

A STUDY OF STANDARDS AND THE MITIGATION OF RISK IN INFORMATION SYSTEMS

A thesis submitted to The University of Manchester for the degree of
Doctor of Philosophy in the Faculty of Humanities

2011

DANIEL GIDEON DRESNER

**MANCHESTER BUSINESS SCHOOL
BUSINESS SYSTEMS DIVISION**

This page intentionally blank.

CONTENTS

LIST OF FIGURES	7
LIST OF TABLES	9
ABSTRACT.....	13
DECLARATION AND COPYRIGHT STATEMENT.....	15
PUBLICATIONS	17
ACKNOWLEDGEMENTS.....	19
CHAPTER 1. ABOUT THIS THESIS	23
1.1 About this chapter	23
1.2 The hypothesis	23
1.3 Research questions	24
1.3.1 Questions and early methodological considerations	24
1.3.2 What prompted the research?	27
1.4 Personal motivation for this research	32
1.5 The design and structure of this thesis.....	34
CHAPTER 2. A LITERATURE REVIEW	37
2.1 About this chapter.....	37
2.2 Why is the problem worthy of research?	39
2.3 Attitudes to standards	40
2.4 What is risk?	42
2.5 Risk management models	45
2.6 What is a standard?.....	48
2.7 The Toynbee conflict	50
2.8 Approaches or responses to risk mitigation: a taxonomy.....	55
2.9 How have attitudes to risk changed?	56
2.10 Why is risk a problem?	57
2.11 Who says it's a problem? The drivers, stakeholders and interested parties	62

2.12	Who sets standards?.....	68
2.12.1	National and International Standards Bodies	68
2.12.2	Professional Bodies	69
2.12.3	Consortia.....	69
2.13	How are standards set?.....	70
2.14	What is the status of the standards?	76
2.15	Differentiation: when is a standard not a standard?.....	78
2.16	How much detail do standards provide?	78
2.17	Conclusion: leading to human vulnerabilities in information systems	79
CHAPTER 3.	LINKING RISK TO STANDARDS	81
3.1	About this chapter.....	81
3.2	Methodology	82
3.2.1	Choice and selection.....	82
3.2.2	Application of the methodology.....	91
CHAPTER 4.	PROJECT DELTA δ: THE RISK OF HUMAN VULNERABILITIES IN INFORMATION SYSTEMS	113
4.1	This chapter in context	113
4.2	What is a human vulnerability?.....	114
4.3	Finding an acceptable level of risk	114
4.4	Software and systems quality.....	116
4.5	Methodology	116
4.6	Application	124
4.6.1	Acquisition of data.....	124
4.6.2	Questionnaire design	128
4.6.3	Analysis method.....	133
4.6.4	User engagement.....	146
4.6.5	Results	149
4.6.6	What may be derived from these results?	157
4.6.7	A tool to identify Human Vulnerabilities	160
4.6.8	The application of the method in establishing improvements in risk awareness	160

4.6.9	Training content	162
4.6.10	A second test of the tool	164
4.6.11	The feasibility study report	164
CHAPTER 5. CASE STUDIES: WHAT ARE ORGANISATIONS DOING TO MITIGATE RISK?		165
5.1	About this chapter.....	165
5.2	Why were these case studies chosen?.....	165
5.3	Developing standards to treat risks: defining a collective methodology for investigation.....	167
5.4	Deploying standards to treat risk: defining a collective methodology for fieldwork	172
5.5	Applying the collective methodology to the development and adoption of standards to treat risk during the procurement of information systems	178
5.5.1	Project ε: Accredited UK	178
5.5.2	Project ζ: The Local e-Government Standards Board	185
5.6	Fieldwork: the deployment of standards to treat risk.....	194
5.6.1	Project η: Housing association – information systems risk (security) strategy.....	194
5.6.2	Project θ: Fieldwork in construction – risk to treatment analysis	202
5.6.3	Project ι: Pensions and actuarial services – risk management (security) policies	204
5.7	Resulting intervention	205
5.7.1	Project η: Housing association – information systems risk (security) strategy.....	205
5.7.2	Project θ: Fieldwork in construction – risk to treatment analysis	218
5.7.3	Project ι: Pensions and actuarial services – risk management (security) policies	219
5.8	Conclusion	221
CHAPTER 6. ANALYSIS, CONCLUSIONS, AND FUTURE WORK		223
6.1	About this chapter.....	223
6.2	Revisiting the aims and objectives of the research	223
6.3	A personal epistemology	224

6.4	Answering the research questions	226
6.5	How do the outcomes of the projects explain the answers to the research questions?	228
6.6	Reviewing the methodologies.....	232
6.7	Contribution to the body of knowledge	234
6.7.1	Idiosyncrasy as the saviour of standardisation	235
6.7.2	Linking risk and standards	239
6.7.3	Security culture as an indicator of which standards are needed	240
6.7.4	Enhancing learning through research frameworks	244
6.8	Recommendations for future work.....	245
6.8.1	Do standards mitigate risk?	246
6.8.2	Developing the tool to find human vulnerabilities in information systems ..	246
6.8.3	The language of risk.....	250
6.8.4	Looking back	252
6.9	Conclusions	252
REFERENCES.....		255
Appendix A. References for Project Delta δ: The risk of human vulnerabilities in information systems		267
Appendix B. Project catalogue		269
Appendix C. Achievements based on this research		271
A.1.	Projects.....	271
A.2.	Books.....	271
A.3.	Conferences and seminars.....	271
A.4.	Papers and articles.....	273
A.5.	Education and training.....	274
A.6.	Action research/field work	275
A.7.	Other activity.....	276

Word count: 78474

LIST OF FIGURES

Figure 1: Rigour in the method. Is the use of standards coincidental in the mitigation of risk?	25
Figure 2: Elements relevant to any piece of research (Checkland and Holwell, 1998)	29
Figure 3: Desk research and case studies	30
Figure 4: Relevance of the case studies to the three research questions	30
Figure 5: Checkland and Holwell's research construct as applied	31
Figure 6: The design and structure of the thesis	34
Figure 7: This chapter in the context of the thesis	37
Figure 8: Literature and its relative strength – a personal view	38
Figure 9: The project envelope	44
Figure 10: Risk management extremes	45
Figure 11: Risk stirs Emotion which promotes Idiosyncrasy that releases the Knowledge from standards	50
Figure 12: Project envelope affected by risk and regulated by mitigating standards	52
Figure 13: Layers of risk and a taxonomy of response	53
Figure 14: Standards are localised and lessons learnt are centralised	54
Figure 15: Risk threatens the desired shape of the Project Envelope	55
Figure 16: Uptake of accredited BS 7799 (ISO/IEC 27001) certification	65
Figure 17: Maturing: Explicit to Explicit	71
Figure 18: This chapter in the context of the thesis	81
Figure 19: A sample from the catalogue tables	109
Figure 20: Creating and updating the catalogue	112
Figure 21: This chapter in the context of the thesis	113
Figure 22: The risk attitude spectrum (Hillson and Murray-Webster, 2007)	118
Figure 23: Risk criteria	119
Figure 24: Communications models	120
Figure 25: Creating a zone of common acceptance using standards to treat risks	121
Figure 26: Calculating the depth of a human vulnerability in an information system	127
Figure 27: Interviewee engagement process	147

Figure 28: In-depth interviews: organisational appetite compared with individual attitude...	154
Figure 29 A comparison of organisational appetite with individual attitude from the on-line survey	155
Figure 30: The frequency of scored responses (scores rescaled to 0 – 100 range)	157
Figure 31: The proforma chart of appetite and attitude scores.....	160
Figure 32: Improvement in risk and treatment awareness measured in the first session of training.....	164
Figure 33: This chapter in the context of the thesis	165
Figure 34: The overall structure of the Accredited UK standard.....	178
Figure 35: The LeGSB standards life cycle	186
Figure 36: The structure of ISO/IEC 27001 for information security management.....	196
Figure 37: ISO/IEC 27002 controls for information security management	199
Figure 38: Structure for the questions repeated across the stakeholders interviewed.....	200
Figure 39: The organisation's information life cycle.....	206
Figure 40: Core information assurance strategy for the housing association.....	210
Figure 41: Relevance of the case studies to the three research questions	226
Figure 42: Risk stirs Emotion which promotes Idiosyncrasy that releases the Knowledge from standards.....	235
Figure 43: Standards are localised and lessons learnt are centralised	238
Figure 44: When is a standard not a standard?.....	239
Figure 45: A risk chart: where are mitigating activities needed?	241
Figure 46: Placing respondents on the at-risk from human vulnerabilities monitor	242
Figure 47: The three-tiered framework of knowledge and research	244
Figure 48: A framework for learning about information assurance	245
Figure 49: Activity in the method for finding the human vulnerabilities in information systems.....	248
Figure 50: The gap between a non-expert language for formal specification of security requirements and available standards	251

LIST OF TABLES

Table 1: The classic maturity model	47
Table 2: Approaches to risk mitigation	56
Table 3: Realised risk and the potential for standards intervention	59
Table 4: Roles in the Soft Systems Methodology	63
Table 5: Standards development processes.....	72
Table 6: Projects documented in this chapter.....	81
Table 7: Research sources and validation.....	82
Table 8: The method for selecting the 10 risks.....	85
Table 9: The method for setting the project brief for BSI.....	87
Table 10: Methodological elements supporting the research questions.....	88
Table 11: Research and development stages for cataloguing IA standards	89
Table 12: Surveys reviewed for the survey.....	92
Table 13: Common groups of risk from the surveys	94
Table 14: Risks from the surveys sorted into the groups.....	98
Table 15: Excluded risks	104
Table 16: 'Delphi' panel response.....	105
Table 17 NCC members by sector.....	106
Table 18: NCC members by IT staff number	106
Table 19: Ranking of the risk treatments in the catalogue.....	111
Table 20: Research stages for the human vulnerabilities detection methodology	122
Table 21: Project γ literature review.....	124
Table 22: Questions of attitude	131
Table 23: Attitudes to risk.....	132
Table 24: Application of scores to answers about their organisations/communities	134
Table 25: Adjustment of risk treatment to account for behaviour.	137
Table 26: Analysis of an individual.....	139
Table 27: Scores for Table 30.....	140
Table 28: Explanation of scores for Table 27	141

Table 29: Second party evaluation of the individual (scored for 'Free thought' or policy status unknown)	142
Table 30: Second party evaluation of individuals in general in the community or organisation (scored for 'Free thought' or policy status unknown)	143
Table 31: For consideration of how the appetite score of the organisation /community may be affected by the respondent	144
Table 32: Scores for responses to the On-line survey analysis of an Organisation's appetite for risk.....	145
Table 33: Scores for responses to the On-line survey analysis of an individual's attitude to risk	146
Table 34: IS/IT roles.....	148
Table 35: Options for investigation	149
Table 36: Before and after training – measures of risk attitude	163
Table 37: Case studies documented in this chapter.....	166
Table 38: The development of the action research methodology for this study	167
Table 39: Key stakeholder groups for the Accredited UK project.....	169
Table 40: LeGSB project checkpoints.....	172
Table 41: Risk attributes for housing association information	173
Table 42: Possible action research approaches to ISMS implementation	174
Table 43: Action research across the life cycle of a standard	177
Table 44 Source standards for Accredited UK.....	179
Table 45: The core format of the Accredited UK standard	181
Table 46: Accredited UK Maturity Model for Process Evidence	183
Table 47: Results and interpretation of Project ε (Accredited UK).....	184
Table 48: RFPs selected to test the standards adoption process	188
Table 49: Trialling the standardisation method.....	189
Table 50: Results and interpretation of Project ζ (LeGSB)	194
Table 51: Project η: Method for defining an information systems risk (security) strategy in a housing association	197
Table 52: Method for project θ: fieldwork in construction – risk to treatment analysis	202
Table 53: Method for project ι: A review of risk management (information security) policies in a financial services firm delivering pensions and actuarial products.	204

Table 54: Recommendations for the housing association target of Project η	206
Table 55: Recommended contents of an information security policy	211
Table 56: Results and interpretation of Project η (Housing association)	218
Table 57: Results and interpretation of Project θ (Construction)	219
Table 58: Results and interpretation of Project ι (Finance).....	221
Table 59: Contrasting three types of action research	222
Table 60: Research questions	224
Table 61: Research questions answered.....	227
Table 62: Research questions: what can we learn from the research projects?	229
Table 63: How the research contributes to the body of knowledge	234
Table 64: Ranking of the risk treatments in the catalogue.....	240
Table 65 Benchmarks of risk appetite and risk attitude	241
Table 66: Components of the method for finding the human vulnerabilities information systems	249
Table 67: Final evaluation of the research questions	253
Table 68: Variables for the methods' success	254

This page intentionally blank.

ABSTRACT

Organisations from the multinational Organisation for Economic Cooperation and Development through to national initiatives such as the UK's Cabinet Office, have recognised that risk – the realisation of undesirable outcomes – needs a firm framework of policy and action for mitigation. Many standards have been set that implicitly or explicitly expect to manage risk in information systems, so creating a framework of such standards would steer outcomes to desirable results.

This study applies a mixed methodology of desk enquiries, surveys, and action research to investigate how the command and control of information systems may be regulated by the fusion and fission of tacit knowledge in standards comprising the experience and inductive reasoning of experts. Information system user organisations from the membership of The National Computing Centre provided the working environment in which the research was conducted in real time. The research shows how a taxonomy of risks can be selected, and how a validated catalogue of standards which describe the mitigation of those risks can be assembled taking the quality of fit and expertise required to apply the standards into account. The work bridges a gap in the field by deriving a measure of organisational risk appetite with respect to information systems and the risk attitude of individuals, and linking them to a course of action – through the application of standards – to regulate the performance of information systems within a defined tolerance. The construct of a methodology to learn about a framework of ideas has become an integral part of the methodology itself with the standards forming the framework and providing direction of its application.

The projects that comprise the research components have not proven the causal link between standards and the removal of risk, leaving this ripe for a narrowly scoped, future investigation. The thesis discusses the awareness of risk and the propensity for its management, developing this into the definition of a framework of standards to mitigate known risks in information systems with a new classification scheme that cross-references the efficacy of a standard with the expertise expected from those who apply it. The thesis extends this to the idea that the framework can be scaled to the views of stakeholders, used to detect human vulnerabilities in information systems, and developed to absorb the lessons learnt from emergent risk. The research has clarified the investigation of the security culture in the thrall of an information system and brought the application of technical and management standards closer to overcoming the social and psychological barriers that practitioners and researchers must overcome.

This page intentionally blank.

DECLARATION AND COPYRIGHT STATEMENT

Declaration

No portion of the work referred to in the thesis has been submitted in support of an application for another degree or qualification of this or any other university or other institute of learning.

Copyright Statement

- i. The author of this thesis (including any appendices and/or schedules to this thesis) owns any copyright in it (the "Copyright") and he has given The University of Manchester the right to use such Copyright for any administrative, promotional, educational and/or teaching purposes.
- ii. Copies of this thesis, either in full or in extracts, may be made only in accordance with the regulations of the John Rylands University Library of Manchester. Details of these regulations may be obtained from the Librarian. This page must form part of any such copies made.
- iii. The ownership of any patents, designs, trade marks and any and all other intellectual property rights except for the Copyright (the "Intellectual Property Rights") and any reproductions of copyright works, for example graphs and tables ("Reproductions"), which may be described in this thesis, may not be owned by the author and may be owned by third parties. Such Intellectual Property Rights and Reproductions cannot and must not be made available for use without the prior written permission of the owner(s) of the relevant Intellectual Property Rights and/or Reproductions.
- iv. Further information on the conditions under which disclosure, publication and exploitation of this thesis, the Copyright and any Intellectual Property Rights and/or Reproductions described in it may take place is available from the Head of School of Manchester Business School (or the Vice-President) and the Dean of the Faculty of Life Sciences, for Faculty of Life Sciences' candidates.

This page intentionally blank.

PUBLICATIONS

Books

Dresner, D.G., (2006) *Information Security Management: A standards approach. A Best Practice guide for decision makers in IT*, The National Computing Centre, ISBN 0-85012-885-4

Armstrong, J., Rhys-Jones; M., Dresner, D., (2004) *Managing Risk: Technology and Communications*, Lexis Nexis, ISBN/ISSN 0-7545-2468-X (Chapter 7: Managing Operational ICT Risk with Standards and Best Practice)

Papers

Dresner, D.G., (2010). *Business Oriented Security Strategy: when did you last see your data?* The National Computing Centre Guidelines for IT Management 332

Dresner, D.G., (2008). *Information Systems Continuity - a framework for accountability, continuity, quality, security, sustainability and maturity*. The National Computing Centre Guidelines for IT Management 319

Dresner, D.G., (2008). Desert Island Standards II. The National Computing Centre Guidelines for IT Management 275.

