collapse of Enron. But these are fake records that provide fake evidence. In other words fake records demonstrate fake accountability. Fake records can be forged by unethical individuals, could be laymen or professionals, for the sake of hiding their mismanagement or corruption. The collapse of Enron proved that the presence of

good record keeping alone is inadequate to demonstrate accountability of governance in the absence of good ethical values which eventually led to the collapse of one of the largest firms in the US. Frauds on this scale can only be perpetrated by those who know exactly what they are doing. Those involved must have had two sets of records. The first set would have contained fake records that are to be made available to the public. The second set would have contained actual records that are made available to ring members only.

Surprisingly, the external auditors, Arthur Andersen, one of the biggest and most trusted audit firms in the world, compromised their professional standards by committing the infamous crime - breach of trust. Records merely function as a tool that provides evidence of an event or a transaction. Hence, in the absence of good ethical values, records can be deliberately manipulated by irresponsible individuals. To this end, corporate governance failed to achieve its objectives simply because the actors failed to perform their jobs responsibly. Arguably, poor governance as much as corruption was the key reason for the collapse of Enron.

Other cases of poor governance, such as mismanagement and corruption in the Australian government in the 1980s and 1990s, murders by Shipman, have cost considerable amounts of public money to investigate. To this end, it is certainly better to prevent rather than to cure. In such situations, accountability can no longer be sustained by informal relations of trust, audits must be formalised as a check and balance mechanism that facilitates the process of determining accountability, effectiveness and integrity of an employee, a department and even an organisation. Audits are simply answers to problems of accountability (Power, 1994). Auditors are bound by a professional code of ethics that requires them to be independent and transparent in reporting their findings.

Regardless of the degree of scrutiny, audits can only be effective when auditors stick rigidly to their code of ethics. The collapse of Enron was partly a result of the breach of trust of Enron auditors and a failure of the whole audit process. This situation was forecast more than twenty years ago when Power (1994) argued audit was introduced largely when trust has broken down, and yet the spread of audit actually creates the very distrust it is meant to address, culminating in ‘a regress of mistrust’ in which the

performances of auditors and inspectors are themselves subjected to audit'. The impact of mismanagement and breach of trust varies depending on the context of the mismanagement, but at best could damage reputation and at worst lead to the collapse of the organisation itself.

It is evident, from the case studies, that organisations with higher commitment to accountability possess not only effective audit committees and, legal and compliance divisions but also good record keeping practice. This is mainly because auditors know that authentic and up-to-date records are keys to their tasks. Therefore, the pre-requisite is they have to ensure good record keeping is practiced across the organisation to facilitate audit processes. It was discovered that audit committees in the EIB and Standard Life are given higher authority than that in the NHSGGC Board. Hence, it is not a surprise the EIB and Standard Life possess better record keeping practice in comparison to the NHSGGC Board. In conclusion, records have significant role and good record keeping is central to the accountability of governance. It is far more important in organisations that operate under tight regulations and compliance regimes than to public organisation that operate under less demanding environments.

III. To identify the relationship between risk management and managing records.

Theoretically, there is a symbiotic relationship between risk management and managing records. Records management ensures the availability of records for risk assessment and systematically captured the records of risk management processes. Risk management is a cyclical and dynamic process. Therefore, records that are produced must be kept for future assessment to determine whether recommended risk mitigation has been followed by relevant business process owners. Risk management aims to reach a state whereby all risks and their mitigation can be anticipated by an organisation. Therefore, whenever a risk occurs, all necessary resources to mitigate the risk are readily available.

Risk is prioritised based on the likelihood and the impact of occurrence. Business operations of high level of likelihood and impact should be given highest priority, whereas business operations of least likelihood and impact should be given least priority or perhaps tolerable to the organisation. It is dangerous to confine risk

management to compliance as risk management is about clarity and the ability to not only identify the correct opportunities but also to maintain discipline in pursuing them (Sharon, 2005a). Hence the biggest risk of all is to take no risk, and thereby fail to take opportunities.

In reality, however, there is no evidence of such relationship until the case study in Standard Life was conducted. The case study discovered a pragmatic record keeping approach that integrates risk and records management. The risk scorecards produced by the Group Risk Committees were subsequently used by the Records Management division to establish records retention schedules. Previously, risk scorecards are meant for business process owners only, but now the benefit has been extended as they become an invaluable source of information for the Records Management division. As a consequence, the process of allocating retention period is more efficient as associated risks have been identified in risk scorecards by the authorised Group Risk Committees.

The availability of such highly reliable input means the process of managing records is more economic as the priority is based on risk identified by the Group Risk Committees. Records of higher risk must be given higher priority whereas records of lower risks should be given lower priority. Perhaps, under some circumstances records of lower risk can be destroyed prematurely if the cost associated with such records is much lower than the cost of keeping them. Records managers and senior management must understand that managing records is not only about keeping records but it is also about destroying records. Destroying records can increase efficiency but it must be done with careful consideration to avoid unexpected risk. Indeed, this is the strength of the integrated risk and records management approach.

The integration of risk and records management has a bright future as its synergy enables the identification of not only risk but also business opportunities, maintains competitive advantage as well as facilitating the achievement of the strategic objectives of the organisation (Sharon, 2005b). It is evident that Standard Life is benefiting from the integrated approach. Hence, it is not surprising when the EIB Inspectorate General showed a great interest in the integrated approach. With infrastructure in place including the GED, there is a great potential for the Bank to

adopt what is being implemented in Standard Life. It is evident that integrating risk and records management is no longer rhetoric but a pragmatic approach that can ensure the sustainability of the organisation as proved by Standard Life. Risk management and managing records are complementing each other and beneficial to the organisation as a whole.

Having discovered the benefits of integrated risk and records management approach, it is suggested that the NHSGGC Board should consider a change to its present record keeping practice. The Board must be convinced that integrated risk and records management enables them to achieve their strategic objectives. However, there is a pre-requisite. Good record keeping practice and risk management elements must be nurtured and embedded in all business activities across the organisation. This can be realised by forming a working committee comprising the Audit Committee, Archivist and Records Manager and Risk Management team to implement such an approach across the Board. Only then, will the benefits of the integrated approach gradually surface. The Board as a whole would then be able to seize the opportunity and function effectively while remaining aware of the associated risks. If this happens transparency and accountability will not be hard to demonstrate and sustainability can be assured.

5.4 Recommendations

In order to enhance the role of records management in underpinning the accountability of governance, five recommendations have been identified, namely:

i. Instigate and develop awareness of the importance of good records management. The awareness of the importance of records management for transparency, accountability and sustainability of the organisation is essential at all levels particularly, the senior management level. The Board of Directors must be convinced that records management is not only about keeping records, but also about destroying unnecessary records, which in turn enables economic efficiency and avoids unnecessary risk. The awareness among senior management would facilitate the implementation of good record keeping practice such as, in the EIB and Standard Life. To this end, records management professionals need to understand the nature of business and culture of the organisation in order to determine

appropriate strategies for implementing good record keeping. Records management professionals must be able to identify the strategic role of records management in achieving organisational goals in order to justify the essence of practising good record keeping to the organisation. It would be damaging if records management professionals cannot see the wood for the trees. Detailing good record keeping practices should not be alienated from the organisation's strategic goals. Failure to do so will lead to adversities which could tarnish the reputation of the records management profession and even worse leave it isolated.

ii. Embed good record keeping practice into business processes.
Records management professionals must find ways of how good record keeping practice can be embedded into all business functions. The essence of authentic and reliable records in decision making, risk management, audit and internal controls is proven, such as in the case study in the EIB and Standard Life. In other words, record keeping requirements must be made user friendly possible if not seamless to records creators and users as imposing the requirements should not be an impediment to business tasks. In addition, records management professionals must be positive thinking and avoid being prejudiced against business managers' willingness to adopt good record keeping practice as such a perception is not helpful in developing good working relationships. It is a fact that business managers want to have an effective record keeping system but they have other priorities as asserted by the Group Records Manager for Standard Life.

iii. Integrate risk and records management.
Managing records requires a new approach that can align its role with organisational goals. It is recommended that an integrated risk and records management approach discovered in the research could be the best option for enabling records managers to play a more significant role in leading the organisation to not only transparency and accountability but more importantly sustainability. To this end, records managers need to change their mindset, if not experience a paradigm shift, that managing records is about balancing costs and benefits to the organisation. Records managers must be able to persuade senior management and particularly the board of directors to adopt good record keeping practice in the organisation. This in turn, would facilitate collaboration with other

professionals, such as the experience of Standard Life. In order to persuade senior management and to establish collaboration with other professionals, records managers must learn to understand their languages. In other words, records management professionals need to be pro-active if records management is to be recognised by others.

iv. Enhance the role of higher learning institutions and professional bodies.
The quality of records management professionals in the future is mainly dependant on the role of higher learning institutions and professional bodies through their relevant education and training. Higher learning institutions should recruit more students from IT-related or computer science background. This can be done by promoting the program to potential students from these fields. Arguably, with strong IT background they can become capable records manager just like the former Group Records Manager of Standard Life. Another option that can be adopted by higher learning institutions and professional bodies is enhancing their curriculum by including more IT elements and risk management. The case studies in Standard Life and the EIB showed that there is an increasing demand for records managers to understand risk management, compliance and legal requirements in managing records. The understanding of risk management would facilitate collaboration between records managers and other professions as all share a common understanding towards achieving organisational goals. To this end, an initiative to implement good record keeping systems would be much easier done. In other words, it is essential to diversify the knowledge based on new entrants and allow them to maximise their potential. It also helps diminish a sense of inferiority in records managers and enables them to collaborate with other professions in their organisations.

v. Further research on the integration or risk and records management
Having analysed risk management and managing records, there is huge potential for integrating both management areas as the synergy enables an organisation to achieve cost efficiency. Records management professionals and IT experts should collaborate exploring the potential. Producing software that integrates both risk and records management would be a much better option for organisations instead of buying or using records management software only. If this can be done, an

organisation as a whole will be more certain about the availability, authenticity and reliability of records and risk exposure. This in turn, will facilitate strategic decision-making thus enables the organisation to be more competitive. It is recommended that further research into this area would enable the discovery of the true value and benefits of the integrated approach to organisations. This will eventually redeem the records management profession from being a passive player to an active team player alongside other professions in contributing to the achievement of organisational goals.

