FEASIBILITY STUDY ON INCORPORATING IEC/ISO27001 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) STANDARD IN IT SERVICES ENVIRONMENT

HAU LIAN HONG

A project report submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Advance Informatics School (AIS)
Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

June 2013

ACKNOWLEDGEMENT

I would like to express my gratitude and special appreciation to a wonderful group of people who have been there to support and make this project a success.

Special thanks to my project supervisor Dr. Bharanidharan Shanmugam who have been encouraging and supportive throughout the research study period. He was very supportive and committed on our regular meeting for project progress updates and guidance.

Very important, I shall thank to my family, friends and AIS office's staffs. A millions thanks to all that have been given the support throughout the period. I hope this project would be a success with the support given from all of you.

ABSTRAK

Kajian Kemungkinan menggabungkan IEC/ISO27001 Sistem Pengurusan Keselamatan Maklumat (ISMS) dalam bidang IT Persekitaran Perkhidmatan adalah satu kajian penyelidikan dengan mengambil organisasi sebagai kajian kes untuk menjalankan kajian kemungkinan tentang keselamatan maklumat organisasi yang sedia ada dan mencadangkan ISO27001 ISMS maklumat rangka kerja keselamatan kepada organisasi. Aktiviti-aktiviti yang melibatkan penilaian keselamatan jurang, merangka dokumen mandatori kerana setiap ISO 27001 standard keperluan ISMS. Objektif kajian ini adalah untuk mengenal pasti insiden keselamatan maklumat umum dan ISO27001 amalan ISMS tindakan pembetulan dan pencegahan. Disamping itu, kajian ini memberi tumpuan kepada menganalisis keadaan semasa organisasi dengan menjalankan kajian kemungkinan mengenai kesediaan ISO27001 ISMS yang diamalkan oleh organisasi. Metodologi kajian ini telah diperolehi dengan rangka kerja penyelidikan operasi yang terdiri daripada beberapa fasa projek, ISO27001 fasa pelaksanaan ISMS yang dipetakan kepada serahan. Serahan dan hasil yang diharapkan adalah siri set dokumen yang perlu mematuhi standard ISO27001 ISMS seperti draf awal pengguna dasar ISMS, metodologi penilaian risiko, laporan penilaian risiko, penyata kebolehgunaan (SOA) akan dibangunkan untuk memenuhi keperluan ISO27001 ISMS dan kriteria. Juga, sebahagian daripada aktiviti mandatori seperti taksiran jurang, penilaian risiko keselamatan maklumat akan dicadangkan dan dijalankan dengan laporan yang berkaitan akan disediakan sebagai sebahagian daripada keputusan dan penemuan untuk mencapai objektif kajian penyelidikan ini. Kajian penyelidikan ini tidak meliputi kitaran pelaksanaan keseluruhan ISMS ISO27001. Oleh itu, kerja-kerja masa depan kajian penyelidikan ini boleh diteruskan dari pentas dengan membangunkan dasar dan prosedur yang perlu berdasarkan serahan laporan penilaian risiko dan penyata kebolehgunaan.

ABSTRACT

Feasibility Study on incorporating IEC/ISO27001 Information Security Management System (ISMS) in IT Services Environment is a research study by taking an organization as a case study to carry out a feasibility study on existing maturity level of managing information security and propose an implementation approach to the organization based on ISO27001 ISMS standards. The activities involve the security gap assessment, drafting the mandatory documents as per ISO 27001 ISMS standard requirement. The objective of this study is to identify the common information security incidents and the ISO27001 ISMS practices on corrective and prevention actions. Beside, this research study is focusing on analyzing the current state of an organization by conducting a feasibility study on the readiness of ISO27001 ISMS practiced by the organization. The methodology of this research study was derived with the research operational framework that comprised of several project phases, ISO27001 ISMS implementation phases that mapped to the deliverables. The deliverables and expected results are series of document sets that must comply to the ISO27001 ISMS standard such as initial draft of ISMS policy manual, risk assessment methodology, risk assessment report, statement of applicability (SOA) will be developed to meet the ISO27001 ISMS requirement and criteria. Also, the mandatory activities such as gap assessment, information security risk assessment will be proposed and conducted with the relevant reports to be prepared as part of the results and findings to accomplish the objectives of this research study. The findings of the feasibility study from the gap assessment that has been performed within an organization are not meeting the requirement of ISO27001 ISMS. Hence, this research study proposed the implementation approach based on ISO27001 ISMS standards to implement the ISMS controls to close the gaps and mitigate the risks identified from the gap assessment findings.