Dresner, D.G., and Wood, J.R.G. (2007). *Operational risk: acceptability criteria*. The Third International Symposium on Information Assurance and Security (IAS 2007), IEEE CS Press.

Dresner, D.G., Roebuck, W., (2005). ICT Legal Compliance. The National Computing Centre Legal Guideline 5.

This page intentionally blank.

ACKNOWLEDGEMENTS

University of Manchester

- Professor Bob Wood, for guidance, friendship, encouragement, and steering me towards showcasing the art of the practitioner within the rigour of experiment.
- Professor Trevor Wood-Harper, University of Manchester, for guidance, friendship, encouragement, and making me realise that in every good discussion there is a paper waiting to be written.
- Dr Joy Garfield for friendship through thick and thin, mutual respect, and being a beacon of encouragement.

The National Computing Centre

- Dr Andy Hopkirk for pointers and guidance throughout the research projects and a keen view from the academic-industry bridge.
- Christine Jack for the evaluation of the rapid survey element of the investigation into the human vulnerabilities in network security.

Cabinet Office

- Dr Steve Marsh for inspiration and leadership that helped to light the blue touch paper.

And

- Beverley Filer for the diligent proof reading. I can only pray that my implementation of the corrections do justice to her attentiveness and encouragement.
- Avi and Sherelle, Shoshanna, Eliana, and Yehuda – the real brains in the family.
- Dr Harold Dresner ז"ל all this would have meant so much to him.

And with thanks to the A-mighty for 7 years of plenty.

This page intentionally blank.

ACRONYMS

ALARM	The National Forum for Public Sector Risk Management
BERR	Department for Business Enterprise and Regulatory Reform (replaced by BIS)
BIS	Department for Business Innovation and Skills
BoK	Body of Knowledge
BSI	British Standards Institution
CESG	Communications and Electronic Security Group of GCHQ
CMM	Capability Maturity Model
CPNI	Centre for the Protection of the National Infrastructure (formerly National Infrastructure Coordination Centre NISCC)
CSIA	Central Sponsor for Information Assurance (renamed IS&A)
DTI	Department of Trade and Industry (replaced by BERR)
ENISA	European Network and Information Security Agency
FSA	Financial Services Authority
GCHQ	Government Communications Headquarters
HR	Human Resources
IA	Information assurance
ICAEW	Institute of Chartered Accountants in England and Wales
ICO	Information Commissioners Office
ICT	Information and Communication Technologies
IS&A	Information Security and Assurance
ISMS	Information Security Management System
ISO	International Standards Organization
LeGSB	Local e-Government Standards Body (Board)
MARS	Methodology to Articulate Requirements for Security
MP3	MPEG-1 or MPEG-2 Audio Layer 3
MPEG	Moving Picture Experts Group

NCC	The National Computing Centre
OECD	Organisation for Economic Cooperation and Development
PCI DSS	Payment Card Industry Data Security Standard
PID	Project Initiation Document
RFC	Request for Comment
RFP	Request for Proposal
RIPA	Regulation of Investigatory Powers Act
SCES	Security Climate Evaluation Survey
SCTI	Security Culture Type Indicator
SEC	Securities and Exchange Commission
SEI	Software Engineering Institute (Carnegie Mellon University)
SME	Small to Medium-sized Enterprise
SQL	Structured Query Language
SSM	Soft Systems Methodology
TSE	Toward Software Excellence
UPS	Uninterruptible Power Supply
VDU	Visual Display Unit
WARP	Warning, advice, and reporting point
WEP	Wired Equivalent Privacy
WPA and WPA2	Wi-Fi Protected Access
XML	eXtensible Markup Language

CHAPTER 1. ABOUT THIS THESIS

1.1 About this chapter . . .

In this chapter...

- I suggest that knowledge of the risks to information systems could be signposts to the standards that would treat them.
- Consider the questions that have driven this research.
- Consider the motivation for this research.
- Map out the design and structure of the thesis.

1.2 The hypothesis

*In this section, I suggest that knowledge of the risks to information systems creates signposts to the standards that would treat them. The research of this key premise – that **standards mitigate risk** – led me to consider the accessibility of standards and how standards may be linked to respective risks.*

This thesis addresses the treatment of risk within the development and use of information systems. Both the public and the private sectors face many risks which must be managed or mitigated in order to avoid undesirable outcomes (Swann, 2000). The lessons learnt through the distillation of best practice and the use of proven tools and techniques, as encapsulated in standards, can support organisations¹ in mitigating such risks (DTI, 2005) but despite this research, The National Computing Centre had observed that only 10% of organisations had a formal and well integrated IS/IT risk management framework (NCC, 2003). Managing risk is an integral part of good governance (Turnbull, 1999) and is something many managers do already in one form or another in daily decision making; risk management recognises and prepares for a range of possible future outcomes (NISCC/CESG, 2005 and Morton, 2002).

The ubiquitous and pervasive nature of information systems in business would suggest that organisations would be well advised to apply standards that mitigate at least the known risks. To achieve this, the relevant information contained within standards must be accessible. 'Standards mitigate risk' is my core hypothesis.

¹ This thesis uses the labels 'organisation' and 'business' interchangeably. In both instances, no assumptions are made as to their size and complexity.

There are many standards which can usefully be applied to the development and use of information systems². Therefore, there is a clear need for an accessible, scalable, route map through such standards to assist all sizes of business in understanding, selecting, and utilising the appropriate standards for their individual circumstances. Such a route map would create a beneficial environment for innovation together with a stable, sustainable 'ecosystem' through which existing practices can be supported and the production of new practices optimised. Weaker links in supply chains will therefore be strengthened thus encouraging trust and security (Dresner and Wood, 2007). The challenge is to identify the respective risks and then to link them to the mitigating standards (CESG, 2009). This lexicon of risk and mitigating standards could then be represented in a scalable framework that would be useful for corporate bodies, SMEs, academe and the public sector. Such a prescription for reducing the likelihood of known errors should provide the confidence for innovation (*see the discussion of the 'Toynbee Conflict' in chapter 2*). As long as the dynamic of risks and change is recognised, the framework of risks and risk-treating standards would inhibit reliance on the checklist-bound mentality associated with compliance with documented standards.

1.3 Research questions

In this section I consider the three questions that have driven this research:

- 1 Do implemented 'Standards' mitigate risk?
- 2 Can 'Standards' be made more accessible?
- 3 How do you link risks to the 'Standards' that may mitigate them?

1.3.1 Questions and early methodological considerations

My research looks at how to link risks to the standards that may mitigate them. I bear in mind the risk (sic!) that any methodology which may emerge from the research could, when employed, become a risk in itself (Thomas, 1997). What problems may emerge as a result of deploying the methodology? Because of this, my analysis in Chapter 6 also considers where the selected standards could affect the outcomes of the mitigating action, the difference in outcomes that may result from different approaches to analysis, and how the interpretation of standards – their accessibility – may affect the use of standards to mitigate risk.

These potential conundrums are laid out in *Figure 1* which suggests that it may be possible to get the wrong result by implementing the correct method (as defined by a standard) and

² See catalogues for BS/CEN/ISO/IEC et. al., the e-Government Interoperability Framework, *Technical Standards Catalogue*, version 6.1, 17 September 2004, and *A Catalogue of Publicly Available Information Assurance Guidance* (described in Chapter 3)

vice versa. This uncertainty bears out the need for my investigations into the application of codified, acquired knowledge of good practices – standards – as mitigating actions to treat risk and the causes of risk. Instances where the application of the knowledge – that is, the implementation of the standard in practice – becomes a risk in itself are exemplified by the popular recommendation to encrypt data (CESG, 2009 and Cabinet Office, 2008) to protect it from inappropriate disclosure. This may render that data inaccessible to the legitimate users if the decryption key is forgotten (Anderson, 2008).





	Standards Implemented	Standards not Implemented
Risks Mitigated	 <p>Appropriate action is carried out with the expected good results.</p>	 <p>Appropriate action is not carried out but good results happen anyway.</p>
Risks realised	 <p>Appropriate action is carried out with unexpected bad results.</p>	 <p>Appropriate action is not carried out with expected bad results.</p>

Figure 1: Rigour in the method.

Is the use of standards coincidental in the mitigation of risk?

A method of risk assessment is only complete if it weighs up the balances of implementing the risk treatment suggested against accepting it untreated. A quick reaction to risk can have greater adverse effects than the realised risk (CESG, 2009 and Ranum, 2005).

Two core questions were originally considered for this research (Dresner, 2005):

- Can standards be made more accessible by relating them to risk and the causes of risk?
- Do implemented standards mitigate risk?

My interest in these questions lies in the observation that documented standards tend to be shunned by people and their organisations unless some external influence – such as the threat of a fine from a regulatory authority³ – suggests that they would support their

³ Typically exemplified by £980,000 fine imposed by the Financial Services Authority (FSA) on the Nationwide Building Society that had lost a laptop computer holding unprotected, confidential

objectives. This may in the crudest form be a regulator (in this context, a body who sets regulations) or stakeholder demanding compliance, or the self-realisation of a problem awakening a readiness to embrace the lessons learnt elsewhere. If this 'problem' is referred to as 'risk' – uncertainty that matters (Hillson and Murray-Webster, 2007) – it is observed that when faced with risk, people become more amenable to approaching these documented standards when they understand them to be an explicit encapsulation of best practice. That is, what to do about it. This is an observation made during my work of over 10 years on the members' help desk at The National Computing Centre. Information systems practitioners looking for support with a variety of sociotechnical issues in the life cycle of their information systems would be satisfied by being referred to published standards hithertofore not considered or even wholly undiscovered⁴. The documented standards provided the trusted, recorded know-how to deal with the risks faced⁵. This is exemplified by the challenge to capture knowledge and keep it relevant in its explicit form and release it back into a tacit environment. This is discussed in Chapter 2.

My intention was to investigate these questions respectively by:

- (1) Designing a usable framework from which mitigating standards may be identified from the risks that give rise to their need.
- (2) Creating a methodology to populate this framework.
- (3) The analysis of standards implementation to understand if risk was managed as a result of the application of standards.

From a practical viewpoint, the framework manifested as *A Catalogue of Publicly Available Information Assurance Guidance* (project γ which is discussed in Chapter 3). This catalogue adapted the taxonomy of risks to information documented in the International Standard ISO 17799:2005 (now 27002:2007 and often referred to as BS 7799) *Information technology — Security techniques — Code of practice for information security management*. The populated catalogue was refined using a Delphi-like method with participants acknowledged in the resulting report. However, the development of the framework catalogue was unsatisfying in providing a broad piece of research that investigated the interaction of information systems, the people involved in their life cycle of concept, development, use, and decommissioning and assumed that there would be early take up of the framework catalogue as a selection tool for risk treatments. Information assurance professionals

details of customers' bank accounts and more recently (August 2008) Zurich SA lost an unencrypted back-up tape of 46,000 account records during a routine transfer to a data storage centre, resulting in an FSA fine of £2,275,000 (including a 30% discount for prompt payment!).

⁴ A profile of NCC members can be found in Chapter 3.

⁵ See the discussion of tacit/explicit pathways in Chapter 2 referring to Nonaka, Toyama, and Konno, 2000.

welcomed the catalogue, 'a fantastic resource and the mapping to controls is exactly how we map controls through our set of HMG baseline guidance' (correspondence from CESG, 12 January 2010), but it was not widely distributed! I had created the framework postulated in the early formulation of this research, complete with a supporting paper for its sponsors about how to refresh and update it. But it was apparent that behind the fundamental hypothesis, there were clearer questions to be answered as well as the original standards-risk-mitigation paradigm. This linkage – the human factors consideration of those involved with information systems, and the practicality of applying standards in risk management were extruded as the questions which remained as the foundation for the research. I could then apply a hybrid research methodology comprising several discrete projects, combining validated desk research and action research to apply standards in the area of information security and the management of its associated risks. Taking the original questions and the methodological considerations into account, I settled on three questions:

- (1) Do implemented 'Standards' mitigate risk? Can 'Standards' be implemented to mitigate risk?⁶
- (2) Can 'Standards' be made more accessible? (How can 'Standards' be made more accessible by relating them to risk and the causes of risk? What are the barriers? Why don't people access standards?)
- (3) How do you link risks to the 'Standards' that may mitigate them?⁷

1.3.2 What prompted the research?

Managing risk is an integral part of good governance (Turnbull, 1999) in business, and good governance is realised by effective action against, at least the risks that are, or should be, known (Carr, Konda, et al., 2003). The corollary is that good governance requires not only encyclopaedic knowledge of risks but also of the accepted practices to mitigate them. Such as standards (Swann, 2000). As I have stated above, there are many standards⁸ which can usefully be applied to information systems – some of which are very specific (Cabinet Office, 2004) – but there is no accessible, scalable, route map through the body of knowledge represented by published standards that can show which standards may mitigate the risks

⁶ How can risk reduction techniques be linked to the reduction in risk with surety? cf. Y2K which is now cited as a false alarm because too few examples of the risk were realised to suggest that the value of the work done to change the date calculations of many systems was worth the effort involved. Was the lack of impact of the 'Year 2000 Problem' the result of careful analysis and reprogramming of the systems' inventory, or the overestimation of the danger caused? Does one stop an inoculation programme because outbreaks of a disease are reduced or eradicated?

⁷ Do the selected standards affect the outcomes of the mitigating action? Does the difference in outcomes that results from different analysis methods become a threat/risk?

⁸ See catalogues for BS/CEN/ISO/IEC et. al.

that those standards were created to manage. Such a route map could create a beneficial environment for innovation and a stable, sustainable 'ecosystem' for existing practices, where production can be optimised.

Connecting standards form a framework of linked ideas (Checkland, 1985). This framework may be applied in, and academically honed by, action research to an area of concern (Figure 2). My literature review (Chapter 2) establishes the area of concern for this thesis as *the treatment of risks by standards*. The experience of risk treatment, deliberately or coincidentally, encourages a codification of knowledge in the development of the standards that comprise the ideas in the framework. The emerging framework of research (Figure 3) that related directly to the research questions (Figure 4) was applied directly to the investigation of my overarching hypothesis that standards mitigate risk (Figure 5). My area of concern was the encouragement of the use of the explicit knowledge of standards in the tacit expertise displayed in the deployment of information systems. The standards 'body of knowledge' is represented in the Checkland/Holwell model as framework (F). Framework (F) maybe an ontology of standards focused by the worldview or *weltanschauung* (Checkland, 1985) of owner, actors, and customers of an information system at risk. A focus on the mitigation of risk in information systems drew my study towards standards to treat security risk, that is, risk associated with confidentiality, integrity and availability of information handled in and around those systems. The intention of my research planning – described in chapters 3, 4, and 5 – was to apply fitting methodologies to either determine the existence of the framework – such as which standards are likely to mitigate risk – or to become convinced that a belief in the causal link is futile. The framework (F) of the standards and the methodologies of the investigating projects (M) merge, in as much as the research papers yielding the learning are themselves a framework. The framework of projects overcame at least part of the problem of finding a single methodology that can present meaningful results with surety. So, the framework of projects presents itself as the answer to the meta-research questions about the efficacy of the methodology itself – is this framework a good way of investigating whether standards mitigate risk? The construction of what became a framework of frameworks is described in Chapter 6 – Analysis, conclusions and future work – in which the learning opportunity presented by the three frameworks of ideas (standards, research methodologies, and projects) yields learning about the area of concern (standards and risk).