In a nutshell, if an organisation such as Standard Life continuously makes profit under high regulatory regimes that require comprehensive and effective record keeping, there is no reason why public organisations should continue spending public money on unnecessary costs that can easily be avoided if effective record keeping systems were in place. The benefits of sound records management come in both tangible and intangible forms, though they will not surface immediately. Effective records management does not only ensure compliance with the FOI, but more importantly it improves the efficiency and effectiveness of an organisation. An integrated record and risk management approach is a much better option that can be adopted by public organisations in achieving their business goals and increasing value for money by balancing costs and benefits that is essential for the sustainability and accountability of the organisation.

BIBLIOGRAPHY

"'Female champion' Hewitt discriminated against man". *The Independent.* 12 October 2005. http://news.independent.co.uk/uk/politics/article318857.ece (12 October 2005).

A Modern Archives Reader: Basic Reading on Archival Theory and Practice by Maygene F. Daniels and Timothy Walch (ed). (1984). Washington: National Archives Trust Fund Board.

Accenture. (2004). *eGovernment Leadership: High Performance, Maximum Value*. http://www.accenture.com/NR/rdonlyres/D7206199-C3D4-4CB4-A7D8-846C94287890/0/gove_egov_value.pdf (20 June 2007).

AIRMIC, ALARM, and IRM. (2002). *A Risk Management Standard.* London: AIRMIC, ALARM, and IRM.

Allinson, C. (2001). Information system audit trails in legal proceedings as evidence. *Computers & Security.* 20 (5), pp. 409-21.

An, X. (2003). An integrated approach to records management. *The Information Management Journal,* July/August, pp. 24-30.

Atkinson, E. (2002). Much ado about metadata. *Records Management Journal*, 12(1), pp 19-23.

Audit Commission. (2006). *Learning the Lessons from Financial Failure in the NHS*. http://www.audit-commission.gov.uk/Products/NATIONAL-REPORT/9BCDC50E-B139-46f8-B559-B890590FA40A/financial_failure_nhs.pdf (14 December 2006).

Audit Scotland. (2006). *Overview of the Financial Performance of the NHS in Scotland 2005/06*. http://www.audit-scotland.gov.uk/publications/pdf/2006/06pf10ag.pdf (14 December 2006).

Australian Public Service Commission. (2003). *The Australian Experience of Public Sector Reform. Canberra: Commonwealth of Australia*. http://www.apsc.gov.au/about/exppsreform.pdf (19 April 2006).

Baier, A.C. (1995). *Moral Prejudices: Essays on Ethics*. Cambridge, Mass.: Harvard University Press.

Bansal, P. and Kandola, S. (2003). Corporate social responsibility: why good people behave badly in organisations. *Ivey Business Journal*, March/April 2003. http://www.iveybusinessjournal.com/view_article.asp?intArticle_ID=469 (28 June 2006).

Bantin, P.C. (2001). *Strategies for Managing Electronic Records: Lessons Learned from the Indiana University Electronic Records Project*. http://www.indiana.edu/~libarch/ER/bantin-saa2001.pdf (20 June 2007).

Bearman, D. and Trant, J. (1998). Authenticity of digital recources: towards a statement of requirements in the research process. *D-Lib Magazine*. http://www.dlib.org/dlib/june98/06bearman.html. (14 May 2004).

Bearman, D. (1993). Record-keeping systems. *Archivaria*, 36, Autumn, pp.16-36.

Bearman, D. (1989). Archival Methods. *Archives and Museums Technical Report #9.* Pittsburgh: Archives and Museums Informatics. http://www.archimuse.com/publishing/archival_methods/#intro (20 July 2005).

Beechey, B. (1997). Corruption, incompetence and death: the 'benefits' of privatisation. *Green Left Weekly*. http://www.greenleft.org.au/back/1997/276/276p7.htm (22 June 2006).

Bichard Inquiry. (2004). *The Bichard Inquiry Report*. London: The Stationery Office.

Boelk, W. (2004). The relationship between records management and archives. *Archives Society of Alberta Newsletter,* 24(1), Fall. http://www.archivesalberta.org/vol24_1/woelk.htm (28 May 2005).

Brenkert, G.G. (1998). Trust, morality and international business. *Trust Within and Between Organisations: Conceptual Issues and Empirical Applications by Christel Lane and Reinhard Bachmann (eds.)*. New York: Oxford University Press. pp. 273-97.

British Computer Society. (2000). *Expert Panels: Legal Affairs Expert Panel: Submission to the Criminal Court Review, Lord Justice Auld*. http://www.computerevidence.co.uk/Papers/LJAuld/BCSComputerEvidenceSubmission.htm (9 May 2007).

Brodsky, D. *et al*. (2003). Trend in corporate governance …the new role of audit committee. *Executive Action*, (63), July 2003.

Brosius, M. (2003). Ancient archives and concept of record-keeping: an introduction. *Ancient Archives and Archival Traditions: Concept of Record-keeping in the Ancient World by Maria Brosius (ed.)*. Oxford: Oxford University Press, pp. 1-16.

Buckland, M. (1991). *Information and information system*. Greenwood Press, New York.

Buzzard, K. (1999). Computer security – what should you spend your money on? *Computers & Security,* (18), pp. 322-34.

Chartered Institute of Public Finance and Accountancy. (2002). *An Assessment of the Possible Applications of the Public Sector Audit Model to the UK Private Sector.* http://www.cipfa.org.uk/pt/download/0969audit_model.pdf (31 January 2006).

Clanchy, M.T. (1979). *From Memory to Written Record*. London: Edward Arnold.

Coffee, J.C. (2006). *Gatekeepers: the Professions and Corporate Governance*. Oxford: Oxford University Press.

Colledge, G. and Cliff, M. (2003). The implications of the Sarbanes-Oxley Act: it's time to take records management seriously. *KMWorld*, 12(8). http://www.kmworld.com/publications/whitepapers/Records/colledge&cliff.pdf (19 September 2005).

Committee of Privy Councillors. (2004). *Review of Intelligence on Weapons of Mass Destruction*. London: House of Commons.

Committee of Standard in Public Life. (2006). *Annual Report of the Committee Standards in Public Life 2006.* http://www.public-standards.gov.uk/upload/assets/www.public_standards.gov.uk/cspl_web.pdf (24 September 2006).

Committee on the Financial Aspects of Corporate Governance. (1992). *The Report of Committee on the Financial Aspects of Corporate Governance*. London: Gee Publishing.

Conway, P. (1996). *Preservation in the Digital World*. http://www.clir.org/pubs/reports/conway2/ (20 June 2007).

Cook, T. (2006). Remembering the future: appraisal of records and the role of archives in constructing social memory. *Archives, Documentation and Institutions of Social Memory: Essays from Sawyer Seminar by Francis X. Blouin Jr and William G. Rosenberg (eds.)*. Michigan: The University of Michigan Press, pp. 169-181.

Cox. R.J. (2006). *Ethics, Accountability and Recordkeeping in a Dangerous World*. London: Facet Publishing.

Cox, R.J. (2001). *Managing Records as Evidence and Information*. Connecticut: Quorum Books.

Craig, B.L. (2002). Rethinking formal knowledge and its practices in the organisation: the British Treasury's Registry between 1900 and 1950. *Archival Science*, 2(1-2), pp. 111-136.

Cullen, C.T. (2000). Authentication of digital objects: lessons from a historian's research. *Authenticity in a Digital Environment*. Washington: Council on Library and Information Resources, pp. 1-7. http://www.clir.org/pubs/reports/pub92/pub92.pdf (5 May 2004).

Cumming, K. (2005). Metadata matters. *Managing Electronic Records by Julie McLeod and Catherine Hare (eds.)*. London: Facet Publishing, pp. 34-49.