TABLE OF CONTENTS

CHAPTER	TITLE		PAGE
	DECLARATION		**i**
	DEDICATION		**ii**
	ACKNOWLEDGEMENT		**iii**
	ABSTRAK		**iv**
	ABSTRACT		**v**
	TABLE OF CONTENTS		**vi**
	LIST OF TABLES		**xi**
	LIST OF FIGURES		**xiii**
	LIST OF APPENDIX		**xiv**
1	**INTRODUCTION**		**1**
	1.1	Overview	1
	1.2	Background of the problem	3
	1.3	Problem Statement	4
	1.4	Project Aim	4
	1.5	Research Questions	5
	1.6	Research Objectives	5
	1.7	Research Scope	5
	1.8	Summary	7

2	**LITERATURE REVIEW**		**8**
	2.1	Introduction	8
	2.2	Overview of Data Security Breaches	9
	2.3	Common Security Threats	10
	2.3.1	Cybercrime Threats	11
	2.3.2	Insider Threats	12
	2.4	Common Security Controls	12
	2.4.1	Organizational Security Awareness	12
	2.4.2	Government Legislation and Compliance	14
	2.4.3	Information Handling	14
	2.4.4	Separation of Duties	15
	2.5	The Consideration of Information Security Blueprint	15
	2.5.1	IEC/ISO 27001 ISMS	15
	2.5.2	Gartner Information Security Governance Model	19
	2.6	ISO27001 ISMS Gap Assessment	20
	2.7	Risk Assessment Framework Recommendation for Information Security Management System (ISMS)	24
	2.7.1	ISO 31000 Risk Management	25
	2.7.2	Health Insurance Portability and Accountability Act (HIPAA)	25
	2.7.3	Control Objectives for Information and Related Technology (COBIT)	26
	2.7.4	Sarbanes-Oxley (SOX)	27
	2.7.5	ISO/IEC 27005 Information Security Risk Management	28
	2.7.6	The Advantages and Disadvantages of Risk Assessment Framework	29
	2.7.7	The Outcomes of Risk Assessment Framework	32

	2.8	Common Problems in ISO27001 ISMS Project Implementation	32
	2.9	Critical Success Factors and Lessons Learned	34
	2.10	Summary Table of Literature Review	35
	2.11	Summary	41
3	**METHODOLOGY**		**42**
	3.1	Introduction	42
	3.2	Research Operational Framework	42
	3.3	ISMS Implementation Methodology	43
	3.3.1	Phase 1: Assessing the Current Gaps of ISMS	44
	3.3.2	Phase 2: Scoping and Security Organization Development	45
	3.3.3	Phase 3: Risk Assessment Methodology & Report	45
	3.4	Research Design	45
	3.5	Research Data Analysis and Findings Presentation	46
	3.6	Summary of Research Techniques	49
	3.7	Summary	51
4	**ISMS IMPLEMENTATION**		**52**
	4.1	Introduction	52
	4.2	ISO27001 ISMS Policy Document Design and Planning	53
	4.2.1	The Objective of Information Security Policy	53
	4.2.2	ISMS Scoping Development	54
	4.2.3	ISMS Committee and Responsibilities	54
	4.2.3.1	ISMS Steering Committee	55

	4.2.3.2	ISMS Advisor	55
	4.2.3.3	ISMS Manager	55
	4.2.3.4	ISMS Committee Member	55
	4.2.4	Documentation Controls	56
	4.2.5	Training and Awareness	57
	4.2.6	ISMS Measurement and Improvement	58
	4.3	Gap Assessment Approach	58
	4.3.1	ISMS Gap Assessment Maturity Level Rating	61
	4.3.2	ISMS Controls Compliant Level for Gap Assessment	62
	4.3.3	The Example of Gap Assessment Report	62
	4.4	Risk Assessment Methodology	63
	4.4.1	Risk Assessment Objectives, Scope and Responsibilities Identification	65
	4.4.2	Assets Identification and Valuation	65
	4.4.2.1	The primary and Supporting Assets	65
	4.4.3	Threats Identification and Valuation	67
	4.4.3.1	Threat Level Details and Action Required	67
	4.4.4	Vulnerabilities Identification and Valuation	68
	4.4.5	Risk Measurement	68
	4.4.6	Risk Treatment Plan	70
	4.4.7	Control Objectives and Selection	71
	4.4.8	Residual Risk	72
	4.5	Summary	72
5	**ISMS DELIVERABLES AND RESULTS**		**73**
	5.1	Introduction	73
	5.2	ISMS Gap Assessment Report	73
	5.2.1	Summary of Gap Assessment Results	74
	5.3	Risk Assessment Report	85