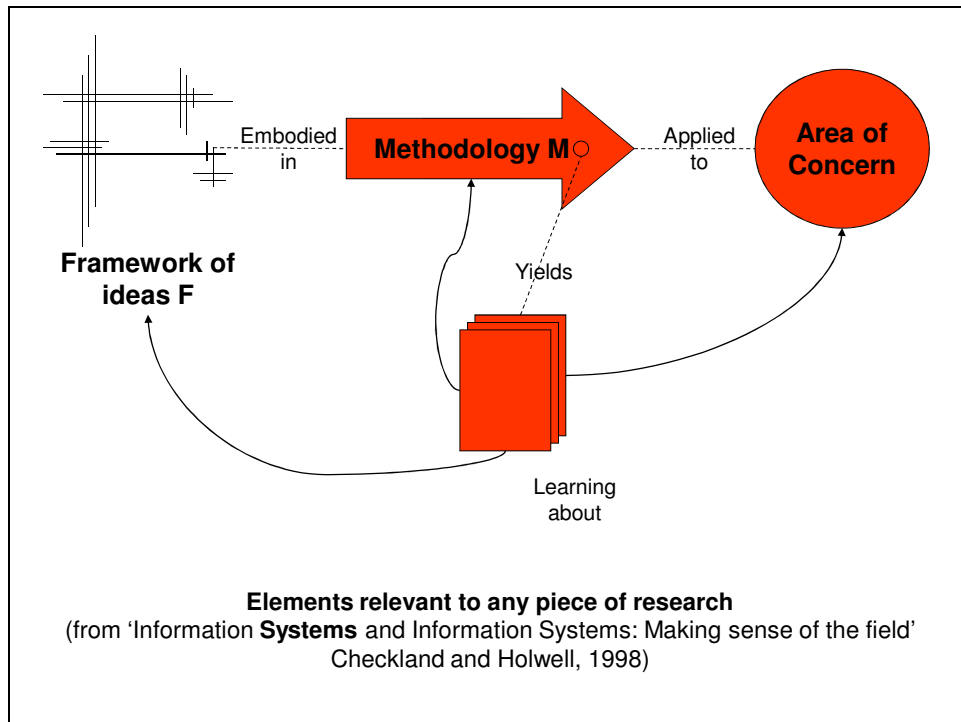


Figure 2: Elements relevant to any piece of research
 (Checkland and Holwell, 1998)

The projects each had methodologies varying from desk to action research that could be analysed to explore several different but complementary ends. These projects were:

- Alpha α : Top Ten IS/IT Risks - An analysis of surveys for the Small Business Service of the Department of Trade and Industry, February 2005
- Epsilon ϵ : Accredited UK General Segment – Developing a standard to manage the risk in the supply of ICT by small to medium sized ICT suppliers (2006).
- Work with BSI and the Local e-Government Standards Board
 - Beta β : Using Standards to Mitigate Risk in Information Systems: Project Brief, a response to: the work programme of Committee IST/15 Software Engineering in collaboration with BSI Publications (2004)
 - Zeta ζ : Local e-Government Standard Board: defining and piloting a Standards Development and Adoption Process (2005 – 2006)
- Gamma γ : Maintaining a catalogue of standards and best practice advice for effective information assurance, for the Central Sponsor for Information Assurance (2006 - 2007).
- Fieldwork (2006 – 2008) where standards were applied to mitigate information security risk in a housing association (Eta η), a construction company (Theta θ), and a firm offering financial services related to pensions (Iota ι).

- Delta δ : Are you now, or have you ever been, a vulnerability? – A project to investigate how to find the human vulnerabilities in network security and improve an organisation’s risk culture (2007).

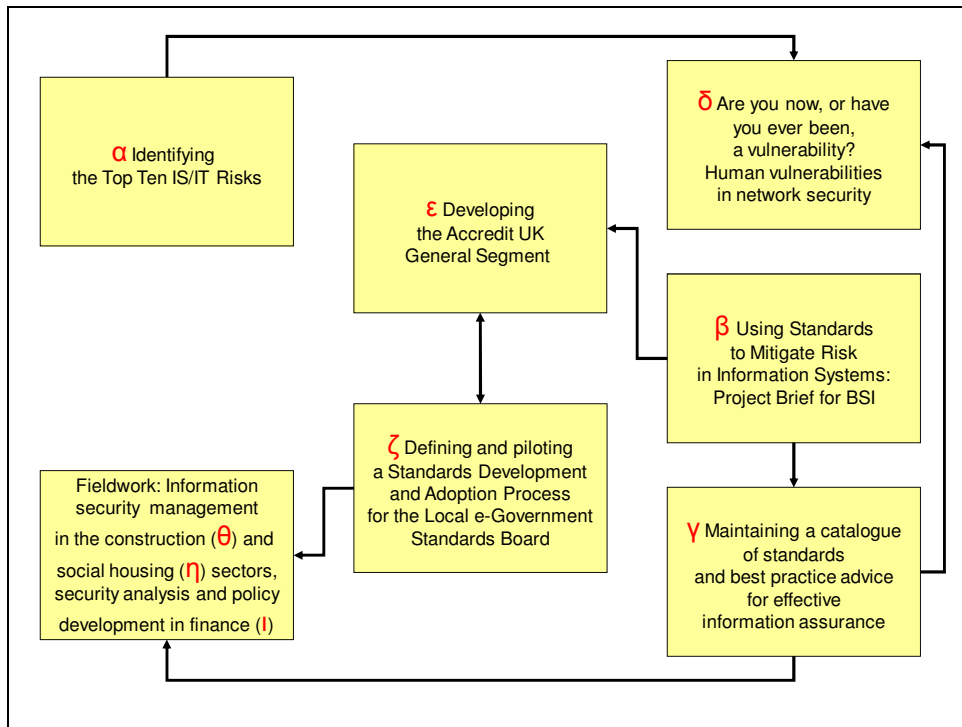


Figure 3: Desk research and case studies⁹

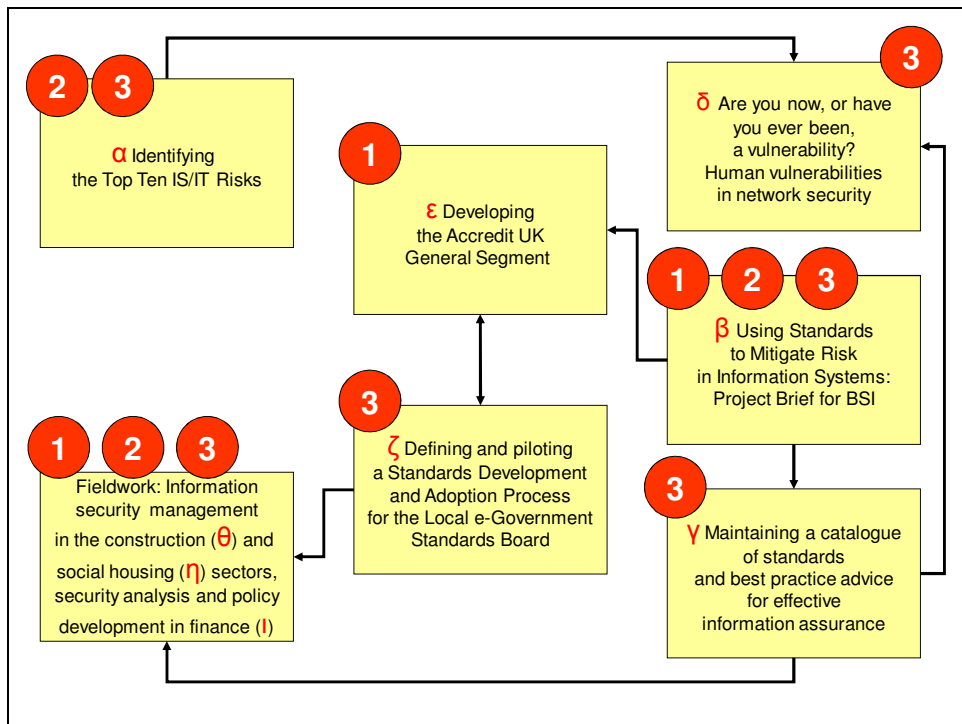


Figure 4: Relevance of the case studies to the three research questions

⁹ A table of projects is shown in Appendix A.

As there are many risks to information systems (Bundesamt für Sicherheit in der Informationstechnik, 2001) some selection was needed to focus the attention of the research. Responding to a call for the DTI¹⁰/SBS study (described in Chapter 3) gave the impetus to select a ‘top 10’. Top of this list were issues associated with human factors in information systems security and so a call for research from TSB/ESRC into the human vulnerabilities in network security gave the opportunity to investigate one specific area of risk and suggest that the framework of standards (catalogued in the project to compile a catalogue of publicly available risk treatments – particularly standards – for the Central Sponsor for Information Assurance) would provide the means to react to the findings of implementing the methodology that emerged (Figure 5).

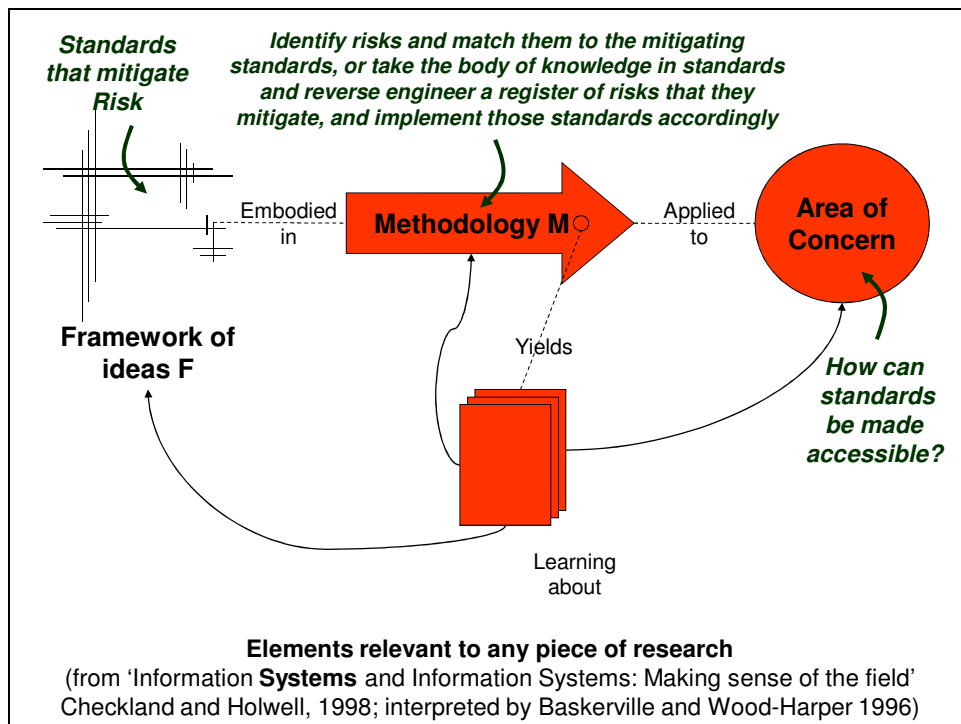


Figure 5: Checkland and Holwell's research construct as applied

¹⁰ The Department for Trade and Industry became the Department for Business Enterprise and Regulatory Reform (BERR) and then the Department for Business, Innovation and Skills (BIS). See the preliminary pages for a list of acronyms.

1.4 Personal motivation for this research

In this section I explain how the thesis makes use – but is not driven by – the results of studies that have taken place at The National Computing Centre during the period of research. I discuss how data from the studies has been used to (a) improve and (b) answer the research questions. I explain my interest in the 'human factor' of risk in information systems which emerged as the most perceived risk in a view of the top 10 risks to information systems (NCC, 2005).

I can trace back my continued motivation for learning to the final year (1984 – 5) of my undergraduate degree¹¹ when I was challenged to design a pragmatic method for white-light holography at Manchester Polytechnic. During the literature search and writing up the experiments, I postulated the opportunity to continue learning through written work as a career. This led me to discover the discipline of technical writing and the subsequent blessing of a graduate training position at Ferranti Computer Systems working on urban and motorway traffic control systems. When I moved from civil to military (training) systems within Ferranti, I first experienced the explicit, audited, application of standards to the technical publications, particularly as I became the principal author for software documentation and became involved in Ferranti's audit by the Ministry of Defence to the NATO information technology (IT) standards AQAP 1 and 13 (which were replacing Ferranti's benchmark to the previous UK military standard 05-21). The result of preparing for this audit made me aware of Deming's (applying Shewhart) practical quality process of plan-do-check-act (Deming, 1950) and the application of documented 'standards' as a tool to strive for predictable, successful outcomes. The expectations of what was needed to successfully use and maintain the systems we were building was described in standards that the documentation was expected to comply with, in order to meet contractual obligations and so receive the stage payments for the work that was tied to completion of the documentation. This interest in quality management become more focused after moving to The National Computing Centre (also as a technical author) and becoming a quality manager taking the organisation first through certification to ISO 9001 (the internationalised version of the original manufacturing standard BS 5750 Part 1 which itself was based on 05-21) for its activities in consultancy, training and education and subsequently – under the TickIT inspection framework – for software development. The national role of the Centre in promoting good practice for effective use of IT awarded me the opportunity not only to apply standards, engage with the Centre's members in advising on such application, but also to join some of the standards-setting committees of the British Standards Institution (BSI), namely for Software Engineering and the TickIT Certification Scheme. The TickIT Scheme,

¹¹ BSc (Hons) Combined Studies: Applied Physics and Computing Science. (Subidiary, Science, Technology and Society.)

although also concerned with good practice in software engineering, warranted its own steering committee giving some indication of the perceived bureaucracy and political distraction that is often the public face of standardisation (Backhouse, Hsu, and Silva, 2006).

My experience in technical writing spanned writing for two contrasting audiences: the technicians who would program the software (including programming described as 'maintenance' to correct defects that became apparent when the software was in use) and the end-users who would apply the software and who would have no need to understand how it worked to be able to fulfil the tasks the software was designed to do. In that second group – the users – the documentation presented on paper or on-line (perhaps as 'help') – became an integral part of the usability of the software. This led me to study human factors, particularly usability, more closely through the 'Usability Now!' programme of the Department of Trade and Industry that was run by The National Physical Laboratory. This programme was primarily concerned with the effective application of knowledge about human-computer interaction (HCI) and built on the outputs emerging from the European Esprit Methods for Usability in Computing (MUSIC) project (Bevan and Macleod, 1994). From this I learnt about the application of standards to manage risk in usability testing, making a presentation on the connection between usability testing and the ISO 9001 standard for quality systems (Dresner, 1992). From this I learnt about the application of standards to manage usability risk and the psychology of HCI (Dresner, 1996). My interests in human factors and risk management converged in this post-graduate research in a project to investigate the detection and treatment of human vulnerabilities in information systems (Chapter 4). The premise of that project was that if the vulnerability could be detected, standards – such as those catalogued for the Cabinet Office (Chapter 3) – could be used to treat the risk and reduce the vulnerability. The importance attending to the human factors in information system (security) risk management is shown by the survey of surveys described in Chapter 3 and encouraged the project – described in Chapter 4 – which made a significant contribution to answering the third research question: How do you link standards to the risks that may mitigate them?

Chapter 5 encapsulates my regular day-to-day activity which began rooted in challenging, relevant consultancy and continues under the rigorous mantle of research. This has all brought rich opportunities to see project and operational work at different stages. Engaging with the gamut of organisations and their information systems was providing a learning opportunity that was ripe for organising into a structure beyond the ad hoc chance of professional development. I saw the rewarding possibility of bringing much of my professional work into the structure of postgraduate, doctoral studies to enable me to consolidate the experience of 18 years in the work place and build it up – G-d willing – to enable me to both learn and teach for many more. This research apprenticeship has gladly changed me from a head to foxes to a tail to lions¹². Further growth is assured, not least by

¹² Rabbi Masya ben Charash, *Ethics of the Fathers*.

the possibilities documented in the final chapter (Chapter 6) which analyses the work done, the success of the methodologies employed, and sets out the research position (see 6.3) that I am entrenched in.