Cumming, K. (2001). *Metadata: the Convergence of Theory and Reality*. https://www.rmaa.org.au/StaticContent/StaticPages/pubs/nat/natcon2001/section007.pdf (26 May 2004).

Cunningham, A. (1997). Ensuring essential evidence – changing archival and records management practices in the electronic recordkeeping era. *Provenance of the Web Magazine*, 2(2), Spring. http://www.netpac.com/provenance/vol2no2/features/evidence.htm (20 January 2000).

Currall, J. (2006a). Security and the digital domain. *Record Keeping in a Hybrid Environment: Managing the Creation, Use, Preservation and Disposal of Unpublished Information Objects in Context by A. Tough and M. Moss (eds.).* Oxford: Chandos Publishing, pp. 47-68.

Currall, J. (2006b). *Proceedings 1st Northumbria International Witness Seminar Conference: Exploring the Essence of Records Management: Engaging with Experts,* St James Park, Newcastle upon Tyne, United Kingdom, 4-5 May 2006.

Currall, J. and Moss, M. (2006). We are archivists, but are we ok? *The Second Asia-Pacific Conference for Archival Educators and Trainers*, Tokyo, Japan. 17-20 October 2006.

Currall, J. (2005). *Personal interview with James Currall*, 30 August 2005, in his office in Computing Service Department, University of Glasgow.

Currall, J. *et al.* (2002) *"No Going Back?" the Final Report of the Effective Records Management Project*. (Glasgow: University of Glasgow). http://www.gla.ac.uk/InfoStrat/ERM/Docs/ERM-Final.pdf. (20 December 2003)

Curtin, G.C. *et al.* (2004). The World of e-Government. Binghamton: Haworth Press.

Davies, A. (1999). *A Strategic Approach to Corporate Governance*. London: Gower Publishing Limited.

Davison, R.M., Wagner, C. and Ma, L.C.K. (2003). From government to e-government: a transition model. *Information Technology & People*. 18(3), pp. 280-299.

Day, P. and Klien, R. (1987). *Accountabilities: Five Public Services.* London: Tavistock Publications.

Dietel, J.E. (2000). Improving corporate performance through records audits. *The Information Management Journal*. 34(2), April, pp. 18-26.

Digitale Bewaring Testbed. (2003). *From Digital Volatility to Digital Permanence: Preserving Database*. http://www.digitaleduurzaamheid.nl/bibliotheek/docs/volatility-permanence-databases-en.pdf (17 March 2006).

Department of Defense (2002). *Design Criteria Standard for Electronic Records Management Software Applications*. Washington: Pentagon.

Duff, W. (2004). *Metadata: Setting the Scene or a Basic Introduction*. http://www.asu.edu/ecure/2004/duff/index.html (15 March 2005).

Duff, W. (2003). Metadata in digital preservation: foundations, functions and issues. *Metadata in Preservation: selected papers from ERPANET seminar held in Marburg, 3-5 September 2003 by Frank M. Bischoff, Hans Hofman and Seamus Ross (eds.)*. Marburg: Archivschule Marburg, pp. 27-38.

Duff, W., Hofman, H. and Troemel, M. (2003). *Getting What You Want, Knowing What You Have, and Keeping What You Need*. http://www.erpanet.org/events/2003/marburg/erpaTraining-Marburg_TrainingMaterial.pdf (20 June 2007).

Duff, W. (2001). Letter from the guest editor: issues of authenticity, social accountability, and trust with electronic records. *The Information Society*, 17, pp. 229-31.

Duff, W. (1996). Ensuring the preservation of reliable evidence: a research project funded by the NHPRC. *Archivaria*, 42, pp. 28-45.

Dunleavy, M. (2006). *Proceedings 1st Northumbria International Witness Seminar Conference: Exploring the Essence of Records Management: Engaging with Experts,* St James Park, Newcastle upon Tyne, United Kingdom, 4-5 May 2006.

Duranti, L. (2001a). Concepts, principles, and methods for the management of electronic records. *The Information Society*, 17, pp. 271-9.

Duranti, L. (2001b). The impact of digital technology on archival science. *Archival Science*, 1(1), pp. 39-55.

Duranti, L. (1998a). *Keeping the Records Straight*. http://www.publicaffairs.ubc.ca/ubcreports/1998/98mar05/98mar5pro.html (21 May 2004).

Duranti, L. (1998b). *Diplomatics: New Uses for an Old Science*. Lanham, Md.: Scarecrow Press.

Egbuji, A. (1999). Risk management of organisational records. *Records Management Journal*, 9(2), August, pp. 93-116.

Electronic Resource Preservation and Access Network. (2004). *European Investment Bank Case Study Report*. Glasgow: ERPANET.

Esmail, A. (2005). Physician as serial killer – the Shipman case. *New England Journal of Medicine*, 352 (18), May, pp. 1843-44.

European Investment Bank. (2006a). *Annual Report 2005, Vol.1: Activity Report*. http://www.eib.org/report/pdf/ar2005en.pdf (20 November 2006).

European Investment Bank. (2006b). *Audit Committee: Annual Report to the Board of Governors for the 2005 Financial Year*. http://www.eib.europa.eu/Attachments/general/reports/ac_2005_en.pdf (20 June 2007).

Financial Services Authority. (2003). Reducing *Money Laundering Risk: Know-Your-Customer and Anti-Money Laundering Monitoring.* http://www.fsa.gov.uk/pubs/discussion/dp22.pdf (8 November 2006).

Finer, H. (1941). Administrative responsibility and democratic government. *Public Administration Review*, 1, pp. 335-50.

Fisher, P. (2004). Electronic records as evidence: the case for Canada's new standard. *The Information Management Journal*, March/April, pp. 39-45.

Friedrich, C.J. (1940). Public policy and the nature of administrative responsibility. *Public Policy by C.J. Friedrich and E.S. Mason (eds.)*, Cambridge: Harvard University Press. Cited in Mulgan (2000).

Fukuda-Parr, S. and Ponzio, R. (2002). *Governance: Past, Present, Future Setting the Governance Agenda for the Millennium Declaration*. http://unpan1.un.org/intradoc/groups/public/documents/un/unpan006224.pdf (8 November 2004).

Fukuyama, F. (1995). *Trust: the Social Virtues and the Creation of Prosperity*. London: Hamish Hamilton.

Getronics. (2005). *Reduce Risks and Improve Productivity Through Efficient Record-Keeping*. http://www.getronics.com/NR/rdonlyres/ehfkvw637k5qvlyv7etcfnfjhnsougp2tf2xyojkr2zgibw7bh5alaqciam332zatbphify6mes7dxrw6m4tbx7odud/wp_gartner_records_management_reduce_risk.pdf (17 September 2005).

Gilliland-Swetland, A.J. (2000). *Introduction to Metadata: Pathways to Digital Information*. http://www.getty.edu/research/conducting_research/standards/intrometadata/2_articles/index.html (30 January 2006).

Giri, A. (2000). Audited accountability and the imperative of responsibility: beyond the primacy of the political. *Audit Cultures by Marilyn Strathern (ed.).* London: Routledge, pp. 173-95.

Government Accountability Office. (2005). *Tax-Exempt Sector: Governance, Transparency, and Oversight are Critical for Maintaining Public Trust*. http://www.gao.gov/new.items/d05561t.pdf (17 October 2005).

Government of Canada. (2001). *Record Keeping Metadata Requirements for the Government of Canada*. http://www.imforumgi.gc.ca/products/meta/metadata3_e.pdf (7 February 2006).

Hänger, A. (2003). Electronic records management metadata: the DOMEA-Concept in Germany. *Metadata in Preservation: Selected Papers from ERPANET Seminar held in Marburg, 3-5 September by Frank M. Bischoff, Hans Hofman and Seamus Ross (eds.)*. Marburg: Archivschule Marburg, pp. 161-83.

Hansen, L. (2003). The digital long-term archive at the Swedish Social Insurance Administration (SIA) – flexible use of archival standards and contextual metadata. *Metadata in Preservation: Selected Papers from ERPANET Seminar held in Marburg, 3-5 September by Frank M. Bischoff, Hans Hofman and Seamus Ross (eds.)*. Marburg: Archivschule Marburg, pp. 143-67.

Harrison, W. (2004). The digital detective: an introduction to digital forensic. *Advances in Computers*, 60, pp. 75-119.

Harvey, R. (2003). Preserving Digital Documentary Heritage in Libraries: What Do We Select?, *Symposium 2003: Preservation of Electronic Records: New Knowledge and Decision-making*, Ottawa, Canada, 15-18 September 2003.

Healy, P.M. and Palepu, K.G. (2003). The fall of Enron. *Journal of Economic Perspectives*. 17(2), Spring, pp. 3-26.

Hedstrom, M. (2002). Archive, memory, and interfaces with the past. *Archival Science*, 2(1), pp. 21-43.

Hedstrom, M. (2000). Recordkeeping metadata: definitions and relationships to other types of metadata. *Working Meeting on Recordkeeping Metadata*, The Hague, Netherlands, 5-7 June 2000. http://www.archiefschool.nl/docs/hedshowt.pdf (30 May 2005).