	5.4	Statement of Applicability (SOA)	89
	5.5	Internal Audit Report	90
	5.5.1	Establishment of ISMS	91
	5.5.2	Implementation of ISMS	91
	5.5.3	ISMS Documentation	91
	5.5.4	Compliance to the ISO27001	91
	5.6	Summary	92
6	**CONCLUSION**		**94**
	6.1	Introduction	94
	6.2	Contribution of Research	94
	6.2.1	Formulation of ISMS Organization	95
	6.2.2	ISMS Awareness Program	95
	6.2.3	Development of ISMS Policy	96
	6.2.4	Formulation of Risk Assessment Methodology	96
	6.2.5	Statement of Applicability (SOA) Development	96
	6.2.6	Formulation of Gap Assessment Approach	97
	6.2.7	Conducting ISMS Internal Audit	97
	6.3	Future Work & Conclusion	97
	6.3.1	Phase 4: Policy and Procedures Development	98
	6.3.2	Phase 5: Management Review	98
	6.3.3	Phase 6: Certification Audit	99
	REFERENCES		**100**
	Appendices A - H		**103 - 137**

LIST OF TABLES

TABLE NO	TITLE	PAGE
1.1	Number of Certificates Per Country (Version 215, August 2012)	2
1.2	ISO27001 ISMS Implementation Phase and Project Phases Mapping	6
2.1	Risk Assessment Framework Comparison Table	30
2.2	Summary Table of Literature Review	35
3.1	ISO27001 ISMS Implementation Phase and Deliverables Mapping	43
3.2	User Group Involvement for Guided Checklist	47
3.3	ISO27001 ISMS Implementation Phase and Research Technique Mapping	50
4.1	User Group Involvement for Gap Assessment	59
4.2	Background and Qualification of the Process Owner	60
4.3	Risk Assessment Methodology Process Flow Chart	64
4.4	Business Impact Table	66
4.5	Risk Measurement	69
5.1	Mandatory Documentation Findings	75
5.2	Average Maturity Level of ISMS Controls	78
5.3	ISMS Gap Assessment Report (Red Maturity Level)	80
5.4	ISMS Gap Assessment Report (Amber Maturity Level)	82
5.5	ISMS Gap Assessment Report (Yellow Maturity Level)	83
5.6	ISMS Gap Assessment Report (Green Maturity Level)	84

5.7	User Group Involvement for Risk Assessment	85
5.8	Risk Assessment Approach	86
5.9	Example of Risk Assessment Report	88
5.10	Example of Statement of Applicability (Not Applicable)	90

LIST OF FIGURES

FIGURES NO	TITLE	PAGE
2.1	Organization System (Veiga and Eloff, 2010)	13
2.2	Example Questions by Kruger and Kearney (2006)	14
2.3	ISMS PDCA Model (ISO/IEC 27001:2005)	17
2.4	Typical ISO27001 Implementation Process	18
2.5	The Gartner Information Security Governance Model	19
2.6	Gap Assessment Compliant Level	23
2.7	Maturity Benchmark of Compliant for Each Domain	23
2.8	The information security risk process by ISO 27005 (Cath Everett, 2011)	29
3.1	ISMS implementation Methodology	44
3.2	Sample Spider Web Diagram on Maturity Level	49
4.1	ISMS Committee Organization Chart	54
4.2	ISMS Controls Compliant Level	62
4.3	Example of Gap Assessment Report	63
5.1	ISMS Controls Maturity Level	77
5.2	Percentage of ISMS Controls Maturity Level	78
5.3	Percentage of ISMS Compliant	92