1.5 The design and structure of this thesis

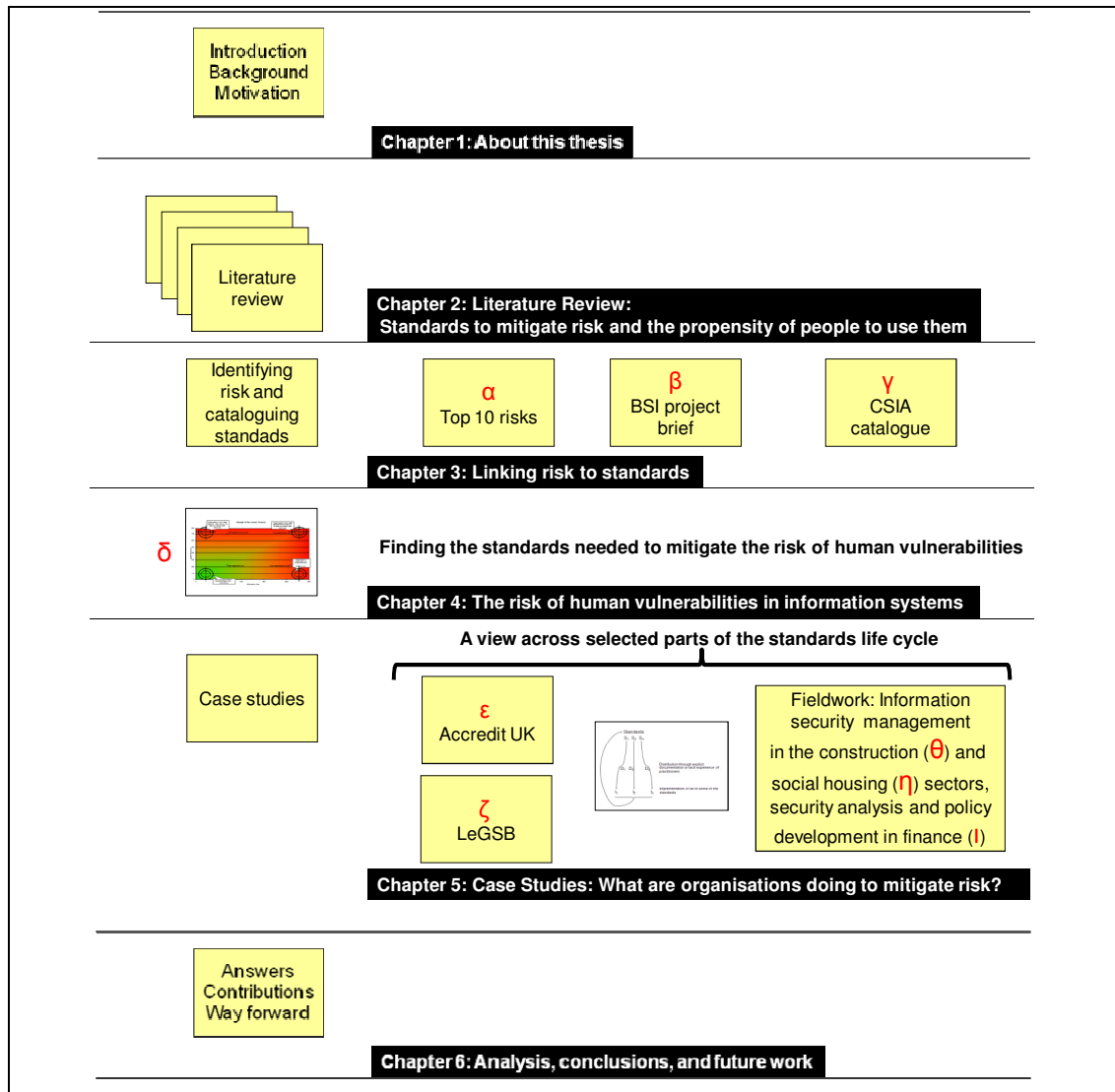


Figure 6: The design and structure of the thesis

This thesis is divided into six chapters. The first two chapters establish the background for the research and look at the complementary work that has been done in this discipline:

- **About this thesis** (this chapter) – about the research, the thesis, and the research questions. This chapter looks at the motivation for the research and how I went about learning how to learn again.
- **Literature review** – where I set out the main literature study with the arguments of both the academic literature that underly the rigour of the research, and the political and business literature that confirms the relevance of the research topic.

With the background and literature support for the research established in the first two chapters, the central three chapters discuss the purpose, methodology, and application of the respective methodologies for the research that was carried out. This comprised desk research which was commissioned by government and private bodies who concur with the basic premise of the thesis that standards mitigate risk, action research with private and quasi-governmental organisations to set standards and implement them within the life cycle of information systems, and the research and development of a method to test the exposure to risk of information systems from human vulnerabilities in relation to the expectations on implemented standards to mitigate such risks. These chapters comprise:

- **Linking risks to standards** – A chapter that describes the desk-based research to identify the core risks that threaten information systems and a catalogue of standards in a framework for risk treatment.
- **The risk of human vulnerabilities in information systems** – A chapter that describes the research and development of testing the effectiveness of what organisations are doing to manage risk by applying the standards identified by the desk-based research.
- **Case studies: what are organisations doing to manage risk?** – A chapter that describes action research to develop and set standards and to benchmark the application of some of the standards referenced in the desk-based research (from Chapter 3).
- **Analysis, conclusions and future work** – A chapter that analyses the research from desk and action research projects (the theoretical and practical work of chapters 3, 4, and 5), looks at the level of success in the research in demonstrating that standards mitigate risk, and discusses the tools and methods that are emerging that validate the approach and findings of the research.

Although the main literature review is contained in *Chapter 2*, relevant literature is brought into the discussions about the research projects in the respective chapters. For each project, I discuss the reasoning behind the selection of the research methodology for that project, the assessment of the results of that research, and the conclusions that may be drawn therefrom.

This page intentionally blank.

CHAPTER 2. A LITERATURE REVIEW

2.1 About this chapter

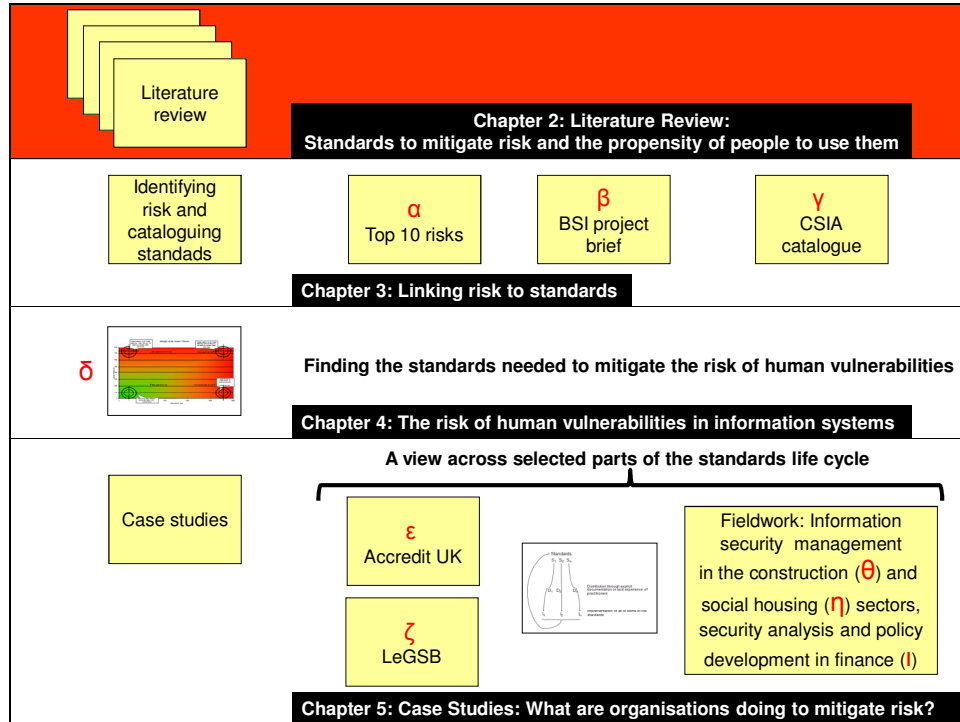


Figure 7: This chapter in the context of the thesis

This chapter introduces the theoretical basis for this research on the topic of risk, standards, and their importance in the management of information systems by reviewing and analysing the academic, practitioner, and governance literature in the disciplines of cybernetics, information security, knowledge management, standards, and risk. Academic, from the body of knowledge peer reviewed by academe, practitioner material – mostly in the form of industry reports and text books – and governance literature, mostly in the form of published standards. And this is significant for the research activity which comprised a complementary mix of ethnographic (see Chapters 3 and 4) and clinical (Schein, 1976) case studies (Chapter 5). Standards – particularly those published by national and international standards bodies (such as the International Standards Organisation or the British Standards Institution) or consortia (such as the World Wide Web Consortium W3C) – have a rigorous peer review system of their own that filters the wheat of experience from the chaff of speculation (see 2.13). The review of standards – which is discussed in this chapter – is at least as strong as the review of academic literature if not more so as the standards development process¹³, has an early phase of considering ‘new work items’ which may result in the rejection of any further research under the aegis of the standards bodies involved. Academic research may

¹³ See Table 5: Standards development processes

only be rejected by a wider audience when its author presents it for publication. Until then they will continue to embrace their favoured paradigm (Cawthron and Rowell, 1978). Figure 8 shows my relative consideration of material included in this literature review.

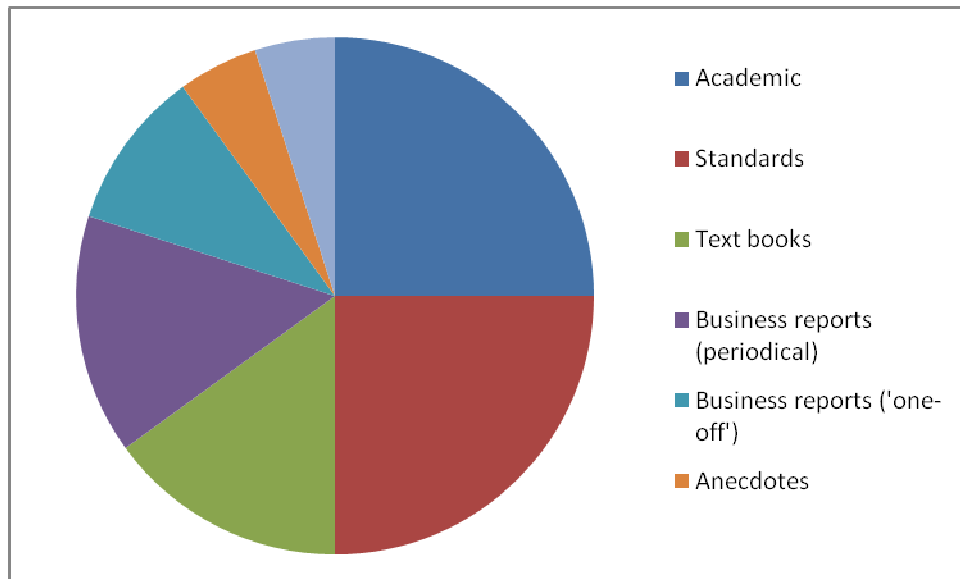


Figure 8: Literature and its relative strength – a personal view

There is insightful work on 'Standard Making' (of particular note is the special issue on the subject (MIS Quarterly Vol. 30, 2006) and critical work (Seddon, 1998 and Thomas, 1997) but a work on a causal link between risk and its mitigation by standards is hard to find. In this chapter, I consider the risks and the causes of risk to information systems (in advance of selecting a 'top 10' list in Chapter 3) whilst contemplating if risks and the causes of risk can be usefully separated, and discuss how the perception of risk affects the way that risk is managed, with an interest in where standards are applied to do so. My objective for this approach was to address the research question: *Do implemented standards mitigate risk?* I do not suggest that there is a simple relationship between a risk and a standard – one standard may mitigate one risk, part of a risk or require other standards to be applied with it¹⁴. Nor is the value of standards regarded universally, a problem which is discussed below after a consultation with standards users.

The original research plan to analyse whether standards are efficacious in the treatment of risk was founded on the assumption of seeking a consensus opinion that standards may be implemented to mitigate risk in information systems. This consensus view pervades the basis of the projects and case studies (*see Chapter 1*) that were carried out during the period of research and so I have presented this *literature review* as the formal recording that risk reduction techniques be linked to the reduction in risk with surety. The theme of this

¹⁴ As shown during the compilation of the catalogue of risk treatments for the Central Sponsor for Information Assurance (Chapter 3).

literature review is that where papers and reports recommend the uptake of standards¹⁵, they are making the general recommendation to espouse good practice for desirable outcomes rather than explicitly acknowledging the standards-risk relationship. Failed projects are treated as historical occurrences, not as the overt realisation of risk or risks.

This chapter has considered the evidence and support for the notion that the application of standards treats risk – that standards remove either the problem or part of the problem – with due caution of plucking simplicity out of complexity: models attenuate (Beer, 1993). The field of literature has been surveyed, tempered with the view of considering levels of mitigation rather than absolute resolution. The gap in the premise is discussed in the final chapter of this thesis, *Chapter 6 Analysis, conclusions, and future work*.

2.2 Why is the problem worthy of research?

It turns out that not only are there losses from undesirable outcomes (Swann, 2000) but that the uptake of standards to mitigate these losses is not endemic (BCS and RAE, 2004). However, the third report on standardisation for the National Strategic Standardisation Framework says that where standards are implemented, they contribute £2.5 billion to the UK economy (DTI, 2005). It would seem that a method to encourage the application of standards to information systems would highly advantageous; information systems could be immunised against avoidable losses. Customers, actors, and owners (Checkland, 1981) in the life cycle of information systems may be encouraged to ‘only make new mistakes’ (Dourado, 2007).

If losses are associated with the result of risk, a validated method for mitigating risk is likely to be welcomed. This may well comprise a method that could be clearly laid out and explained in a format that can be taken up by organisations of varying size and encourage them to use standards as a matter of course and benefit from the explicit knowledge therein in risk management programmes. This may result in more effective strategic planning as a result of increased knowledge and understanding of key risk exposures. There would be fewer costly surprises, because undesirable outcomes are prevented from occurring, programme sustainability results from effectiveness, efficiency, and greater openness and transparency in decision-making and the ongoing management processes. Projects that are more efficiently and effectively managed - where advisers and stakeholders understand their vulnerability to risk and take adequate preventative or mitigation measures – there is a greater likelihood of projects attaining their objectives because constraints are minimised and opportunities maximised. The desirable outcomes will have a greater likelihood of being sustainable. A methodology for applying the knowledge in standards as mitigation to risk will provide greater openness and transparency in project decision making and management

¹⁵ For example, DTI Economics Paper No. 12, *The Empirical Economics of Standards*, June 2005

processes. This contributes to improved governance (ISO/IEC 38500:2008) that can be in itself a development objective.

This research builds on preceding work that identifies standards as a solution to warding off undesirable outcomes (Swann, 2000) but does not offer the means by which practitioners may be encouraged to take up the advice in standards. This research proposes such a method. The soft systems method (Checkland and Holwell, 1998) highlights the importance of understanding the 'weltanschauung' or perspective of stakeholders in an information system. My research suggests that as 'risk is in the eye of the beholder' (Bernstein, 1998) it is a sufficiently important to deal with it in the context of stakeholders and so this research will be a useful addition to modelling systems from a soft viewpoint. It is also likely to benefit system life cycle modelling (ISO/IEC 15288:2008) and project management techniques and processes (BS 6079-3:2000). For example, the methodology developed in Chapter 4 – for the detection of human vulnerabilities in information systems – provides a decision support tool for selecting the balance of technology and process controls with end-user awareness during information systems design.

2.3 Attitudes to standards

Collated feedback collected during a consultation with 'Knowledge Networks' of interested parties comprising National Computing Centre members¹⁶ showed concern about the accessibility of standards – and the processes used to develop them. It is relevant to this research because it shows how the emerging risk treatment framework can itself mitigate some of these concerns. The consultation took place December 2003 to January 2004. It is included here because issues raised by the respondents have some of their solutions based in the risk treatment framework proposed in this thesis, namely: overcoming the perceived complexity of too many standards through to navigation based on stakeholder views of risk; the approach to risk treatment using standards is agnostic of the source of the standard and picks out the risk treatment regardless of the publisher of that standard; the 'standards treat risk' paradigm increases risk awareness in the utility of standard to reduce the failures that have given concern over the performance of organisations who have been certificated to standards; linking risk and treatment by standard will not make standards cheaper to procure from publishing organisations but it can be used to direct users to very specific standards that will offer them value for money through the treatment of otherwise expensive risks.

¹⁶Contributors: Senior Performance Test Analyst, Operational Acceptance Test Services, Service Introduction and Planning, Group Technology, HBOS plc; Chief Executive Emeritus of The National Computing Centre, IT Manager from a large North East of England Law Firm, Parliamentary Lobbyist on Information Technology issues, Project Officer from the Information Security Policy Group of the Department of Trade and Industry.

The complexity of standards is a result of the need to try to include not only the intended scope of implementing a technology or process, but also predict the effect of unintentional applications. This results in the perception of much of the information in standards as being preventive and therefore negative. Successful standards are seen to be simple or minimalist, with the emphasis on communication rather than 'prevention'. Although it is undoubtedly important that the impact of proposed changes are understood, it is more important that the need for the change is recognised and accepted by all stakeholders. Leadership and teamwork were cited as the framework for successful projects; standards provide a communications medium within that framework. The source of standardisation was also noted by participants as an area of confusion, with many contributors to the body of knowledge of IT standardisation. One respondent to the survey cited, as examples, ECMA, ITU, BSI, and ISO. Another respondent referred to the declaration of certain suppliers as being the owners of standards, whereas they may have been more successful in penetrating the market place with a particular technology. References were made to the oft quoted remark by Professor Andrew S. Tanenbaum in *Computer Networks*, Prentice-Hall, Inc., (first published in 1980) which describes the International Standards Organisation Open Systems Interconnection model¹⁷:

'The nice thing about standards is that there are so many of them to choose from'

referring to the proliferation of standards, and *The Matelot's Prayer*¹⁸, that says:

'Let's drink to our wives, wonderful wives, bane of our lives; And if we have one wife may we also have ten.'

This intimates a love-hate relationship with standards whose proliferation is not differentiated by quality. The development process in which standards are formulated, reviewed, agreed, and then published was deemed to take too long, have too many roles involved, and be too concerned with synthesising a product that satisfies all view points. The problems were specifically reported as: time-consuming – the derivation of standards from series of meetings, will normally take place over a period of years, whereas market changes and business opportunities seem to be more immediate, and bureaucratic – the layers of committees and standards bodies mean that it is very difficult to navigate how a standard is progressing or have access to the latest thinking until a consensus is reached. The effort to gain a consensus agreement is time consuming and can lead to the omission of useful information that, having been removed during editing, is not circulated to the wider standards audience¹⁹.