Higgs, D. (2003). *Review of the Role and Effectiveness of Non-Executive Directors.* London: Department of Trade and Industry.

HM Treasury. (2004). *The Orange Book: Management of Risk – Principles and Concepts*. London: HMSO. http://www.ogc.gov.uk/sdtoolkit/reference/ogc_library/related/orange-book.pdf (6 October 2005).

Hofman, H. (2005). The use of standards and models. *Managing Electronic Records by Julie McLeod and Catherine Hare (eds.).* London: Facet Publishing, pp. 18-33.

Horsman, P. (2006). Identity and paradigm shift. *Proceedings 1st Northumbria International Witness Seminar Conference: Exploring the Essence of Records Management: Engaging with Experts,* St James Park, Newcastle upon Tyne, United Kingdom, 4-5 May 2006.

House of Representatives, Standing Committee on Legal and Constitutional Affairs. (2004). *Crime in the Community: Victims, Offenders and Fear of Crime*. Vol.2. Canberra: Commonwealth of Australia.

Hurley, C. (2005). Recordkeeping and accountability. *Archives: Recordkeeping Society by Sue McKemmish et al*. (eds.). New South Wales: Charles Sturt University, pp. 223-53.

Hurley, C. (2004). What, if anything, is records management? *RMAA Conference,* Canberra, September 2004.

Hurley, C. (1999a). *Heiner on Sunday – Again*. http://www.gwb.com.au/gwb/news/goss/sunday1.htm (9 May 2006).

Hurley, C. (1999b). *Shredding of the "Heiner Affair" Records: an Up-dating Summary*. http://www.caldeson.com/RIMOS/summary.html (19 April 2006).

Hutton, B. (2004). *Report of the Inquiry into the Circumstances Surrounding the Death of Dr David Kelly C.M.G*. London: The Stationery Office.

Hynes, D. (1996). Michel Foucault's the archaeology of knowledge. *The Codgito*. 4. http://www.mun.ca/phil/codgito/vol4/v4doc1.html (18 March 2005).

Independent Commission on Good Governance in Public Services (The). (2004). *The Good Governance Standard for Public Services.* London: Office for Public Management Limited and the Chartered Institute of Public Finance and Accountancy.

Information Security Forum. (2003). *Information Risk Management and Corporate Governance: Workshop Report.* London: Information Security Forum.

Information Systems Audit and Control Association. (2003). I*S Auditing Guideline: System Development Life Cycle (SDLC) Reviews*. http://www.isaca.org/AMTemplate.cfm?Section=Standards,_Guidelines,_Procedures_for_IS_Auditing&Template=/ContentManagement/ContentDisplay.cfm&ContentID=26905 (4 December 2006).

International Council on Archives (The). (2004). *Electronic Records: a Workbook for Archivists*. http://www.ica.org/sites/default/files/Study16ENG_5_2.pdf (22 June 2007).

International Records Management Trust. (1999a). *Managing Public Sector Records: a Study Program – Preserving Records*. http://www.irmt.org/download/DOCUME%7E1/EDUCAT%7E1/MPSR/preserving.pdf (15 January 2004).

International Records Management Trust. (1999b). *Managing Public Sector Records: a Study Program - glossary*. http://www.irmt.org/download/DOCUME%7E1/EDUCAT%7E1/MPSR/glossary.pdf (5 February 2004).

InterPARES. (2002). *Findings on the Preservation of Authentic Electronic Records.* http://www.gseis.ucla.edu/us-interpares/pdf/InterPARES1FinalReport.pdf (21 June 2007).

InterPARES. (2001). *Authenticity Task Force final report*. http://www.interpares.org/book/interpares_book_d_part1.pdf (20 October 2003).

Institute of Chartered Accountants in England and Wales (The). (1999). I*nternal Control: Guidance for Directors on the Combined Code*. http://www.ecgi.org/codes/documents/turnbul.pdf (12 November 2004).

Jenkinson, H. (1949). *Guide to the Public Records: Part 1: Introductory*. London: Public Record Office.

Jenkinson, H. (1954). Modern archives: principles and techniques. *Selected Writings of Sir Hilary Jenkinson by Roger H. Ellis and Peter Walne (eds.).* Chicago: Society of America Archivists.

Johnston, G. (2006). *Proceedings 1st Northumbria International Witness Seminar Conference: Exploring the Essence of Records Management: Engaging with Experts,* St James Park, Newcastle upon Tyne, United Kingdom, 4-5 May 2006.

Jones, G. W. (1992). The search for local accountability. *Strengthening Local Government in the 1990s* by S. Leach (ed.) cited in Mulgan (2000).

Kaler, J. (2002). Responsibility, accountability and governance. *Business Ethics: A European Review*, 14(4), October, pp. 327-34.

Kinnell, H.G. (2000). Serial homicide by doctors: Shipman in perspective. *British Medical Journal*, 321(7276), December, pp. 1594-97.

Knight, K. (2007). Everything but the technology … a view from the financial services. *Records Management Society Scotland Group Meeting*, Edinburgh, 11 January 2007.

Kondo, S. (2002). Fostering dialogue to strengthen good governance. *Public Sector Transparency and Accountability: Making It Happen*. Paris: OECD.

Laffan, B. (2003). Auditing and accountability in the European Union. *Journal of European Public Policy*, 10(5), October, pp. 762-77.

Lane, C. (1998). Theories and issues in the study of trust. *Trust Within and Between Organisations: Conceptual Issues and Empirical Applications by Christel Lane and Reinhard Bachmann (eds.)*. New York: Oxford University Press, pp. 1-30.

Leach, J. (2003). Improving user security behaviour. *Computers & Security*, 22(8), pp. 685-92.

Lemieux, V. (2006). *Proceedings 1st Northumbria International Witness Seminar Conference: Exploring the Essence of Records Management: Engaging with Experts,* St James Park, Newcastle upon Tyne, United Kingdom, 4-5 May 2006.

Leroux, O. (2004). Legal admissibility of electronic records. *International Review of Law Computers & Technology*. 8(2), July, pp. 193–220.

Levy, D.M. (2001). *Scrolling Forward: Making Sense of Documents in the Digital Age*. New York: Arcade Publishing.

Levy, D.M. (2000). Where's Waldo?: reflections on copies and authenticity. *Authenticity in a Digital Environment*. Washington: Council on Library and Information Resources, pp. 24-41. http://www.clir.org/pubs/reports/pub92/pub92.pdf. (6 May 2004).

Limbachia, K. (2005). Ever-increasing complexity favours the specialists regulation, compliance and governance: many institutions choose to hand the task to their custodians. *Financial Times* (London). 6 September 2005.

Lindeberg, K. (1999). *The Beginnings of Shreddergate: the Shredding of the Heiner Inquiry Documents and Related Materials*. http://www.gwb.com.au/gwb/news/goss/history99.doc (8 May 2006).

Lion, R. and Meertens, R.M. (2005). Security or opportunity: the influence if risk-taking tendency on risk information preference. J*ournal of Risk Research*, 8(4), June, pp. 283-94.

Lynch, C. (2000). Authenticity and integrity in the digital environment: an exploratory analysis of the central role of trust. *Authenticity in a Digital Environment*. Washington: Council on Library and Information Resources, pp. 32-50. http://www.clir.org/pubs/reports/pub92/pub92.pdf. (6 May 2004).

Mackie, R. (2005). *The New Public Management of Scotland: Local Government and the National Health Service*. Edinburgh: W. Green & Son Ltd.

MacNeil, H. (1996). *Trusting Records: Legal, Historical and Diplomatic Perspectives*. Dordrecht: Kluwer Academic Publishers.

Malhotra, Y. (2004). Why knowledge management systems fail? Enablers and constraints of knowledge human enterprises. *American Society for Information Science and Technology Monograph Series*, pp. 87-112.

Marciano, R.J. and Moore, R.W. (2005). Technologies for preservation. *Managing Electronic Records by Julie McLeod and Catherine Hare (eds.).* London: Facet Publishing, pp. 81-100.

Marshall, G. and Moodie, G.C. (1959). *Some Problems of the Constitutions*. London: Hutchinson, cited in Mulgan (2000).

McCoy, D.R. (1978). *The National Archives: America's Ministry of Documents 1934 – 1968*. Chapel Hill: The University of North Carolina Press.

McDonald, J. (2002). Understanding records means understanding business process … *Records Management Journal*. 12(12), pp. 75-78.

McDonald, J. (1999). Record keeping systems: lesson learned from the experience of the Canadian Federal Government. *Australian Society of Archivist 1999 Conference*. Also available at http://www.archivists.org.au/events/conf99/mcdonald.html (17 June 2005).

McKemmish, S. (2005). Traces: document, record, archive, archives. *Archives: Recordkeeping in Society by Sue McKemmish et al. (eds.)*. New South Wales: Charles Sturt University, pp. 1-20.

McKemmish, S., Reed, B., and Piggott, M. (2005). The archives. *Archives: Recordkeeping in Society by Sue McKemmish, Michael Piggott, Barbara Reed and Frank Upward (eds.)*. New South Wales: Centre for Information Studies, Charles Sturt University, pp. 159-95.