LIST OF APPENDIX

APPENDIX	TITLE	PAGE
A	PROJECT GANTT CHART	103
B	ISO27001 COMPLIANCE CHECKLIST	107
C	CHECKLIST 1	109
D	CHECKLIST 2	113
E	CHECKLIST 3 (Risk Assessment Report)	117
F	THREAT LIST	127
G	VULNERABILITIES LIST	129
H	STATEMENT OF APPLICABILITIES (SOA)	132

CHAPTER 1

INTRODUCTION

1.1 Overview

In recent years, Cybercrime and Cybercriminal activities are relatively concerning to most of the organization as they growth of their businesses widely especially the way organization is managing the information asset to prevent information leakage is still the most challenging issue. As of today, when the Government is planning to enforce information security policy such as Personal Data Protection Act, Cyber Law Act, and Evidence Act are getting important for the organization to comply. Most of the organization seeing the challenges to comply with this regulatory and more importantly the question will be “What should we do about it” when it comes to the managing the information security as a whole on their information assets, people, processes and at the same time to adhere the legal compliance.

IEC/ISO27001 Information Security Management System (ISMS) is to provide a standard framework, governance and guidance on managing information security within an organization. In the IEC/ISO27001 ISMS, it is focusing on the information security based on the three important constraints such as people, process and technology. Furthermore, the information security governance shall be defined clearly in the organization policy and procedures, and thereafter the policy enforcement is mandatory processes to ensure all the employees comply to the company policy that approved and supported by the management.

In this study, the implementation of ISMS will be conducted on the IT Services Centre (ISC) organization as a case study to identify the gaps of ISMS best practices and the implementation roadmap is focusing on the planning stage of ISMS implementation. The core business of the IT Services Centre (ISC) is providing IT services and operation support to the various organizations, which focusing in Property investment businesses. The ISC has identified the Data Centre activities as the scope for the ISO27001 ISMS certification.

At a glance, the following Table 1.1 shows the number of ISO27001 certification issued worldwide. As of August 2012, total of 66 Malaysia organizations that were declared their ISO27001 certification out of the total 7940 organizations world-wide. Based on the total number of certificate issued for each country, Malaysia was ranged at 12 worldwide and this shows that ISO27001 certification is important and brings benefit to the organization.

Table 1.1: Number of Certificates Per Country (Version 215, August 2012). (http://www.iso27001certificates.com)

Japan	4152	Singapore	29	Belgium	3
UK	573	Saudi Arabia	24	Gibraltar	3
India	546	UAE	19	Lithuania	3
Taiwan	461	Bulgaria	18	Macau	3
China	393	Iran	18	Albania	3
Germany	228	Portugal	18	Bosnia Herzegovina	2
Czech Republic	112	Argentina	17	Cyprus	2
Korea	107	Philippines	16	Ecuador	2
USA	105	Indonesia	15	Jersey	2
Italy	82	Pakistan	15	Kazakhstan	2
Spain	72	Colombia	14	Luxembourg	2
Malaysia	**66**	Vietnam	14	Malta	2
Poland	61	Iceland	13	Mauritius	2
Thailand	59	Kuwait	11	Ukraine	2

1.2 Background of the Problem

IT Services Centre Sdn. Bhd. (ISC) has an intention to reduce the cost and complexity of its IT infrastructure, while continuing to support multiple operations systems. The challenge to the implementation of ISC was in deciding on the right IT governance and security best practice framework to drive and manage the day-to-day operation in a secure and holistic manner. With the existing Information Technology Infrastructure Library (ITIL) framework is being practicing internally, ISC would like to uphold the principles of good IT governance, risk management, IT security and controls presently wishes to further strengthen these by achieving ISO/IEC27001 (the information security management system certification standard).

Based on the research study in common security threats faced by most of the organization, the researcher Lo and Chen (2012) highlighted the cybercrime was one of the key concerns by most of the organization such as information security breaches, identity theft and financial fraud. Subsequently, the famous common security threats is insider threats as described by Farn et al. (2008). The insider was classified into 2 types – malicious and non-malicious. The key challenges by most of the organization now days, they are more concerning on the non-malicious attack, meaning the defects of the information security breach was caused by unintentionally or careless with lack of knowledge or experience employees. Hence, most of the organizations believe that the insider threats are the most dangerous and difficult to control without clear understanding on the segregation of duties and responsibilities.