¹⁷ Professor of Computer Science, Department of Computer Science, University of Amsterdam

¹⁸ 20th Century Royal Navy song

¹⁹ An example being in the development of ISO/IEC 9421 for graphical user interfaces. A draft of this standard contained a conceptual model describing the relationship between the representation of information in the machine, the representation of that information graphically on screen, and the

Whereas kite marking²⁰ of certain products such as glass, hot-water bottles, and tyres commands a certain degree of respect in the relevant market places, compliance with information system standards – particularly process standards – does not command similar respect where standards are expected to deliver a degree of assurance on the part of the supplier. This may be the result of the contrast between product and process standards. The perceived (at least) effectiveness of information technology and systems usually depends on the compliance of their suppliers to standards for organisational process²¹. Compliance was also seen as difficult as there seems to be limited understanding that there is more than just simple pass-fail tests to be applied, particular in a complex IT-based information system.

The NCC study reported that would-be standards followers saw the cover price of standards as prohibitive, particularly to small businesses, who see the full cost in terms of 'cash flow' rather than the benefits that accrue from the implementation of the standard, possibly on many occasions, spreading the cost over more than one project.

This research looks to mitigate many of these perceived flaws by making the information in standards that is directly relevant to operational issues accessible and more obvious. This may be accomplished by using a taxonomy-centric framework that avoids adding any layers of complexity to the standards. However, the changes to time-consuming, bureaucratic and overly 'political' standards development process are outside the scope of such a framework.

2.4 What is risk?

Although most definitions of risk tend to be mainly concerned with harm, loss, or danger²², the risk management process is increasingly recognized as being concerned with both the positive as well as the negative aspects of uncertainties (PD ISO/IEC Guide 73:2002; DEFRAS, 2002; ALARM, 2001; Hillson and Murray-Webster, 2007). Similarly if risk is viewed in terms of its outcomes, such as losses and gains, then the definitions do little to separate hazards²³, or the causes of risks, from the actual 'loss/gain' resulting from the risks

cognitive understanding of the symbolism on screen. The diagram and explanatory text was removed in favour of a document merely listing the screen icons and their meaning so removing any appreciation of the decision making process for standardising an icon and the subsequent improved commitment to memory of an understood semiotic.

²⁰ A trademark of the British Standards Institution and not applicable to any other quality marque.

²¹ Such as ISO 9001 for quality, ISO/IEC 20000 for IT service management, or ISO/IEC 27001 for information security.

²² Houghton Mifflin American Heritage Dictionary

²³ Hazard is an event or situation which can cause harm (including ill health and injury; damage to property, plant, products or the environment; production or financial losses, increased liabilities, etc.). ALARM – the forum for risk management in the public sector *A key to success - a guide to understanding and managing risk* February 2001

themselves. The concept of risk as an 'undesirable outcome' (Swann, 2000) can, however, still be a useful focus. A review of risk registers (which are discussed later) supports the assertion that there is usually poor differentiation between risk (as the outcome – the loss) and the cause(s) of the risk. Risk may be defined, therefore, as a catch-all term pertaining to the possibility of loss, the loss itself, or any characteristic, object or action that is associated with that possibility (Kontio, 1998). The subject of risk management is now associated with good governance across corporate governance in all disciplines (PD 6668: 2001).

The idea of risk appears to have been coined first by 16th and 17th Western explorers and the word 'risk' seems to have come into English through Spanish or Portuguese where it was used to refer to sailing into uncharted waters. Thus it had an orientation to space, eventually being transferred to time as used in banking and investment, in order to include the calculation of the probable consequences of investment decisions before referring to a wider range of other situations of uncertainty. It gradually became clear, therefore, that there is no risk where an outcome is 100% certain (Giddens, 1999).

The Basel Committee for Banking Supervision (the self-regulating body for banking²⁴) defines operational risk as:

- 'the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events' (Harris, 2002)

and this definition was adopted widely in banking (The Federal Reserve Bank of San Francisco, 2002). The challenge, however, is how to model external events of processes, people and systems with a view to controlling them and to avoid undesirable outcomes and so achieve positive results. Without effective and repeatable risk identification methods, truly effective risk management is impossible (Carr, Konda, et al., 2003). It therefore follows that a course of action is required to deal with the identified risks and to have them accepted by the respective, authoritative stakeholders.

Other approaches model generic risk as a combination of consequence or impact and likelihood or probability. (PD ISO/IEC Guide 73:2002; Defense Contract Management Command, 1999; Financial Services Authority, 2003; Australian Agency for International

²⁴ The Basel Committee was established at the end of 1974 and comprises members from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, United Kingdom and United States. Countries are represented by their central bank and also by the authority with formal responsibility for the prudential supervision of banking business where this is not the central bank.

The Committee formulates broad supervisory standards and guidelines and recommends statements of best practice in the expectation that individual authorities will take steps to implement them through detailed arrangements – statutory or otherwise - which are best suited to their own national systems. (www.bis.org) The 'banking crisis' of first decade of the 21st century suggests a lack of enforcement of the standards and guidelines.

Development; IEEE Std 16085:2003; PD 6668: 2001) and these approaches can be seen as being bounded by the project envelope (BS IEC 62198, 2001) of cost, schedule, quality, or technical constraints (US Office of the Under Secretary of Defense, 2004). This is shown in *Figure 9* where the area within the cloud outline represents the boundary within which the project resources and attributes should be contained to achieve the desirable outcomes. Desirable outcomes suggest that risk is managed. Resources are applied directly to mitigating the security risks associated with information systems (ENISA, 2006). Even so, contingencies to make the outcomes more or less satisfactory are typically built into project plans and there are at least 16 methods of risk assessment (BS 6079-3:2000) although the emphasis seems to be on opening up the issues rather than matching them with a method of treatment.

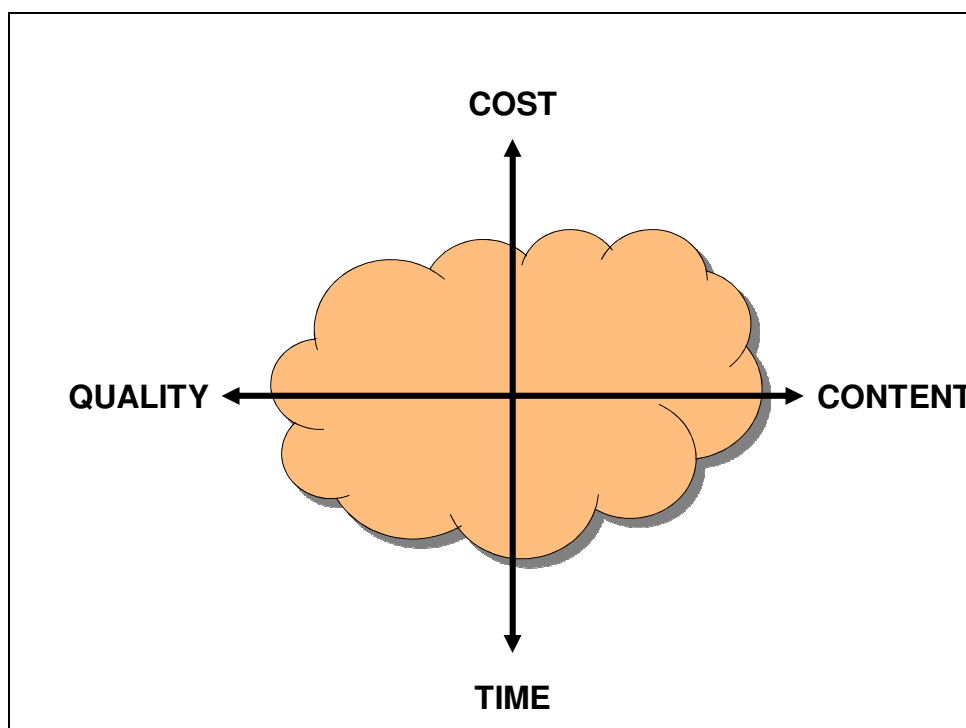


Figure 9: The project envelope

Risks are associated with one or more certain or uncertain events (a single occurrence or a series of occurrences of a particular set of circumstances) which have a likelihood or probability, that is, an extent to which an event is likely to occur. The impact of the event may be judged by whether the risk is 'uncertainty that matters' (Hillson and Murray-Webster, 2007). Events have consequences (outcomes) that can range from the positive to the negative and there can be more than one consequence from one event. However, consequences are always negative for safety aspects and consequences can be expressed qualitatively or quantitatively (PD ISO/IEC Guide 73:2002). Information assurance processes need to have structure (BS 7799-2:2002) to see that good governance (Turnbull, 1999) of programmes of projects put in place at board level can be carried through to the management of risk and, hence business continuity of information systems.

2.5 Risk management models

The contemporary focus on maturity models²⁵ may be used to contrast two extreme approaches to risk management (*Figure 10*). In a mature process there is adequate planning included as a key stage of a recognised life cycle of predictable activities to realise the project's aspirations. Project management should recognise a clear taxonomy (Pickford, J. (Ed.), 2001) of the risks which may affect the successful, efficient conclusion of the project as well as developing a feedback loop that will collect the lessons learnt from the emergent risks that were either unforeseen or thought to be less significant. A risk management accreditation documentation set is expected to be kept up to date for UK public sector information systems (NISCC/CESG, 2005) and a risk and issues log is expected as good practice, on projects concerned with the development and delivery of information systems and associated services (BS 6079-3:2000).

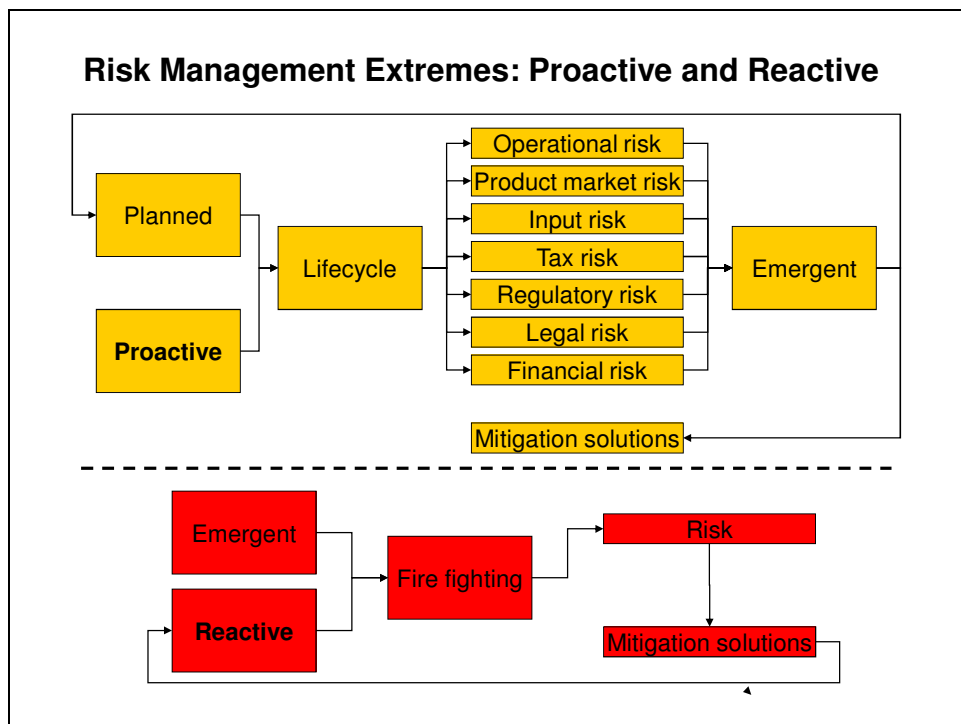


Figure 10: Risk management extremes

Lessons learnt in projects are important. As an example, in order to come to the conclusions of acceptable risk in terms of watertight bulkheads, lifeboats, crew drills etc., the imagination of the Titanic's designers was not constrained by the later tragedy because no one had been able to imagine such a disaster on that scale before (Kuntz, 1998): Now that the events of history are knowledge, later shipbuilders can prepare to mitigate the causes of a 'Titanic'-like

²⁵ Particularly the Carnegie Mellon University *Software Engineering Institute Capability Maturity Model*, and the International Standards Organisation's process assessment model *ISO/IEC 15504 Process Assessment*, and in 2010, the development of a *Common Assurance Maturity Model (CAMM)* and an *Information Assurance Model for SMEs (IASME)*.

disaster. This concept of having an individual view point has a significant impact on attitude to risk and this point will be discussed later in this chapter where the idea of 'weltanschauung' is analysed.

The process in the lower section of Figure 10 shows that operating reactively to risks which emerge creates not a feedback loop, but rather a cycle of always dealing with risks as they emerge 'on the fly'. This is the approach of small organisations²⁶ (also Lacey and James, 2010).

The classic maturity model (Crosby, 1979) that resonates with auditors has five states (viewed here from a security perspective):

²⁶ As reported at consultation meeting for small businesses held at the Computer Software and Services Association (CSSA – now Intellect) in December 1999. A software process assessment scheme was proposed by the Department of Trade and Industry (DTI). Small software development companies were invited to comment on the proposal which comprised an on-line assessment based on the Carnegie Mellon University Software Engineering Institute Capability Maturity Model. The consensus opinion was that small businesses may aspire to good quality practices but are usually focused on a particular customer's problem, the need to deliver information to the accountant, or meet the bank manager for additional investment. The programme that emerged from the DTI proposal is Towards Software Excellence (TSE).

Table 1: The classic maturity model		
Level	Label	State of the organisation
1	Initial or Ad Hoc	When the organisation works on a project by project basis. From a security point of view, policies are rarely seen and at best were cut and pasted from elsewhere. Corporate security is in the hand of the employee; audit trails are at best contrived, at worst there is no evidence of any good practice.
2	Repeatable	When stakeholders occasionally get involved to articulate what would otherwise have been an unknowable risk. The good news is that the risk treatments get embedded in the business and can be carried out over and over again. This is usually the time when an ISO management standard sticks its head over the parapet and raises the organisation to 'Level 2½' in conflict with the quantum nature of maturity modelling. The standard-build PC or other technology-led security policies are typical and pragmatic examples.
3	Defined	Where policies are not only becoming better tailored to the organisation's needs, risk management is becoming a better balance of people, process and some automated technology. Return on investment can start to show in audit costs settling down. There will be enough connecting controls and security governance to make automation worthwhile.
4	Managed	The level that can only be achieved through measurement. Measuring security is a contemporary challenge; the search is on for meaningful, leading metrics for information security. Reports of 'how few laptops have been lost this year' are unlikely to instil confidence.
5	Optimised	The organisation is 'self healing'. Events and incidents are as predictable as can hope for. When they occur, the state of forensic readiness feeds the dashboards of management information, decisions are supported, improvements made, threats are held at bay.

2.6 What is a standard?

This section of my literature review looks at complementary or competing organisations who declare standards and concludes that a 'respectable' standard is the product of a refinement process which may be empirical, by consensus, or by a combination of both. An organisation or individual with the wherewithal to make their views known may declare their way of doing things as 'standard'. The corollary may be the emergence of a 'standard' way of doing things – such as a ubiquitous computer operating system – without intention of it becoming standard in the sense of a formal, published, peer-reviewed specification but rather with the (usually) commercial aim of making something the most popular. Therefore, as well as the corpus of work that may be referred to unchallenged as standards – such as those from the British Standards Institution – may find itself alongside other corpii or single pieces of work that originate from sources with apparently less rigid governance. It is unusual to find work to assess the accuracy of a standard except in cases where there is a challenge to the standard's *modus operandi* (Seddon, 1998; Lacey, 2008) but there is limited debate about whether a product or process should be declared as standard and who is authorised to make such a declaration.

Standards have different connotations²⁷. Standards, which can be seen as useful when a plug fits a socket, worry some innovators with perceived threats of constraint or rigidity (Knight, 2005; Schultze and Stabell, 2004). This may be the inherent danger in the transfer of knowledge. The accessibility of standards may be inhibited by the loss of idiosyncrasy during the conversion of tacit²⁸ to explicit²⁹ knowledge (Figure 11). Practitioners may benefit from the successful channelling of emotions stimulated by risk to internalise the explicit knowledge of standards back to tacit realisation. Explicit knowledge 'can be expressed in words and numbers, and easily communicated and shared in the form of hard data, scientific formulae, codified procedures, or universal principles'(Nonaka and Hirotaka, 1995). Would-be standards users find it difficult to understand that the availability of many standards (Tanenbaum, 1980) is part of the refinement process that they crave³⁰. Too little knowledge

²⁷ NCC Knowledge Network Consultation, December/January 2003/2004.