McKemmish, S. (2001). Placing records continuum theory and practice. *Archival Science*, 1(4), pp. 333-59.

McKemmish, S. (1999). T*he Smoking Gun: Recordkeeping and Accountability*. http://www.sims.monash.edu.au/research/rcrg/publications/recordscontinuum/smoking.html (3 July 2004).

McKemmish, S. and Acland, G. (1999). Archivists at risk: accountability and the role of the professional society. *Australian Society Archivists 1999 Conference*. http://www.archivists.org.au/events/conf99/mckemmish_acland.html (17 June 2005).

McKemmish, S., Cunningham, A., and Parer, D. (1998). Metadata mania. *Place, Interface and Cyberspace: Archives at the Edge,* Proceedings of the 1998 Conference of the Australian Society of Archivists, Fremantle 6-8 August 1998.

Mehr, R.I. and Hedges, B.A., (1974). *Risk Management: Concepts and Applications*. Illinois: Richard D. Irwin Inc.

Meijer, A.J. (2003). Trust this document! ICTs, authentic records and accountability. *Archival Science*, 3(3), pp. 275-90.

Meijer, A. (2001). Accountability in an information age: opportunities and risks for records management. *Archival Science*, 1(4), pp. 361–72.

Meulbroek, L. (2002). The promise and challenge of integrated risk management. *Risk Management and Insurance Review*, 5(1), pp. 55-66.

Mill, J.S. (1962). *Representative Government*. London: Everyman's Library, cited in Day and Klien (1987).

Monks, R.A.G. and Minow, N. (2001). *Corporate Governance*. 2nd ed. Oxford: Blackwell Publishes Ltd.

Moss. M. (2009). *Where Have All the Files Gone, Lost in Action Points Every One?* Unpublished manuscript. Glasgow: University of Glasgow.

Moss, M. (2006a). The function of the archive. *Record Keeping in a Hybrid Environment: Managing the Creation, Use, Preservation and Disposal of Unpublished Information Objects in Context by A. Tough and M. Moss (eds.).* Oxford: Chandos Publishing, pp. 227-59.

Moss, M. (2006b). The archives of business and the business of archives. *Business Archives*, 91, May, pp. 60-73.

Moss, M. (2005). The Hutton Inquiry, the President of Nigeria and what the Butler hoped to see. *English Historical Review*, Vol. CXX (487), June, pp 576-92.

Moss, M. and Tough, A. (2003). Metadata, controlled vocabulary and directories: electronic document management and standards for records management. *Records Management Journal*, 13(1), pp. 24-31.

Moss, M. (2000). *Standard Life: The Building of Europe's Largest Mutual Life Company, 1825 – 2000*. Edinburgh: The Standard Life Assurance Company.

Moss, M. (1997). Archives, the historians and the future. *Companion to Historiography* by Michael Bentley (ed.), pp. 960-73. London: Routledge.

Mulgan, R. (2000). 'Accountability': an ever-expanding concept? *Public Administration*, 78(3), pp. 555-73.

Murdock, A. (2006a). Interactions, paradoxes and sub-cultures – managing and archiving records in the digital era. *Managing and Archiving Records in the Digital Era: Changing Professional Orientation*. Baden: Hier + Jetzt, pp. 59–67.

Murdock, A. (2006b). *A Day in a Life – European Investment Bank, Luxembourg*. http://www.archives.org.uk/download.asp?id=1011 (22 June 2007).

National Archives and Records Administration. (January 2005). *NARA Guidance on Managing Web Records*. http://www.archives.gov/records_management/pdf/managing_web_records_index.pdf (5 April 2005).

National Audit Office (The). (2000). *Co-operation Between Internal and External Auditors: a Good Practice Guide*. http://www.nao.org.uk/guidance/InternalAudit.pdf (17 November 2005).

NHS Greater Glasgow and Clyde. (2006a). A*nnual Review 2005*. http://library.nhsgg.org.uk/mediaAssets/library/nhsggc_annual_review_2006_self_assessment_report.pdf (20 September 2006).

NHS Greater Glasgow and Clyde. (2006b). *NHS Argyll and Clyde Integration*. *Board Paper No. 2006/03*. http://library.nhsgg.org.uk/mediaAssets/Board%20Papers/06-03.pdf (4 January 2007).

NHS Greater Glasgow and Clyde. (2006c). *Statement on Internal Control 2005/2006. Board Paper No. 06/26*. http://library.nhsgg.org.uk/mediaAssets/Board%20Papers/06-26.pdf (2 December 2006).

NHS Quality Improvement Scotland. (2005a). *Clinical Governance and Risk Management: Achieving Safe, Effective, Patient-focused Care and Services – National Standards – October 2005*. http://www.nhshealthquality.org/nhsqis/files/CGRM_CSF_Oct05.pdf (5 January 2007).

NHS Quality Improvement Scotland. (2005b). *Clinical Governance and Risk Management Arrangements in NHS Scotland: Local Interim Report – June 2005*. http://www.nhshealthquality.org/nhsqis/files/CGRM_LRP_GRGL05.pdf (4 January 2007).

Norton, M. C. (1956). The archivist and records management. *Norton on Archives: the Writings of Margaret Cross Norton on Archival and Records Management by Thornton W. Mitchell (ed.)*. (2003). Chicago: The Society of American Archivists, pp. 247-65.

O'Neill, O. (2002a). *Trust and Transparency*. http://www.bbc.co.uk/radio4/reith2002/lecture4.shtml (6 October 2004).

O'Neill, O. (2002b). *The BBC Reith Lecture: a Question of Trust*. Cambridge: Cambridge University Press.

O'Neill, O. (2002c). *Onora O'Neill on Trust: Spreading Suspicion*. http://www.bbc.co.uk/radio4/reith2002/lecture1.shtml (12 Oct 2004).

Organisation for Economic Co-operation and Development. (2004). *Principles of Corporate Governance*. Paris: OECD.

Organisation for Economic Co-operation and Development. (2002). *Public Sector Transparency and Accountability: Making it Happen*. Paris: OECD.

Organisation for Economic Co-operation and Development. (2001a). *Governance of the 21st Century.* Paris: OECD.

Organisation for Economic Co-operation and Development. (2001b). *E-Government: Analysis Framework and Methodology.* Paris: OECD.

Organisation for Economic Co-operation and Development. (2000). *Trust in Government: Ethics Measures in OECD Countries*. Paris: OECD.

Organisation for Economic Co-operation and Development. (1999). *Principles of Corporate Governance*. Paris: OECD.

Oxford English Dictionary. 2nd ed. (1989) Oxford: Clarendon Press.

Pierre, J. and Peters, B.G. (2000). *Governance, Politics and the State*. London: MacMillan Press Limited.

Posner, E. (1941). The role of records in German Administration. *The Role of Records in Administration: Staff Information Circular No. 11.* Washington: National Archives.

Posner, E. (1972). *Archives in the Ancient World*. Massachusetts: Cambridge University Press.

Power, M. (1997). *The Audit Society: Rituals of Verification*. Oxford: Oxford University Press.

Power, M. (1994). *The Audit Explosion*. London: Demos.

PREMIS Working Group. (2005). *Data Dictionary for Preservation Metadata*. California: OCLC and RLG. http://www.oclc.org/research/projects/pmwg/premis-final.pdf . (8 March 2006).

PricewaterhouseCoopers. (2006). *External Audit Annual Report to Board Members 2005/06 Audit.* http://library.nhsgg.org.uk/mediaAssets/Board%20Papers/06-27.pdf (19 September 2006).

PricewaterhouseCoopers. (2005). *External Audit Annual Report to Board Members 2004/05 Audit*. http://library.nhsgg.org.uk/mediaAssets/Board%20Papers/nhsgg_board_paper_05-47.pdf (14 February 2006).

Public Record Office. (2001). *Sustainable Electronic Records: Strategies for the Maintenance and Preservation of Electronic Records and Documents in the Transition to 2004*. http://www.nationalarchives.gov.uk/documents/preservation_toolkit.pdf (22 June 2007).

Quirk, B. (1997). Accountable to everyone: postmodern pressures on public managers. *Public Administration*, 75, Autumn, pp. 569-586.

Radner, R. (1992). Hierarchy: the economic of managing. *Journal of Economics Literature*, 30, September, pp. 1382-415.

Read-Smith, J., Ginn, M.L., and Kallaus, N.F. (2002). *Records Management*. 7th ed. Cincinnati: South-Western Educational Publishing.

Reed, B. (2000). The tradition and position. *ERPANET Workshop: Managing Records and Archives in the Digital Era*, Bern, Switzerland, 25-26 October 2004.

Reed, B. (1997). Metadata: core record or core business? *Archives and Manuscript*, 25(2), pp. 218-41. http://www.sims.monash.edu.au/research/rcrg/publications/recordscontinuum/brep1.htm (24 May 2004).

Reynolds, P. (2004). *Analysis: Devil in the Detail*. http://news.bbc.co.uk/1/hi/uk_politics/3894403.stm (22 June 2007).