As the IT Services Centre has never conducted any feasibility study on managing the information security, the gap assessment is method that allows the organization to conduct a feasibility study on assessing the maturity level of current practice of ISMS. The outcome from the gap assessment could derive the approach and initiatives to implement the ISO27001 ISMS within an organization.

Risk assessment also playing an important role to ensure the organization is understand their risk profile by considering the tolerant risk versus the risk appetite on their day-to-day business operation (Cath Everett, 2011).

Therefore, the consideration of ISO27001 ISMS information security framework could potentially minimize the risks as mentioned above that allow the

organization to maintain the security controls and improve confidentiality, integrity and availability.

1.3 Problem Statement

The information security is getting important now days that most of the organizations are concerning how to control and prevent the confidential information leakage from the organization to the outsider. The IT Services Centre does not have any clear visibility of the current maturity level of managing information security. Based on their existing practices, there is no benchmark or IT security framework for the organization to follow and adopt. Therefore, this research study is focus on the significant feasibility study on how the organization can adopt the ISO27001 ISMS standard framework in order to apply the recommended security controls and best practices to mitigate the complexity of infrastructure of organization information leakage and improve confidentiality, integrity and availability of information security within an organization.

1.4 Project Aim

The aim of this study is to determine and examine the existing security gaps and current controls against the ISO27001 ISMS standard. A gap assessment report will be prepared together with the proposed initiatives of ISMS implementation approach to achieve the research objectives as stated in this study. This study also focused on the feasibility study by conducting the gap assessment and risk assessment that incorporating the ISO27005 risk assessment framework. The outcome of the gap assessment allows the management to have better understanding on the current maturity level of managing information security within the organization. The key outcome of this project is to propose a implementation approach as accordance to ISO27001 ISMS standard in order to maintain the confidentiality, integrity and availability of information systems within the organization.

1.5 Research Questions

i. What are the current security trends and the best practices of corrective and preventive actions for the organization to maintain confidentiality, integrity and availability of information security?
ii. What is the approach to conduct ISMS gap assessment exercise and the presentation of gap assessment report?
iii. What is the methodology used to conduct risk assessment?
iv. How to formulate the planning on ISMS policy document to comply with ISO27001 standard?

1.6 Research Objectives

i. To identify the current trend of common information security incidents and understand the ISO27001 ISMS practices on corrective and prevention actions.
ii. To propose gap assessment approach and carry out a feasibility study to conduct gap assessment by identifying the current maturity level of ISMS in IT services environment.
iii. To propose ISO27001 ISMS risk assessment methodology for the organization and finalize a complete risk assessment report.
iv. To formulate an implementation plan based on ISO27001 ISMS standard.

1.7 Research Scope

The scope for this study focuses on conducting a feasibility study by incorporating the ISO 27001 ISMS standard in IT Services Environment. The implementation scope covers the data centre, hosting facilities and IT operation services in IT Services Environment.

The ISMS scope covers the data centre facilities management includes the services offering such as data centre hosting facilities, and the day-to-day operation services within the data centre of the IT Services Centre.

The implementation of ISO 27001 ISMS will be running as accordance to the project phases. The basis of the project phases is for monitoring, guidance and management of the ISO27001 ISMS implementation for the IT Services Centre.

For the purpose of this ISO27001 ISMS implementation, the project phases break down into Initiation, Planning, Execution, Monitoring & Control and Project Closure & Post implementation. Table 1.2 showing the direct mapping on project phases to the ISO27001 ISMS implementation phase..

Table 1.2: ISO27001 ISMS Implementation Phase and Project Phases Mapping

ISO27001 ISMS Implementation Phase	**Project Phases**	**Research Study Cover**
Research Methodology Project Proposal Initial Findings	Project Initiation Project Planning	In Scope
Gap Assessment Scope and security organization Risk Assessment Methodology & Report	Project Execution	In Scope

1.8 Summary

This chapter discussed the introduction of the current security risks and concerns to most of the organization and how ISO27001 ISMS is able to manage the information security for an organization based on the security framework point of view. In summary, this chapter also included the study of problem background faced by the existing organization. More importantly, the research questions and research objectives were derived and set as a focus for the entire research project study. The next chapter will be discussing the literature review mainly focusing on the security risks currently facing by most of the organization, and the various risk assessment methodologies were discussed as part of the ISO27001 ISMS mandatory exercise. Beside, some key lesson learned during the ISO27001 ISMS implementation will be discussed that could benefit to this research study.