²⁸ Tacit knowledge is 'knowledge that is nonverbalized, or even nonverbalizable, intuitive, unarticulated' (Hedlund, G. (1994). *A model of knowledge management and the N-Form Corporation*. Strategic Management Journal, 15, 73–90.).

²⁹ Explicit knowledge is 'formal and systematic' (Nonaka, Ikujiro, and Hirotaka Takeuchi. 1995. *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*, New York, NY: Oxford University Press)

³⁰ NCC Knowledge Network Consultation, December/January 2003/2004.

gathering leads to inefficiencies, where as too much results in rigidity³¹. To satisfy the need for knowledge in the short term, the message – like risk management – is to dredge first, hedge later (Banfield, 2001).

Where trust is put in standards, the level of confidence or acceptable level of risk is more tangible. Knowledge management scholars (Schultze and Stabell, 2004) quote Mark Twain, 'All you need in life is ignorance and confidence'. The question that needs to be asked is how much ignorance is acceptable? This may be answered by the observation that risks can be known – if not explicitly as risks, at least as concerns by at least one person, unknown – in so far as they could be found with the appropriate *weltanschauung*, or unknowable – the truly emergent risks that no one could reasonably foresee (Carr, Konda, et al., 2003). Presumably only the unknowable aspect – the unpredictable risk that will emerge in future – of the spectrum of ignorance is acceptable in judgements of an organisation's ignorance.

Perhaps the reticence by many to comply with standards is based on the potentially vicious – rather than virtuous – circle that can develop (Garud and Kumaraswamy, 2005) through the process of capturing knowledge in standards. The process of capturing the knowledge in standards produces, not support, but 'information overload'. Excessive emphasis on the capture and codification of tacit knowledge to create explicit standards can be seen to trivialise the knowledge, particularly when compliance with standards becomes the *raison d'être*, a 'tick' on the compliance checklist rather than the successful conclusion that the tick represents. There is a popular perception that third-party certification of compliance to standards has more advantages in marketing than in the maturing of processes. Certification is attractive therefore for those seeking either competitive advantage or where no certification is a barrier of entry into the market place. Those who do not have faith in the conversion of the tacit to the explicit see sustainability of competitive advantage through resources which are idiosyncratic (and therefore scarce), and not easily transferable or replicable (Grant, 1991)³². The accessibility of standards is therefore inhibited by the loss of idiosyncrasy during the conversion from tacit to explicit. Emotions associated with attention to risk create the spark of idiosyncrasy to convert that knowledge back from explicit to tacit, and so make standards accessible – appreciation of the risk encourage espousing the previously shunned standard (Vara, 2007)³³.

³¹ Ulrike Schultze and Charles Stabell, *Knowing what you don't know? Discourses and contradictions in Knowledge Management Research*, Journal of Management Studies, 2004, quoting Leonard-Barton, 1992; Levinthal and March, 1993; March, 1991)

³² Ulrike Schultze and Charles Stabell, *Knowing what you don't know? Discourses and contradictions in Knowledge Management Research*, Journal of Management Studies, 2004 quoting Grant, R. M. (1991). *The resource-based theory of competitive advantage: implications for strategy formulation*, California Management Review, 33, 3, 114–35.

³³ This article explains how to by-pass risk treatments but explains the dangers of doing so and as a result reinforces why the risk treatments should not be bypassed.

BSI sees a number of drivers to standardise which are tested according to the outcome of any project to develop standards. These drivers create the context – the energy, quality and place or Japanese *ba* (Nonaka, Toyama, and Konno, 2000) within which knowledge is created. *Ba* is the catalyst that drives the knowledge into codified standards and back to the tacit knowledge of those who implement them (Figure 11).

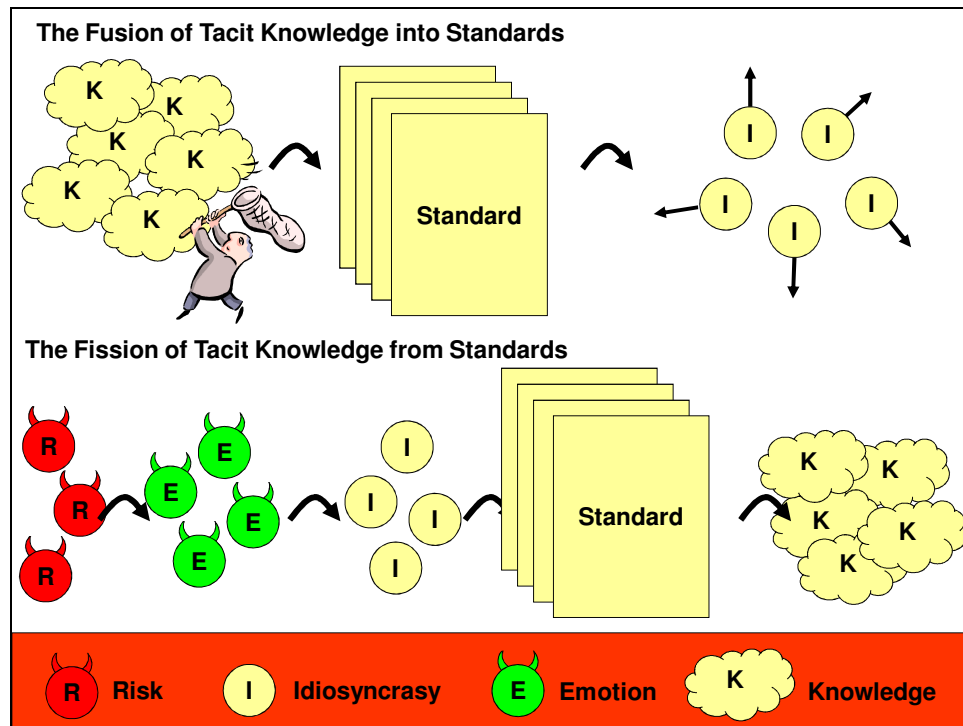


Figure 11: Risk stirs Emotion which promotes Idiosyncrasy that releases the Knowledge from standards

Codification of knowledge reduces the attention to that knowledge whilst those in need of it have to relearn what others have found out by experience.

2.7 The Toynee conflict

The application of standards to mitigate risk is implied in Stafford Beer's work on cybernetics (Beer, 1993) and arguably from the negative reaction to standards in Toynee's historical commentaries (Toynee, 1949). Toynee contends that standards become a risk in themselves because a society that applies them will stagnate and lose innovation. However, this conflicts with Toynee's view that to achieve a positive future, a society must keep the scenario it wants to achieve in view and work unerringly towards that vision. Toynee may not have appreciated that standards hold the lessons learnt about what may prevent the realisation of that future as well as providing key actions to shape it. The knowledge in standards may be applied to avoid mistakes – to be positively risk averse in known areas – allowing for innovation to springboard from those known areas into areas of emerging risk. Toynee may be echoing the concerns of cybernetics (Ashby, 1957) that regards centralised

control as a (negative) risk to innovation. This could indeed see 'stagnation' if it were not for the observation that standards developed with a consensus or central dictat tend to have localised implementation. This facilitates the management of known risks yet allows for Ashby's requisite variety by removing the cybernetic flaw of centralisation.

My postulation that standards mitigate negative risk, and their implementation as a realisation of the positive risk of success, builds on this work in cybernetics. Beer suggests that Ashby's *variety* is a measure of complexity and highlights the risk of modelling as a 'variety attenuator'. However, the model of actions to be taken, or measurements to be achieved that are encapsulated in standards are strong rules which are set to avoid the degradation of the activities that a project or operational plan – as the model of a set of activities to achieve a defined or implied goal – may suffer. This may be evident in attitudes as to what constitutes the core activities to achieve the goal: the *weltanschauung* relevant to the model's purpose. Contemporary interest in business continuity is promoted not by the general expectation of having to counter day-to-day risk, but rather the apocalyptic risks of floods (such as those in Hull and Sheffield in 2007), pandemics (such as the worry of the H5N1 or bird flu in 2007), or man-made catastrophe (such as the explosion at the Buncefield oil depot in 2005). Business models and business continuity models conflict because business continuity requires a business model to expand to deal with events and incidents that do not make a positive contribution to the achievement of business goals.³⁴ Business continuity is a security model – protecting the confidentiality, integrity, and *availability* of information systems from risks faced.

Similarly, the security controls which manifest in the safeguards to realise business or service objectives may be viewed negatively as optional extras to a business plan. Security controls are the implementation of security policies which manage risk to a state where risk is reduced to a level that is acceptable to stakeholders³⁵. So this acceptable level of risk may be measured as the appetite for risk which is in turn apparent in the actual implementation of security policies. These policies are evident as Beers' regulators (Beer, 1993), shaping and guiding activity along a path in the belief that the desired goal will be achieved. The policies become the standards that must be worked towards to achieve the desired goal and so in a social hierarchy, laws may be regarded as standards designed to reduce risks to acceptable

³⁴ Information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant. An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. (PD ISO/IEC TR 18044:2004)

³⁵ Which is why defined, applied, and audited policies are used as an indicator for risk appetite on the human vulnerabilities chart that emerged as the practical application of the research project described in Chapter 4.

levels. Security risks are also recognised as manageable but not necessarily eliminable. Meta-standardisation – the collation of a set of standards as a standard in itself – provides the framework to manage risks that are realised as security events or incidents (PD ISO/IEC TR 18044:2004)³⁶. The comparison of an organisation’s security policies against the consensus view of standards which show what policies *should* be in place present a measure of the organisation’s appetite for risk (The Technology Strategy Board, 2007). The fewer measures in place – as defined by the policies – the greater the appetite for risk (See Chapter 5). Thus, in an attenuating model of an information system (see Figure 12), regulators are standards – shown by the tall rectangles – shaping the project envelope which may encapsulate either the development or the operation of an information system that is threatened by risk – shown by the small squares that threaten to misshape the encapsulating area..

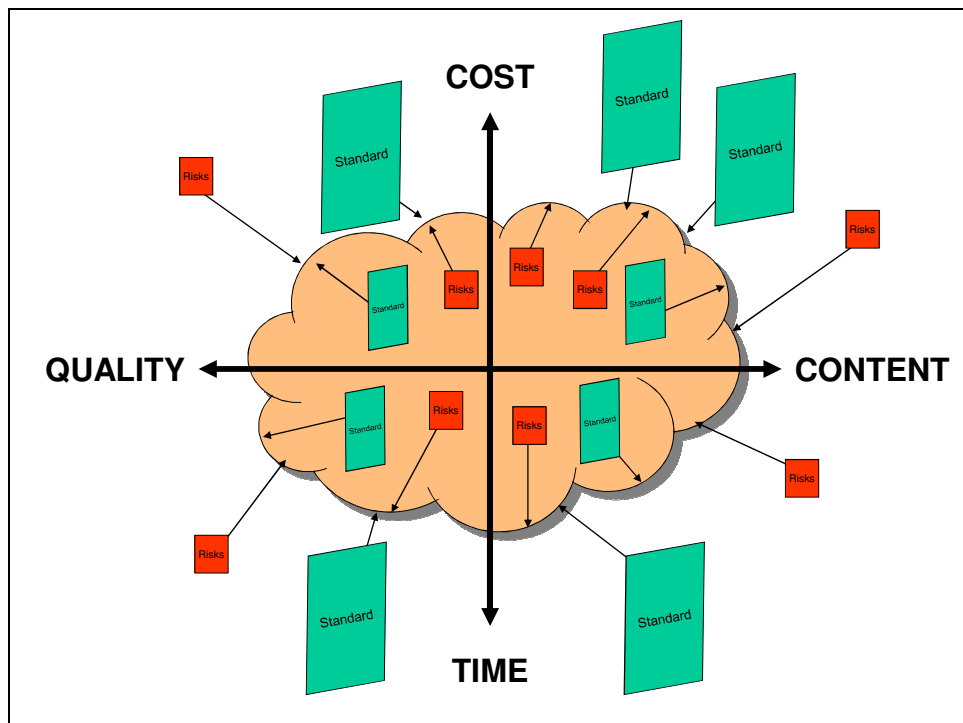


Figure 12: Project envelope affected by risk and regulated by mitigating standards

³⁶ See the cataloguing of standards carried out for the Central Sponsor for Information Assurance in Chapter 3.

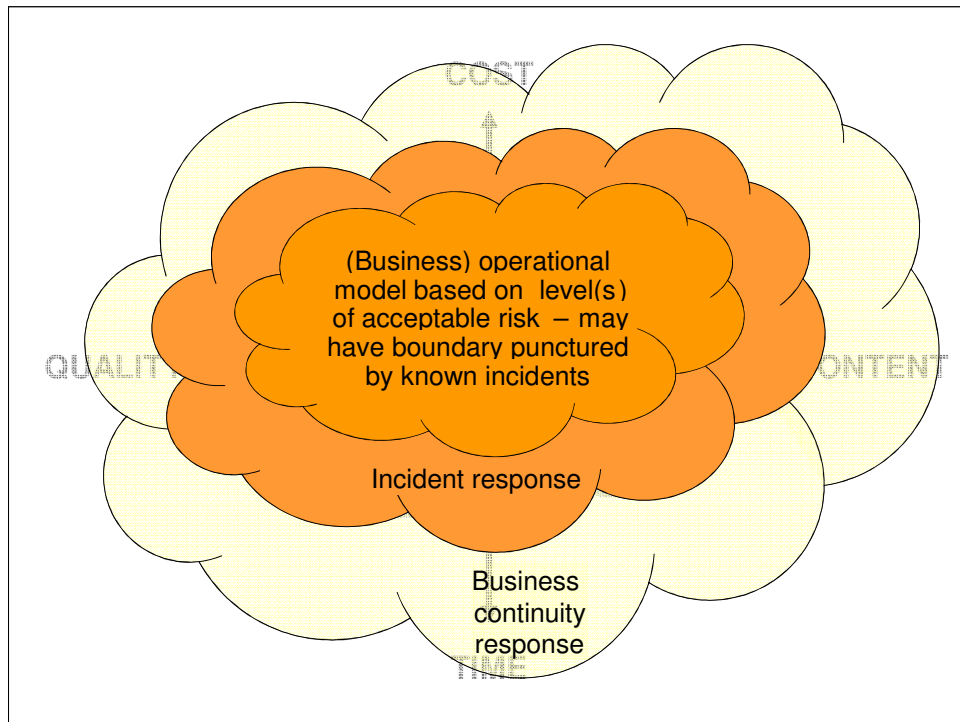


Figure 13: Layers of risk and a taxonomy of response

The discipline or process of incident response (Figure 13) when risks are realised is designed to contain risk within the levels acceptable to the information system's stakeholders. If the response to an incident exceeds expected levels then the regulating policies may need to be adjusted in the realisation of 'plan-do-check-act' (Deming, 1950) life cycle. Differences in otherwise standard practice(s) are the cybernetic regulators of the autonomous components of a cohesive system so standard(s) protect the requisite variety by allowing centralised practice to be adapted by the autonomous components. The feedback of experience³⁷, may make standards the regulating attenuators and amplifiers that lead upwards from each variable component of the 'system' to a central collator such as a government department or standards body. The experience from applying the standards feeds back to be the attenuators and amplifiers to create benchmarks that can be adapted by each autonomous component preserving the requisite variety (Figure 14). Therefore standards, used thus, are a tool for cybernetic success. Standards that aim for uniformity (that is without variety and adaptation) would otherwise lead to Toynbee's assertion that standards lead to uniformity and stagnation through insufficient variation. However it would seem that standards enable variation without chaos arising in an otherwise closed system; the information system is reopened by local changes. Standards are not a tool for central control (and subsequent failure of the 'system'). They facilitate the prerequisite of viability that a system should develop maximum autonomy in its parts according to the law of inter-recursive cohesion (Beer 1993).

³⁷ Through – for example – a Warning Action and Reporting Point (WARP, www.cpni.gov.uk)

The commonality in the standards – when applied to information systems – can create a cohesive whole of integrity with distinguishable parts. Information systems that apply standards procure variety equivalence and therefore requisite variety (Ashby, 1957³⁸) particularly through localising the applied standards (Figure 14). These information systems still retain identity (as in Beer's 'total system identity'³⁹) and feedback lessons learnt to create new standards (plan...capture knowledge in a standard; do...carry out the instructions of a standards; check...the results are desirable; act...on the outcomes of the implementation to improve the standard – Deming, 1950). Improvements may come from the diversity in decision-making (Coles-Kemp, 2008) and are captured in single and double-loop learning (Argyris and Schön, 1974).