Robek, M. F., Brown, G.F. and Stephens, D.O. (1995). *Information and Records Management.* New York: McGraw Hill.

Roberts, D. (1994). Defining electronic records, documents and data. *Archives and Manuscripts* 22, May, pp 14-26. http://www.records.nsw.gov.au/publicsector/erk/dtf/define-1.htm (26 March 2004).

Robinson, P. (2005). Fighting financial crime together. *Financial Crime Conference,* London, 15 November 2005.

Ross, S. (2006). Approaching digital preservation holistically. *Record Keeping in a Hybrid Environment: Managing the Creation, Use, Preservation and Disposal of Unpublished Information Objects in Context by A. Tough and M. Moss (eds.).* Oxford: Chandos Publishing, pp. 115–53.

Ross, S. and McHugh, A. (2005). Audit and certification: creating a mandate for the digital curation centre. *Diginews*, 9(5). http://www.rlg.org/en/page.php?Page_ID=20793#article1 (8 March 2006).

Ross, S. (2000). *Changing Trains at Wigan: Digital Preservation and the Future of Scholarship*. London: National Preservation Office.

Rothenberg, J. (2000). Preserving authentic digital information. *Authenticity in a Digital Environment*. Washington: Council on Library and Information Resources, pp. 51-62. http://www.clir.org/pubs/reports/pub92/pub92.pdf. (5 May 2004).

Rothenberg, J. (1999). *Ensuring the Longevity of Digital Information*. http://www.clir.org/pubs/archives/ensuring.pdf (22 March 2006).

Sampson, K.L. (2002). *Value Added Records Management: Protecting Corporate Assets, Reducing Business Risks*. 2nd ed. Connecticut: Quorum Books.

Schellenberg, T.R. (1956). *Modern Archives: Principles and Techniques*. Melbourne: F.W. Cheshire.

Schultz, E.E. (2004). Sarbanes-Oxley – a huge boon to information security in the US. *Computers & Security*, 23(5), pp. 353-4.

Schultz, E.E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*. 21(6), pp. 526-31.

Scottish Information Commissioner. (2006). *Annual Report 2005*. http://www.itspublicknowledge.info/Documents/annualreport2005.pdf (12 January 2006).

Segen, J. (2006). *Concise Dictionary of Modern Medicine.* New York: McGraw-Hill.

Sharon, B. (2006a). *Risk Management: What Should Be, What Is and What Could Be.* http://www.continuitycentral.com/feature0231.htm (26 December 2007).

Sharon, B. (2006b). *Risk Management: Worrying About the Things That Need To Go Right.* http://www.globalriskguard.com/html/articles.html (26 April 2008).

Sharon, B. (2005a). *Operational Risk Management: The Difference Between Risk Management and Compliance*. http://www.continuitycentral.com/feature0243.htm (12 April 2008).

Sharon, B. (2005b). *Risk Management Is Not Compliance*. http://www.itbusinessedge.com/item/?ci=5239 (26 April 2008).

Shepherd, E. and Yeo, G. (2003). *Managing Records: a Handbook of Principles and Practice*. London: Facet Publishing.

Shipman, A. (2002). Managing e-mails and e-commerce records. *Records Management Journa*l. 12(3), pp. 98–102.

Shipman Inquiry (The). (2005). *Shipman: The Final Report*. http://www.the-shipman-inquiry.org.uk/finalreport.asp (3 January 2006).

Shipman Inquiry (The). (2004). *Fifth Report: Safeguarding Patients: Lessons from the Past – Proposals for the Future*. http://www.the-shipman-inquiry.org.uk/fifthreport.asp (17 July 2006).

Shipman Inquiry (The). (2002). *First Report: Volume 1: Death Disguised.* http://www.the-shipman-inquiry.org.uk/firstreport.asp (15 April 2004).

Shore, C. and Wright, S. (2000). Coercive accountability: the rise of audit culture in higher education. *Audit Cultures: Anthropological Studies in Accountability, Ethics and the Academy by Marilyn Strathern (ed.).* London: Routledge, pp. 57-105.

Simon, R. (1999). How risky is your organisation? *Harvard Business Review*, 77(3), May/Jun, pp. 85-94.

Standard Life Assurance Company (The). (2006). *Annual Financial Statements for the Year Ended 31 December 2005*.

Stephens, D.O. (2005). The Sarbanes-Oxley Act: records management implications. *Records Management Journa*l, 15(2), pp. 98-103.

Stephens, D.O. (2002). Lies, corruption and document destruction. *The Information Management Journal*, 35(5), September/October, p 23-30.

Sternberg, E. (1998). *Corporate Governance: Accountability in the Marketplace*. London: The Institute of Economic Affairs.

Thibodeau, K. (2002). *Overview of the Technological Approaches to Digital Preservation and Challenges in Coming Years*. http://www.clir.org/PUBS/reports/pub107/thibodeau.html (29 March 2005).

Thibodeau, K. (2001). Building the archives of the future: Advances in preserving electronic records at the National Archives and Records Administration. *D-Lib Magazine*, 7(2). http://www.dlib.org/dlib/february01/thibodeau/02thibodeau.html (22 June 2007).

Thompson, D. (2003). Risk management: a brief history: risk management has gradually evolved from a narrow insurance-based discipline to covering anything from traditional financial activities to the risk of a building burning down. *Journal of Banking and Financial Services*, 117(3), June-July, pp. 30-2.

Thurston, A. and Cain, P. (1998). *Record Management as a Public Sector Accountability Function*. http://legacy.transparency.org/working_papers/thematic/irmt.html (3 November 2004).

Tombs, K. (2004). Knowledge management is dead: long live records management. *Records Management Journal,* 14(2), pp. 90-3.

Tough, A. (2004). The post-custodial/pro-custodial argument from a records management perspective. *Journal of the Society of Archivists*, 25(1), pp. 19-26.

Treasury Board of Canada Secretariat. (2001). *Integrated Risk Management*. http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/riskmanagement/rmf-cgr01-1_e.asp (15 September 2005).

Turban, E., McLean, E. and Wetherbe, J. (1996). *Information Technology for Management: Improving Quality and Productivity*. New York: Wiley.

Uglow, S. (1997). *Evidence: Text and Materials*. London: Sweet & Maxwell.

United Nations Development Programme. (1997). *Governance for the Sustainable Human Development: a UNDP Policy Document*. http://mirror.undp.org/magnet/policy (8 September 2009)

United Nations Economic and Social Commission for Asia and the Pacific. (N.d). *What is Governance?* http://www.unescap.org/pdd/prs/ProjectActivities/Ongoing/gg/governance.asp (15 November 2005).

United States Department of Defence. (2002). *Design Criteria Standard for Electronic Records Management Software Applications - DoD 5015.2-STD*. http://jitc.fhu.disa.mil/recmgt/p50152stdapr07.pdf (20 June 2007).

United States Federal Government. (2002). *Sarbanes Oxley Act of 2002*. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.txt.pdf (6 July 2004).

Upward, F. (2000a). Modelling the continuum as paradigm shift in recordkeeping and archiving processes, and beyond – a personal reflection. *Records Management Journal*, 10(3), pp. 115-39.

Upward, F. (2000b). *Record and Recordkeeping*. http://www.records.nsw.gov.au/publicsector/erk/dtf/append-2.htm. (18 January 2005).

Upward, F. (1994). *In Search of Continuum: Ian Maclean's 'Australian Experience' Essays on Recordkeeping*. http://www.sims.monash.edu.au/research/rcrg/publications/fuptrc.html (26 July 2005).

Victoria Government. (1997). *Metropolitan Ambulance Service: Contractual and Outsourcing Practices. Special Report No. 49*. http://www.audit.vic.gov.au/old/sr49/sr49.pdf (18 April 2006).

Wagner, S. and Dittmar, L. (2006). The unexpected benefits of Sarbanes-Oxley. *Harvard Business Review*, 84(4), pp. 133-40.

Walden, I. (1993). Electronic documentation and law. *Electronic Information Resources and Historians: European Perspectives by Seamus Ross and Edward Higgs (ed)*. Proceedings of a workshop held at The British Academy on 25 & 26 June 1993.

Wallace, D.A. (1993). Metadata and the archival management of electronic records: a review. *Archivaria*, 36, pp. 87-110.

Wallace, D.A. (2000). Record keeping metadata. *Proceedings of the Archiving Metadata Forum, The Netherlands, 5-8 June 2000*. http://www.archiefschool.nl/docs/workproc.pdf (13 June 2005).

Walton, B. (2003). Authenticity and accessibility, objects and technologies: digital preservation basics. *Symposium 2003: Preservation of Electronic Records: New Knowledge and Decision-making*, Ottawa, Canada, 15-18 September 2003.

Watzke, G. (2005). *The Arthur Andersen Reversal: Sound Records Management Still Required*. http://www.ironmountain.com/records/resources/authurandersen.asp (21 June 2007).

White, F. and Hollingsworth, K. (1999). *Audit, Accountability and Government*. Oxford: Clarendon Press.

Willis, A. (2005). Corporate governance and management of information and records. *Records Management Journal*. 15 (2), pp. 86-97.