REFERENCES

Armerding Taylor (2012). The 15 worst data security breaches of the 21st Century. URL: Last Access on http://www.csoonline.com/article/700263/the-15-worst-data-security-breaches-of-the-21st-century.

Al-Mayahi, and P. Mansoor. (2008). ISO27001 gap analysis – case study.

Boris Mutafelija and Harvey Stromberg. (2012). Mapping ISO to CMMI. Software Engineering Institute. URL: Last Access on:
http://www.sei.cmu.edu/cmmi/solutions/cmmi12-iso.cfm.
http://www.sei.cmu.edu/cmmi/compatibility/index.cfm.
http://www.sei.cmu.edu/cmmi/compatibility/iso.cfm.

Basie von Solms. (2005). Information Security governance: COBIT or ISO 17799 or both. Computers & Security. 24: 99-104.

Cath Everett. (2011). A risky business: ISO 31000 and 27005 unwrapped. URL: Last Access on:
http://www.sciencedirect.com/science/article/pii/S136137231170015X

Candace Gray. (2003). Understanding and complying with HIPAA. Journal of PeriAnesthesia Nursing. 1089-9472.

Chaiw Kok Kee. (2012). Journey towards Excellence in Information Security Management ISO 27001 ISMS – A Lesson Learnt. URL: Last Access on:
http://www.skmm.gov.my/skmmgovmy/media/General/pdf/ISMS_ASTRO.pdf

Chi-Chun Lo, and Wan-Jia Chen. (2012). A hybrid information security risk assessment procedure considering interdependences between controls. Expert Systems with Application. 39: 247-257.

Christian, B., and Lahti. (2005). Sarbanes-Oxley IT Compliance Using COBIT and Open Source Tools. Pg. 31-57. Chapter 2 - SOX and COBIT Defined.

Chris Byrnes. (2012). Gartner Powerpoint Presentation Slide. Developing a Realistic Infosec Management Strategy.

Collmann, J., Lambert, D., Brummett, M., DeFord, D., Coleman, J., Cooper, T., McCall, K., Seymour, D., Alberts, C., and Dorofee, A. (2004). Beyond good practice: why HIPAA only addresses part of the data security problem. International Congress Series. 1268: 113-118.

Da Veiga, A., and Eloff, J. (2010). A framework and assessment instrument for information security culture. Computers & security. 29: 196-207.

Edward Humphreys. (2008). Information security management standards: Compliance, governance and risk management. Information Security Technical Report. 13: 247-255.

Gary Hardy. (2006). Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. Information Security Technical Report. 55-61.

ISO27K Toolkit. IsecT Ltd (2012).
URL: Last Access on http://www.iso27001security.com/html/27001.html.

Karin Hone, and Eloff, J.H.P. (2002). Information security policy - what do international information security standards say. Computers & Security, Volume 21, Issue 5, Page: 402-409.

Kruger, H.A., and Kearney, W.D. (2006). A prototype for assessing information security awareness. Computers & Security. 25: 289-296.

Kwo-Jean Farn, Shu-Kuo Lin, and Chi-Chun Lo. (2008). A study on e-Taiwan information system security classification and implementation. Computer Standards & Interfaces. 30: 1-7.

Nigel Martin, and John Rice. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. Computers & Security. 30: 803-814.

Sevgi Ozkan, and Bilge Karabacak. (2010). Collaborative risk method for information security management practices: A case context within Turkey. International Journal of Information Management. 30: 567-572.

Steve Wright. (2006). Measuring the effectiveness of security using ISO27001 White Paper.

Stuart Broderick, J. (2006). ISMS, security standards and security regulations, Information Security Technical Report, Volume 11, Issue 1, Page: 26-31.

Whitman ME, and Mattord HK. (2003). Principles of information security. Kennesaw State University: Thomson Course Technology.

Zhou, Zheng, Liu, and Brent, J. (2005). HIPAA compliant auditing system for medical images. Computerized Medical Imaging and Graphics 29: 235-241.