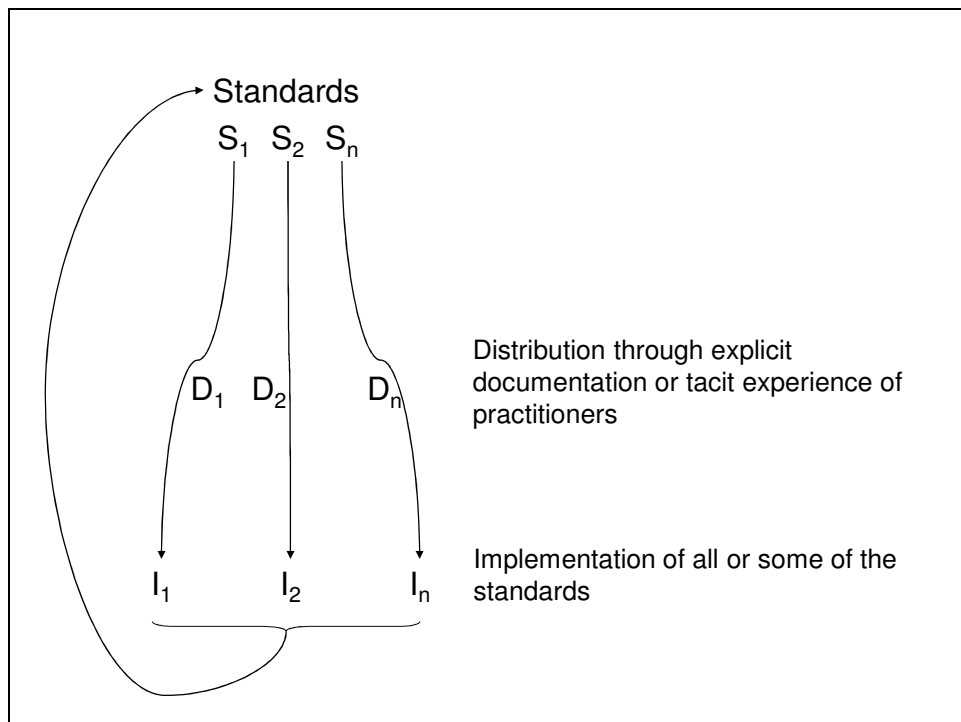


Figure 14: Standards are localised and lessons learnt are centralised

I have termed this 'The Toynbee Conflict' – the contradiction that if standards create uniformity and stagnation, therefore reducing variety, so that (in tune with Ashby and Beer) they lead to systemic failure of society, civilisations need to grasp their image of the future positive in order to achieve it. This aspirational view of the future positive becomes a standard to achieve. This highlights both good standards and bad standards or rather the good and bad implementation of standards. Standards provide guidance to counteract the potential chaos of requisite variety (Figure 15).

³⁸ 'nothing can be achieved by organisations [information systems] that are cybernetically flawed' (Beer, 1993)

³⁹ That is, when does it stop being a system?

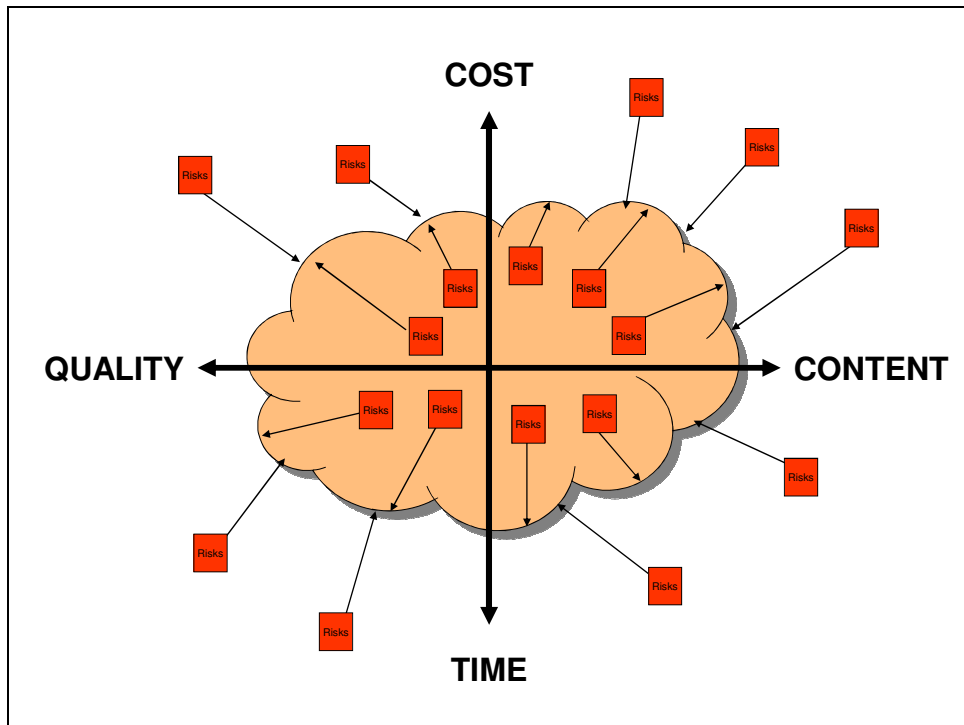


Figure 15: Risk threatens the desired shape of the Project Envelope

2.8 Approaches or responses to risk mitigation: a taxonomy

Table 2 catalogues different approaches to managing risks identified during a risk assessment. They are presented here to contrast each approach with another and to highlight where the hypothesis on which this thesis is based fits.

Table 2: Approaches to risk mitigation	
Approach	Significance
Accept the risk	Unless the chance of a risk can be reduced to zero, there must be some level of acceptance. This will be a combination of the likelihood of occurrence and the impact. In such circumstances, monitoring is the key response once the level of acceptable risk is decided.
Avoid risk	If the level of risk is deemed unacceptable or the means to control it exceeds the desired cost-benefit calculation, the risk may be avoided by not engaging in the activity which could realise it. This may impair the ability of an organisation to achieve certain goals.
Reduce likelihood of the risk occurring	This involves putting controls in place which may vary from design processes to close monitoring for any early warning signals. Both are likely to require educational effort. This preventive approach underpins the methodology of this research project.
Impact mitigation	When there is a high chance of a risk occurring and it is not viable to remove the actions and avoid the risk, the next best thing is to reduce its consequences say, through disaster recovery planning ⁴⁰ .
Transfer (allocate) treatment of the risk ⁴¹	Responsibility for treating risk can be allocated to parties best able to manage it. This transfer can often occur through contracting or other arrangements with a third party. In some circumstances, risk transfer can raise difficult issues of governance – for example, of accountability for risk – and may result in higher costs. Risk communication can be a very important element of this option.

2.9 How have attitudes to risk changed?

Increased access to information has resulted in more informed consumers with less brand loyalty, so that competitive pressures on companies increase (Stewart, 1997). At the same time, improved communication channels have provided the mechanism for business conglomerates of unprecedented size, and although these conglomerates have access to new economies of scale, they also experience new management problems as a result of their global scope. With this increase in size of businesses, public concern has grown about the power of the commercial sector over their private lives, and pressure from electorates has in many places resulted in new laws to govern health and safety, privacy, competition

⁴⁰ BS 25999 for business continuity management as interpreted by BS 25777 for IT continuity management.

⁴¹ Not a transfer of ownership of the risk.

and the environment, which in turn has increased regulatory pressure on business through new legislation.

The focus of business has changed with new business markets emerging from new information and communications technologies and the shift of the majority of the European and American workforce to work in the service sector; heavy industries have moved elsewhere in the world. As the market's businesses targets have changed, so have their assets. The phrase 'intellectual property' had barely been heard of in the early 1990s, yet now IP often represents the most valuable item on the balance sheet (Stewart, 1997). Changes in assets have come with changes in the threats to those assets. Unknown, anonymous hackers can now wreak havoc on critical company systems from thousands of miles away, with minimum effort and resources.

As the pressures have increased and changed, new management techniques have been created for dealing with these pressures including quality and total quality management, business process re-engineering, and risk management or total company risk (strategies for company-wide risk control).

Where the inadequate controls are perceived to threaten economic and social stability, laws and regulations have been established to force organisations to manage risk. This maintains a high profile for risk which may engender a belief in being 'risk averse'; that is, risk is to be avoided completely rather than managed. This contrasts with the potential exorcism of the 'whistle blower' on risk who may be seen as unduly negative. These characteristics manifest in the poor communication of generally known software development risks by a project's technical staff⁴². To counter this, a structured and repeatable, life cycle-spanning method of risk identification is necessary for consistent risk management (IEEE Std 16085:2003). To be effective, the risk identification process must create and sustain a non-judgmental and non-attributive risk elicitation environment so that tentative or controversial views are heard.

2.10 Why is risk a problem?

Here I discuss why risk needs to be mitigated by looking at the consequences of inadequate risk management such as the cost of failure and realised risk in information systems. I also consider the stakeholder organisations that have taken action to raise awareness and provide working frameworks which encourage attention to the obligation to manage risk. These tend to be state and self-regulatory bodies such as government departments or professional institutions (see 2.6). The realisation of risk in information systems can have detrimental effects on the stakeholders who are the thrall of these bodies. They suffer the direct and indirect economic liabilities that result from the increased cost of correcting the information systems, as well as from the failure to realise the cost-benefit ratio expected

⁴² Software Engineering Institute of Carnegie Mellon University.

from the introduction of such systems. There are also ethical liabilities (Cavanagh, 1997) that result from injury or death that might occur from faults in the systems. It is therefore advantageous, both in terms of money and the quality of life of stakeholders, to introduce a method of eliminating as much risk as possible.

In 1988, research (Price Waterhouse, 1988) commissioned by the UK Department of Trade and Industry estimated that the annual loss to the UK economy that resulted from defects in domestically produced software sold on the open market was in the order of £600 million. These costs typically arose from the need to correct defects, both before and after delivery (including unnecessarily high maintenance costs), having to extend the expected delivery time and the development budget, and the indirect costs (such as the loss of business that results from damage to reputation) associated with a frustrated workforce and the frustration that users incurred because of the poor quality of the software (www.tickit.org).

Such losses are not solely confined to the UK and a study (Standish Group, 2003) of 13,522 information technology projects in the United States categorised projects as either: successful, challenged, or failed. Only a third of these projects were deemed to have been successful, with 43% of the projects having failed to keep within budget constraints and 82% of them having been delivered late. Twenty two years on from the DTI report, the failure of major public sector IT-enabled projects is still characterised by delay, overspend, poor performance and abandonment (POST, 2003). The measure of one third of projects being successful may be optimistic with a UK survey⁴³ reporting that only 15% of private sector IT projects were deemed to have been successful, with one in ten projects being abandoned.

There is a rich vein of literature describing projects which have suffered failures (*see Table 3*) related to their information system components through operational risk as rendered in the 'Basel' definition (*see 2.4*) but the language of these papers mainly refers to overall failure in the development process and does not approach this process failure in terms of the realisation of risk. A notable exception is Gotterbarn and Rogerson (2005) who draw out the need to improve risk management within the development process. Their paper presents the problem in these terms when a traffic management system failed. However they convey the view that the software which failed had worked correctly until the coincidence of two circumstances (the need to manually reset the software after a prescribed time and the need to run that software for a period longer than that stipulated in the documentation). This can be classified as *known risk* (Carr, Konda, et al., 2003) which was poorly mitigated against; I regard the software as never having worked properly – it was always broken but required the coincidence of certain circumstances to show this. Some projects where risk was realised are characterised by significant additional costs and extra work to meet requirements, loss of equipment, or the death or some interruption to the quality of life of the stakeholders and some prominent examples are discussed here. The Libra IT system for magistrates' courts

⁴³ Computer Weekly/Oxford University Survey, 2003

was designed for upgrading infrastructure, office automation facilities, a national casework application, and electronic links with other criminal justice agencies. The original contract for £184m was awarded in 1998 but implementation problems led to renegotiation of the contract in 2002, with a revised cost of over £318m, and a delay of two years before the initial benefits were anticipated (BCS and RAE, 2004). The principal cause being that the system was developed to support existing processes rather than re-engineering processes with new IT (National Audit Office, 2003). At the Department for Work and Pensions, a mistake by a computer operator prevented 40,000 PCs from accessing core systems between 22 and 26 November 2004⁴⁴ and problems with the implementation of a new IT system at the UK Passport Agency resulted in a backlog of 565,000 passports, delays of up to 50 days, and queues outside Passport Agency offices.⁴⁵

Table 3: Realised risk and the potential for standards intervention			
Project where risk was realised	Risk/Loss	Cause	Standards that may have helped
Ariane 5	Loss of equipment and subsequent confidence in reliability.	Expecting old software to be compatible with new hardware	Formal inspection of the implications of old software on new hardware (BS 7925-1:1998).
California telephone system stoppage	Loss of social and business communications and the inability to contact emergency services.	System untested after changing three lines of code.	Regression testing (ISO/IEC 12207:1995) ⁴⁶
Credit card fraud	Financial	Allowing staff to access enough details for identity theft.	Staff vetting (BS 7858:2004) and segregated responsibilities (ISO/IEC 17799 (BS 7799) Part 1:2000)

⁴⁴ Computer Weekly, 7 December 2004

⁴⁵ Computer Weekly, 29 June 2000

⁴⁶ Although it is noted that at the time of writing there is little or no international standardisation for software testing despite this being a clear area of risk mitigation.

Table 3: Realised risk and the potential for standards intervention

Project where risk was realised	Risk/Loss	Cause	Standards that may have helped
Department for Work and Pensions	Payments could not be made to benefit recipients.	A software upgrade was inadvertently made to PCs not intended to receive it. ⁴⁷	Configuration management (BS ISO/IEC TR 15846:1998, BIP 0051:2004)
Disclosure of minors' information	Access to information about vulnerable individuals.	Allowing staff with inappropriate intentions to access sensitive details	Staff vetting (BS 7858: 2004) and segregated responsibilities (ISO/IEC 17799 (BS 7799) Part 1:2000).
Libra	Desired gains to efficiency.	The Department developed IT to support existing processes rather than re-engineering processes with new IT (National Audit Office, 2003).	Soft Systems Methodology (Checkland, 1981) Requirements management under the umbrella of the STARTS Initiative (NCC, 1989).
Patriot missile failure	28 people killed	A chopping error (where the software only accepts numbers to a pre-designated significant figure) dulled the accuracy of the interceptor	Risk modelling to determine the level of accuracy required (BS EN 61014:2003).

⁴⁷ <http://www.newsfactor.com/perl/story/28939.html>

Table 3: Realised risk and the potential for standards intervention			
Project where risk was realised	Risk/Loss	Cause	Standards that may have helped
Therac 25	Death from fatal radiation doses to recipients of therapy (Joch, 1995).	Coding errors (Leveson and Turner, 1993).	Modelling the structure and the behaviour of the radiotherapy system using LOTOS (Turner, 2002; BS ISO 8807:1989). Software Quality Assurance framework (British Standards Institution, 2001, PD CR 13694:1999).

Other implemented systems, documented in the literature discussing software reliability, have seen the realisation of significant risks as a result of unreliable software (Jiantao, 1999): Control software known to be reliable for the Ariane 4 rocket was used on new hardware components of the Ariane 5. The old software failed to cope with the faster horizontal drifting speed of the new rocket. The rocket was destroyed. But worse still was the administering of burning radiation doses by the Therac 25 computer-controlled radiation-therapy machine which replaced mechanical safety controls with a software controlled safety mechanism (Leveson and Turner, 1993), and the sinking of the British destroyer Sheffield by an incoming missile mistaken as 'friendly' by radar system software. 28 lives were lost when a cumulative chopping error in guidance software missed 0.000000095 of a second in precision in every tenth of a second, accumulating for 100 hours, so that a Patriot missile failed to intercept a Scud missile. Lives were lost again during the stoppage of the local telephone systems in California and along the Eastern seaboard of the US as a result of changing three lines of code in a signalling program which contains millions lines of code – the change was considered small enough to negate the need for testing (Joch. 1995).

Preliminary data collection in the development of a taxonomy of risk suggested that security risks in information systems are greater in number than other types of risk. This may be because the definition (BS 7799-2:2002) of security risks relates to a wide range of losses affecting confidentiality, integrity, and availability. Typical business publications (NCC 2004; DTI/Price Waterhouse Coopers, 2004) class realised risks in information systems in terms of the vulnerabilities that are exploited. Archetypal examples from these reports include a feature of virus checking software designed to automatically download updated virus 'signatures' being hijacked to operate as an open relay to distribute 'spam' (unsolicited e-

mail, usually comprising sales, promotion, and marketing material). In a similar incident, an incorrectly configured e-mail server was used to relay spam and was blacklisted by several key organisations that are vital in distributing e-mails. Perhaps more serious were instances of theft of customer information by a member of staff who passed it to a third party who used the information to conduct credit card fraud and an member of staff who e-mailed a list of minors' personal details in relation to a sports club to himself before leaving employment.

These are examples where apparently emergent risk was realised although it may be argued that these were all unknown risks (Carr, Konda, et al., 2003) that were eminently discoverable.