Wolkoff, N. (2006). America's regulations are scaring the SOX of small caps. *Financial Times*, 1 August. Available at http://www.ft.com/cms/s/26a51a40-20fa-11db-8b3e-0000779e2340.html (1 August 2006).

Working Meeting on Recordkeeping Metadata. (2000). *Recordkeeping Metadata: Definitions and Relationships to Other Types of Metadata*. Available at http://www.archiefschool.nl/docs/hedshowt.pdf (13 June 2000).

Wyatt, M. (2005). Nonprofit Governance: Why it Matters? Available at http://www.transparency.cz/pdf/wyatt.pdf (9 September 2009).

Zander, M. (2003). *The Police and Criminal Evidence Act 1984. 4th edition*. London: Sweet and Maxwell Limited.

(Number of words: 99, 087)

APPENDIX

- **Folder Structure for a Lending Operation > Operation N° + OPERATION NAME**
  - **1 - Authorisation**
    - **Pre-appraisal**
      - FINREQ - Financing Request
      - PIN - New Project Preappraisal Information (old RQ) SERAPIS
      - ATTRIBPJ - Fiche d'Attribution
      - PJ1REACT - PJ First Reaction
      - PROMQUEST - Promoter Questionnaire
      - FSAOPINPJ - PJ Opinion for Appraisal
      - FSAOPINCRD - CRD Opinion (FSA)
      - FSAOPINJU - JU Opinion (FSA)
      - FSA - Fact Sheet A (SERAPIS)
      - OPMISSREP - Ops Mission Report
      - ADVNOTECA - Advance Note to Board Members
      - AGREECONFI - Agreement on Confidentiality (Declaration of Obligation)
    - **Appraisal**
      - ACPOPINREQ - Letter to ACP Secretariat for opinion on project
      - PJFICHE - Fiche de Projet PJ (legacy)
      - TSOKCRD - RM OK for Term sheet
      - PJMISSREP - PJ Mission Report
      - TERMSHEET - Term Sheet
      - OPFINALN - OP Final Note to CD after FSB (projets structurés)
      - FNOPINCRD - Opinion from RM on Final Note
      - CAOKINFO - Letter informing borrower of CA approval of project
      - CDOKINFO - Letter informing borrower of CD approval of project
      - FEESMISSION - Mission fee sent to client
      - FEESAPPREQ - Request for Appraisal Fees
      - FEESAPPREC - Receipt of Appraisal Fees
      - FEESDDREQ - Request for Due Diligence Fees
      - FEESDDREC - Receipt of Due Diligence Fees
      - FEESMISSION - Mission fee sent to client
      - COSTRECOV - Cost Recovery Letter PPP - sent to client
      - INFACOREPe / INFACOREPf / INFACOREPd - Investment Facility Committee Report (compound document including translations EN, FR, DE)
      - ART14REPe / ART14REPf / ART14REPd - Article 9/14 Report (compound document including translations EN , FR, DE)
      - ART28REPe / ART28REPf / ART28REPd - Article 28 Report (compound document including translations. EN, FR, DE)
      - ART18REP - Article 18 Report to the Board of Governors
      - PJFINALN - PJ Final Note/Final Report PPP - Addendum to Appraisal Rep.
      - PRESSREL - Press Release
      - Shortcut - CD + CA Minutes
      - **External opinions**
        - **Communication with European Commission**
          - COMSUMNOTE - Summary Note for EC
          - COMOPINREQ - EC Opinion Request + Summary Note for EC
          - COMREC - Acknowledgement of Receipt of EC Opinion Request
          - COMOPINGIS - Opinion of the EC Inter-Service Group
          - COMOPIN - EC Opinion
          - COMINFOREQ - EC Request for Additional Information
          - COMINFO - Additional Information for EC / to EC
          - COMOPINREQ2 - Request for Confirmation of favourable EC opinion
          - COMOPIN2 - Confirmation of favourable EC opinion
          - COMBUDGREQ - Request for Budget Authorisation from EC
          - COMBUDG - Budget Authorisation from EC
        - **Communication with State**
          - EUOPINREQ - Member State Opinion Request
          - EUOPIN - Member State Opinion
          - EUOPINREQ2 - Request for Confirmation of Favourable Member State Opinion
          - EUOPIN2 - Confirmation of Favourable Member State Opinion
          - NEUOPINREQ - Request for "No objection/Consent" (sent by Ops to Non Member State concerned)
          - NEUOPIN - No objection/Consent (Non Member Sates)

- **Web publication**
  - WEBLETTER - Letter for Web Publication
  - WEBFORM - Form for Web Publication
  - PUBANSWER - Agreement / justified refusal for publication from promoter
- **Promoter documents**
  - PROMQUEST - Promoter Questionnaire
  - PROMDOCS - Promoter document(s)
- **Fact Sheet B (FSB)**
  - FSB - Fact Sheet B (SERAPIS)
  - FSBREPPJ - PJ Appraisal Report
  - FSBFLYPJ - Fly sheet PJ
  - PJTECHDES - PJ Technical Description annex
  - PJANNEXA2 - Annex A2 of Appraisal Report - Information to be sent to Bank
  - PJMAP - PJ Map
  - PROCURSTAT - Procurement Statistics outside EU
  - PJENVIRONS - PJ Environmental Summary (part of PJ Appraisal report)
  - PJCOHESION - PJ Excel Economic and Social Cohesion Indicators
  - REPPJANNEX - Annex to PJ Appraisal Report
  - VASHEET - Value Added Sheet for Global, Investment, Framework & MIDCAP loans (Annex to Board Report)
  - FSBOPINJU - JU opinion on Fact Sheet B
  - FSBOPINCRD - CRD Opinion on Fact Sheet B
  - FSBOPINFI - FI Opinion on Fact Sheet B
  - FSBFINREP - OP Financial Report = Financial note to CD
  - FSBCAREP - Legacy only : CA Report for a Lending Operation
  - FSBCAREP - Draft Board Report at FSB stage
- **Board report**
  - OPCAREPe / OPCAREPf / OPCAREPd - Board Report (translations EN, FR, DE)
  - VASHEET - Value Added Sheet for Global, Investment, Framework & MIDCAP loans (Annex to Board Report)
- **Correspondence**
- VALEXTREQ - Request for Extension of Validity (Caduc annex) (Signed OP + CRD)

2 - Contract - FI number

- BIBLE - Bible of Legal documents
- **Negociation and Financial close**
  - CONTREQJU - Request to JU for Contract Preparation / Guarantee Preparation
  - CONTOPINFI - FI Comments on Draft Contract
  - CONTREACT - Reactions to draft Contract
  - CONTOKCRD - CRD OK on Contract, Guarantee, amendments, mail including CRD conditions for OK
  - NEGOMEMO - Memorandum of Negotiations
  - COMDELINFO - Loan Approval Info letter to Commission Delegation in Non EU
  - NOTECONJ - Note Conjointe / Contract Agreement Note (SERAPIS)
  - EXTADVICE - External legal opinion / External
  - LEGALSPSH - Legal spread sheet
  - FINANCONT - Finance Contract (including all draft versions & final version)
  - FINONOTIF - Notification of FI Number from FI
  - CONTSIDLET - Lettre d´Encadrement / Contract Side Letter (for FINANCONT & CONTGUA)
  - CONTGUA - Guarantee Agreement
  - SYNDRES - Syndicate Guarantee Reservation details concerning syndicate members
  - PLEDGEOP - Pledge Agreement for a Loan
  - TRIPARTIOP - Tripartite Agreement for a Loan
  - PLEDGEANNEX / PLEDGECERT / PLEDGEVALU - Pledge related documents (Annex updates, certificates, valuations)
  - SECURITY - Security agreement
  - OPSUPPORTJU - Project support agreements

- JUSIGNOTIF - Notification of Signature
- CLOSEMEMO - JU Closing Memorandum
- CLOSENOTE - CRD Closing Note
- FEESUPFRONT - Upfront fee (managemet fee) sent to client .Can be sent alternatively at Disbursement
- CHECKPROC - Procedural Checklist
- OPSIDLET - OPs side letter after Contract signature
- TRANSUMM - OPs Transaction Summary for PPP Operations
- HANDOVNOTE - Handover Note for Project Finance

Contract amendments

- MODIFREQOP - Request from OP to JU for a Contractual Amendment (e.g. for Extension of the contractual limit for disbursemer
- MODIFCONT - Contract Amendment (with corresponding letter of notification of the contract amendment)
- MODIFOPINFI - FI Comments on Contract Modification (also other directorates can comment)
- MODIFCONT - Waiver Letters
- MODIFCONT - Discharge Letters

Disbursement

- ALMMESSAGE (RE LD1) - ALM message
- BORRACCEPT - Acceptance Letter from Borrower
- DISBREQ - Disbursement Request (client)
- DISBCHECKS - Control of Disbursement conditions precedent
- BDV - Disbursment Autorisation/Autorisation de Versement/Bon de Versement/Disbursment Ticket/BDV
- DISBNOTICE (= RE LD2) - Notification of Disbursement to Borrower / Disbursement conditions notification
- DISBEXEC (= RE LD4) - Disbursement Execution Notification (RE)
- DISBCOREQ (= RE LD5) - Correspondent request
- DISBREQREV - Borrower's Request to Revoke Disbursement Request
- EFTADISBREQ - EFTA Disbursement Request
- PAYNONBORR - Borrower 's Written Approval for Payments to non-Borrower Account
- STATEEXPEN - Summary Statement of Expenditures
- DISBREQEXC2 - Exceptional Disbursement Request Notification 2 (sent to CA)
- DISBREQEXC1 - Note to FI-PRO re Borrower's Exceptional Disbursement Request 1
- FICHETIR (= RE LD6) - Fiche de Tirage = Drawdown drawing slip RE
- FICHEVER (= RE LD3) - Fiche de Versement = Disbursement slip RE
- NOTIFTRANS - Tlx, Fax Swift Advice that Funds have been Transferred
- AMORTABLED - Amortization Table for Specific Disbursement
- APPELFONDS - Appel de Fonds to CE
- RATECALC1 - Rate Calculation/Rate Grid & associated notes (done for Disbursement and for Financial Follow up)

Funding call

- FCALLNOTIF1 (= RE LD7) - Funding call notification
- FCALLNOTIF2 (= RE LD7) - Funding call cancellation notification
- FCALLOK (= RE LD8) - Funding call receipt confirmation
- APPELFONDS - Appel de Fonds to CE

Allocations for global loans

- ALLREQ - Allocation Request for Global loans
- ALLFICHE - Fiche d'Affectation pour prêts globaux
- ALLOK - Letter from EIB to Borrower for Agreed Allocations (Affectation prêts globaux) - SERAPIS
- ALLEXTREQ - Request for Extension of Allocation & Disbursement Periods
- ALLEXTOK - Note to Borrower on Extension of Allocation & Disbursement Periods
- ALLREP - Allocation report for statistics and monitoring
- REALLOK - Lettre to Borrower on Reallocation
- ENDALLREP - Final Allocation Report sent to the CA (produced by loan officers)
- ALLLIQ - Notification of receivership (Borrower to EIB)
- ALLLIQREQ - Request for discharge following notification of receivership (Borrower to EIB)
- ALLDISTEMP - ATemporary discharge agreed (EIB to Borrower)
- ALLDISDEF - Definitive discharge agreed (EIB to Borrower)
- ALLANNUL - Cancellation of Allocation (total or partial)
- ALLREJECT - Rejection of Allocation Request after submission
- ALLAMEND - Allocation Amendment

Correspondence

- 3 - Monitoring
  - MONITPROG - Monitoring Program
  - FINREVIEW - Financial & Credit Review
  - CTRLNOTEPJ - Note de Contrôle (PJ)
  - REMINDLP1 - Lettres de rappel PJ (au promoteur)
  - REMINDLP2 - Lettres de rappel PJ (au promoteur)
  - PROGREP - Project Progress Report from client
  - PPR - Project Progress Report from OP
  - PJPPR - Project Progress Report from PJ (serapis Wizard)
  - RFT - Rapport Fin de Travaux / Project Completion Report (PCR)
  - PCR - Project Completion Report (Serapis)
  - RFTSIMPPJ - Raport Fin de travaux simplifié PJ / Simplified project Completion Report
  - RFTCOMPPJ - Raport Fin de travaux complet PJ / Full project Completion Report
  - SCORECARD - Scorecards
  - IMPLCERTIF - Certified Statement on Project's Physical Implementation
  - NOBJTENDER - No Objection to Tender from OP/PJ
  - TENDERINV - Invitation to Tender
  - TENDERAWARD - Tender Award Notice
  - TENDERTTLS - Translated Invitation to Tender (Titles only)
  - PUBTED - Letter to EC Publications Office (e-mail)
  - PROCURCONT - PJ Procurement Contracts for Non-Europe
  - Correspondence
- 4 - Financial follow-up
  - Rate events
    - RATECALCREQ (= RE LD 34) - Request for an interest quote
    - RATECALC2 - Rate Calculation/Rate Grid & associated notes (done for Disbursement and for Financial Follow up)
    - RATEGRID (= RE LD 35) - Interest rate grids (fixed - internal floater) (RE)
    - RATESWAP (= RE LD 36) - Swap rate list (RE)
    - RATECOMMOP - Communication of Interest Rate to OP
    - RATECOMMCL - Communication of Interest Rate to Client
    - RATEPROPOS (= RE LD 22) - Proposition de Taux Revisable = Interest rate revision notification
    - IRATERENEW (= RE LD 18) - Internal floater rate renewal notification
    - ERATERENEW (= RE LD20) - External floater rate renewal notification
    - IRATEROLL (= RE LD19) - Internal floater rate Rollover report
    - RATENOTIF (= RE LD21) - Rate notification after a remuneration mode conversion (RMC)
    - RATECONVC - Conversion Devise Seule (C= Currency)
    - RATECONVR - Conversion de nature de taux seule (R= Rate)
    - RATECONVCR - Conversion de Devise avec changement de Ndt (CR = Currency + Rate)
  - Debt service = Reimbursements
    - PAYADVICE (= RE LD29) - Payment Advice FORCE
    - PENALRET - Penalite de Retard
    - STATEACC (= RE LD30) - Statement of account
    - STATECOMM (= RE LD33) - Statement of commission
    - PAYALLOC - Payment allocation report
    - DEBTSCHED (= RE LD32) - Basic Debt schedule
    - REMINDTLX1 (= RE LD23) - Payment reminder notification (before due date)= First payment reminder= First TLX de rap
    - REMINDTLX2 (= RE LD24) - Carte Payment reminder=Second payment reminder= 2d TLX de rappel
    - FOREXMEMO (= RE LD31) - Transaction memorandum for foreign exchange position
    - Early reimbursement
      - VARREMTB - Remuneration tables for variable remuneration
      - TRANSMEMO - Transaction memorandum
      - SWIFT - SWIFT
      - PREPAYREQ - Prepayment Request (from the Borrower) (provisional / fixed / definitive)
      - PREPAYNOTIF (= RE LD 17) - Prepayment notification and summary table by request
      - PREPAYFORM - Standard Prepayment Sheet / Prepayment Form
      - PREPAYCALC - Prepayment calculation for Borrower (internal doc)
      - PREPAYMAIL - Notes linked to loan covered by pledge+ e-mails related to prepayments
      - PREPAYFAX - Correspondence related to prepayments (cover fax)
      - PREPAYTBCRD - Table of prepayments of CRD
      - PREPAYANAL - Cash flow analysis
      - PREPAYTBFI - Prepayment summary table FI
      - AMORTABLER - New amortisation table
      - PREPAYADV - New payment advice

- **Late payments**
  - LPALERTLTMS (Member State) / LPALERTLTCE (Commission) - Lettres de préavis envoyées aux Etats Membres ou à la Commission
  - LPPREVFXMS (Member State) / LPPREVFXCE (Commission) - Fax de préavis envoyés aux Etats Membres ou à la Commission
  - LPCALLLTMS (Member State) / LPCALLLTCE (Commission) - Lettres d'appel à la Caution envoyés aux Etats Membres ou à la Commission
  - LPSDAYFXMS (Member State) / LPSDAYFXCE (Commission) - Fax envoyés le même jour que l'appel à la garantie aux Etats Membres ou à la Comn
  - LPRETROFIMS (Member State) / LPRETROFICE (Commission) - Note à FI demandant la rétrocession des fonds
  - LPRETROLTMS (Member State) / LPRETROLTCE (Commission) - Lettres de rétrocession annonçant le remboursement des sommes recouvrées
- **Reversement**
  - REREDEBIT - By debit our account (ordre à la trésorerie BOT)
  - RERESWIFT - SWIFT de la BEI pour le reversement de l'argent
  - SWIFT - SWIFT de l'emprunteur pour le reversement de l'argent
- **Credit cancellation**
  - ANNULCREADV / POSTPOCREADV - Letter to Borrower/Guarantor advising credit cancellation/ postponement
  - ANNULCRECOM / POSTPOCRECOM - Letter to EC on credit Cancellation / Postponement
  - ANNULNOTIF / POSTPONOTIF (= RE LD 17) - Credit cancellation/ postponement notification to borrower
  - ANNULCREFI / POSTPOCREFI - Note to FI on credit cancellation / Postponement
- **Subsidy**
  - SUBSINOTIF1 (= RE LD10) - Contract subsidy estimation notification
  - SUBSINOTIF2 (= RE LD11) - Contract subsidy estimation rectification request
  - SUBSICALL (= RE LD12) - Interest Subsidy call document
  - SUBSITABLE (= RE LD13) - Interest subsidy summary table by contract
  - SUBSIREFUND (=RE LD16) - Interest subsidy refund document
- **Correspondence**

5 - Supporting documents

- SUPPORTDOC - Ad-hoc Supporting Documents
- PPM - Private Placement Memorandum
- **Technical Assistance**
  - *FEMIP only*

6 - Images, plans and maps