2.11 Who says it's a problem? The drivers, stakeholders and interested parties

This section discusses the drivers for risk mitigation, representative stakeholder organisations which have identified the need to manage risk and some of the established and developing initiatives that they have created in response.

Information and knowledge are the thermonuclear competitive weapons of our time (Stewart, 1997). Any information that an organisation holds is an important asset and needs to be treated as such (BS 7799-2:2002). Risks are inherent (Carr, Konda, et al., 2003) in the software driving information systems that store and process that information. It is therefore not surprising that in order to secure information, international consortia (such as the Basel Committee for Banking Supervision) and governments have set out regulations with punitive measures for non-compliance to encourage a proactive response to risk⁴⁸. Individual examples of compliance are knitted together under the banner of good governance (Carr, Konda, et al., 2003), so that risks to the disclosure of sensitive, personal information carry national and international obligations⁴⁹ rather than allowing the risk of disclosure to be accepted. In addition to the social obligations of the regulatory regimes, information system users are typically at risk from e-crime (NHTCU, 2004) including the misuse of computer systems for fraud, hacking, virus and denial of service attacks, software piracy, on-line child abuse, extortion and drugs trafficking. In addition to social protection and e-crime, misuse (deliberate or accidental) of information systems by otherwise legitimate users is still the highest security risk (DTI/Price Waterhouse Coopers, 2004).

An interested party is a person or group having an interest in the performance or success of an organisation; a stakeholder is any individual, or organisation, that can affect, be affected

⁴⁸ In April 2010 the Information Commissioner was empowered to fine organisations up to £500,000 for the loss of personal data and in August 2010, the Financial Services Authority (FSA) fined Zurich Insurance £2.76m for the loss of a laptop with 46000 customer records.

⁴⁹ For example: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

by, or perceive itself to be affected by, a risk. Stakeholders include interested parties who may be customers, owners, people in an organisation, suppliers, bankers, unions, partners, or society (PD ISO/IEC Guide 73:2002).

A useful categorisation of stakeholders (Checkland, 1981) is presented by the soft systems methodology (SSM). SSM is a systematic thinking process for tackling situations where problems and issues can at first be unclear, or where there is uncertainty about precise objectives and actions. It is regarded as a business and risk management tool or technique (BS 6079-3:2000) which is appropriate for any type and level of problem identification and problem solving activity (Table 4).

Table 4: Roles in the Soft Systems Methodology	
Stakeholder	Role
Customers	Benefit from the system
Actors	Transform inputs to outputs
Owner	Has the authority to decide whether the system is accessible (that is, they may have the system switched off).

Customers would correspond to the thrall of the information systems, actors would be those developing and servicing the information systems and owners would be those bodies who issue the constraining edicts that should govern how the actors work together with the information system. SSM also refers to *environmental constraints* which may be influenced by those who do not interact directly with a system but rather exist (or coexist) within its thrall and corresponds to the *external events* of the definition of operational risk.

Each stakeholder will have a different view of the risks associated with a system because they will have different world views or 'Weltanschauung'. A wider taxonomy of stakeholders (Alexander, 2007) may be worth considering for the definition of this framework. Communications between stakeholders is often the major obstacle to risk management (Carr, Konda, et al., 2003). This suggests that methods for communicating risks, and what to do about them – proposed here as the application of knowledge encapsulated in standards – should be well received.

Regulatory bodies react to emergent risk by creating laws and regulations (social obligations) to promote the environment in which organisations have to manage risk as part of their operations. The drivers for organisations to proactively respond to these emergent, undesirable outcomes are regulatory pressures. Because, although risk management is a continuous process (Carr, Konda, et al., 2003), regulations are seen to be 'here and now'. In contrast, there is faith that (non regulatory) risks can be avoided. National and international government, and non-governmental organisations have recognised the need to either establish policies for managing risk or deliver tools to implement policies. In the context of

this thesis, a policy to manage risk may be realised by the detail in laws or in one or more standards. The views of the following organisations are considered.

The Organisation for Economic Cooperation and Development (OECD, 2002), which comprises 30 member nations (with connections to 70 others), first published guidelines for information security in 1992 and revised them in 2002. The document advocates such principles as awareness, responsibility, ethics, risk assessment and security design and implementation. The guidelines are a framework to engender greater trust by promoting a culture of security amongst stakeholders in information systems and networks. It is a high-level set of policies to raise awareness of the risks in information systems and networks, and the importance of implementing the policies, practices, measures and procedures available which exist to address those risks. The guidelines are, importantly, intended for both information system users and providers. They cover the respect for ethical values in the development, deployment and use of information systems and networks, to encourage the appropriate environment for co-operation and information sharing, that is deperimeterisation. At the lowest level, it is an encouragement for methods to improve risk culture as described in Chapter 4.

Security and risk was the focus of a proposal by the (then) Department of Trade and Industry for a European Union policy approach. The European Parliament, the Council, and the Commission have sought closer European co-ordination on information security by setting up the European Network and Information Security Agency (ENISA) with a view to ensuring a high and effective level of network and information security within the Community and in order to develop a risk-aware culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations across the European Union. The objective is support for the smooth functioning of the internal market. The Greece-based Agency was granted an initial mandate of 5 years from 2003 but has been sustained beyond this. It was awarded a significant budget of €24,300M for the original 15 Member States and further €9M for the 10 new entrants.

In the mid-seventies, the central banks and financial regulatory authorities of Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, United Kingdom and United States created the Basel Committee for Banking Supervision (Lopez, 2003). By the late eighties their first Capital Adequacy Accord was the benchmark for commercial banks to maintain standards to control credit risk. Following major bank collapses where credit risk was the victim of inadequate operational controls, a new accord – popularly known as Basel II – was established to fill the gap⁵⁰. Basel II comprises three 'pillars' of minimum capital requirements, a supervisory review of capital adequacy, and public disclosure. The key difference between the first and second accords is the new attention to assess and manage 'operational risk'. Just as information technology

⁵⁰ www.bis.org

has learnt much from the banking industry in the management of security, it may be assumed that the force of Basel II will have spin-off lessons in risk management.

In 1994, the Department of Trade and Industry (DTI) commissioned The National Computing Centre to carry out a Security Breaches Survey which showed that virus attacks, misuse, and equipment theft were widespread and cost organisations, on average, £9,000 to put right (a cost rising in subsequent biannual surveys). As a result DTI supported the development of a code of practice using the best practices recorded by a group of leading companies. In 1995, the British Standards Institution refined the code of practice and published it as British Standard (BS) number 7799. BS 7799 was refined in 1999 and 2000 to become a two-part standard defining a collection of information security – not information technology – controls to select from and build into business management systems. This was again refined in 2002 to reflect the Plan-Do-Check-Act (PDCA) life cycle of ISO 9001 (the standard for quality [management] systems) and the first part (the code of practice) was issued as an International standard by the International Standards Organisation (ISO) and given the number ISO/IEC 17799. The management system specification was published in 2005 as ISO 27001. BS 7799 (ISO/IEC 17799 or ISO/IEC 27002) is a framework within which the level of information security can be assured. A second part (BS 7799-2 or ISO/IEC 27001) sets out the requirements for an asset-based information security management system (ISMS) through attention to risk. In 2006, the Small Business Service of the DTI commissioned a tool that combined the policies of BS 7799 with the likelihood and impact of risks that may be realised without them. The risks that this tool addressed were derived from the ‘survey of surveys’ research (see Chapter 3).

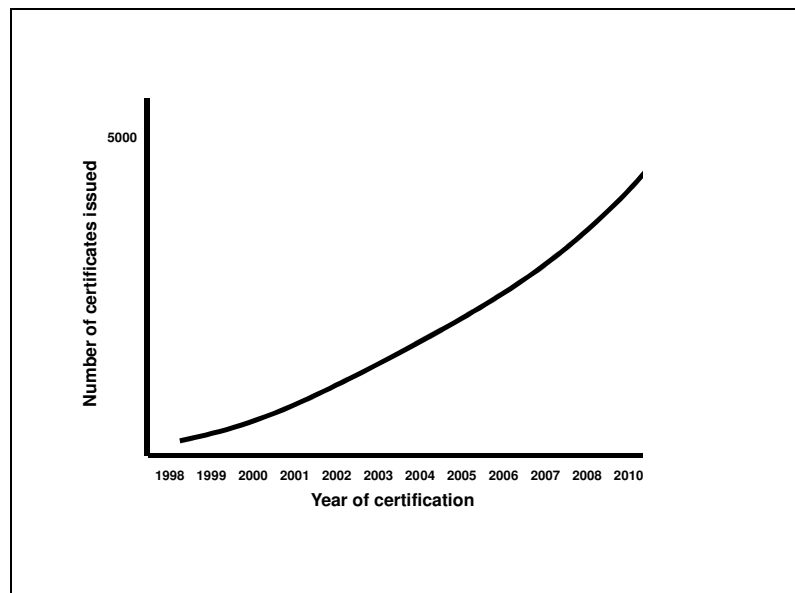


Figure 16: Uptake of accredited BS 7799 (ISO/IEC 27001) certification⁵¹

⁵¹With statistics from www.xisec.com/www.iso27001certificates.com/ Statistics recorded the 27001 User Group.

An ISMS is the implementation of a documented set of policies, processes, and procedures that pin down the general requirements of the code of practice to the individual nature of the organisation. Targets are set, controls are put in place to meet them, and measurements are made to confirm achievements or initiate improvements. Its uptake as a process of risk management is increasing (*see Figure 16*) but in the UK where certification is driven by market pressures the number of certifications remains counted in hundreds whereas in Japan ISO/IEC 27001 certification is a legal requirement for certain types of work, and certificates are registered in thousands.

The UK Department of Trade and Industry (DTI) recognised how the software industry has learnt much from developing the programs that lie at the heart of our everyday lives – from controlling traffic lights to running elevators, from powering microwave ovens to flying jumbo jets. When it goes wrong, lives may be lost, businesses can fail. In 1988, a report for the DTI indicated that quality risks in software development could be mitigated by implementing ISO 9001 (originally BS 5750 and then ISO 9000/9001/9002/9003) for Quality Systems and then being independently certificated for it (British Standards Institution, 2001).

A wealth of good practice had been built up from this experience. Ensuring these practices are available to all, especially smaller enterprises, became the heart of the DTI/NCC-established scheme: Towards Software Excellence (TSE)⁵² The scheme provided self-assessment, advice, and support over the Internet, aimed at helping smaller software development companies and IT enterprises to understand the capability of their current practices and improve their business processes. It was based on ISO/IEC 15504 for Process Assessment (ISO/IEC TR 15504:1999). The overall objective set for TSE, supported not only by UK government but also by industry bodies, enabled smaller enterprises in the UK software supplier industry to compare their contemporary approach with best practice. This gave them the knowledge to manage the risk in their software processes and hence maintain or improve their competitiveness.

Significantly, TSE was free from the pressures of certification, and complemented existing schemes including ISO 9001/TickIT and the Capability Maturity Model (CMM) with the objective of encouraging SMEs to take up such schemes when they feel the time is right and they have the resources available.

The Office of Government Commerce (OGC)⁵³ guidance outlines the approach to managing risk in its 'Management of Risk' (OGC, 2003) and advises on the preventive action approach. It does not detail further where the framework (herein suggested to be the standards knowledge base) may be drawn from.

⁵² Run by The National Computing Centre from 2000 to 2008

⁵³ www.ogc.gov.uk

The collapse of major organisations through fraudulent financial reporting prompted the passing, in the United States, of the Public Company Accounting Reform and Investor Protector Act of 2002 (commonly referred to as Sarbanes-Oxley) and its management through the U.S. Securities and Exchange Commission (SEC)⁵⁴. Section 404 requires board level certification of an organisation's financial activity and the effectiveness and status of the organisations' internal controls. It is these internal controls that manage operational risk so the implied requirements of good governance are now a statute in the US (with significant implications on foreign subsidiaries and non-US firms with listings on Wall Street, NASDAQ *et al.*) rather than implied ethical and moral obligations. As a result, a visible, approach to operational risk management is needed for auditors to see the effective management process and the subsequent accuracy of the reporting. Deficiencies, weaknesses, and acts of fraud must be reported.

The formalisation of ethics and good governance in the UK, leading to a demand for demonstrable management of operational risk, has largely matured since the end of the Twentieth Century (Morton, 2002). The emergent risk of poorly reported inadequacies in high-level governance of the Maxwell pension funds, the Bank of Credit and Commerce International (BCCI), and Polly Peck became the driver. The first set of improvements was proposed by Sir Adrian Cadbury (Cadbury, 1992), former chairman of the Cadbury chocolate company, in *'The Financial Aspects of Corporate Governance'*. This was a code of conduct for stock market-listed companies addressing ethical as well as legal questions. The implementation only really became clear when Turnbull promoted attention to risk management. This evolution of benchmarks for corporate governance was given focus by a working party of the Institute of Chartered Accountants in England and Wales (ICAEW). This was led by Nigel Turnbull (Turnbull, 1999) so the subsequent documents *'Internal Control: Guidance for Directors on the Combined Code'* has become known as the 'Turnbull Report'. Its message is that good corporate governance is achieved by internal controls and risk management. Like Sarbanes-Oxley and Basel II, financial prudence is the driver and a high quality of transparent reporting is a key aspect of compliance. Risks had to be managed and their acceptance must be from the highest level. The ability to put this into practice was been greatly boosted by the Higgs Report (Higgs, 2002) which reviewed the roles and effectiveness of non-executive directors in the UK. As a result, Higgs sets out measures designed to improve the structure and accountability of boardrooms in the UK. This is vital to instil a transparent approach to risk management.

Government (Cabinet Office, 2002; Cabinet Office, 2004 [2]) is concerned with enabling the public and private sectors as well as individuals to achieve secure and resilient information systems. To achieve this, the UK established the Central Sponsor for Information Assurance

⁵⁴ <http://www.sec.gov>

(CSIA)⁵⁵ to facilitate working in partnership with the public and private sector to address the protection of information systems, the information they carry, and their users, from hi-tech crime. The department promotes education and awareness of information security and took in hand training and skills for development in information security (before handing that responsibility to the Institute of Information Security Professionals⁵⁶).

The confidentiality, availability and reliability of information systems and the information they handle is an important concern for Government. The continuous provision of goods and services to citizens depends on the smooth running of the information systems supporting them – particularly in the event of a crisis. But Government cannot make the UK's information systems secure by itself. Most information networks are neither owned nor operated by Government so the actors (Checkland, 1981) who are expected to play a part in protecting information systems – from home computers, to the IT networks behind large companies to local and central government systems – will vary in characteristics and abilities, suggesting that any evaluation of risks emerging from the human vulnerabilities in information systems (see Chapter 4) will have to be focused on a taxonomy of users (Alexander, 2007) to provide sufficient variety (Ashby, 1957) in the responses to those risks. Interconnection and transfer through portable media is such that the contagion from a home computer can spread to business and into Government and vice versa (BIS/Price Waterhouse Coopers, 2010). A new culture of cyber-vigilance requires us to protect our computers from viruses and our privacy and identity from those who would abuse it (HMG's Office of Cybersecurity). The complexity of the risks requires a scalable approach that can be made to fit the size and place of impact. The risk mitigation framework of standards and risks described in this thesis (see Chapter 3) is so designed as to account for the risk and stakeholder view or *weltanschauung* in its application. Risks to security are no longer a simple matter of who you keep out; they are a complex and changing set of layers that decide who you let it in and how far.

2.12 Who sets standards?

Different types of organisation issue standards relevant to information systems. This thesis groups the organisations that develop standards into three categories: National and International Standards bodies, Professional bodies, and Consortia.

2.12.1 National and International Standards Bodies

National Standards Bodies are usually independent of government except for the endorsement of the institution and the granting of some financial assistance. For example, in

⁵⁵ Which became Information Security and Assurance (IS&A) before merging with the Office of Cybersecurity

⁵⁶ <http://www.instisp.com>

the UK, the national standards body is the British Standards Institution (BSI). BSI has a royal charter to set standards and award marks for compliance. BSI receives annual grants for standards development from the Department for Business Innovation and Skills. BSI is active internationally with permanent membership of all senior management committees of the International Standards Organisation (ISO) and the International Electrotechnical Commission (IEC), the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC/CLC). This is a typical arrangement for collaboration which is seen in other standards bodies such as those for Germany (DIN), and France (AFNOR). Outside the European dimension, other national bodies participate, for example: the US (ANSI) and Japan (JISC).

Above the national level, two levels of standards setting are apparent. Within the European Union, the Committee for European Standardisation (CEN) sets its own standards in areas with National Standards Bodies from the EU, supplying expertise and endorsement. Internationally, National Standards bodies participate in the development and endorsement of standards by the International Standards Organisation (ISO). National standards bodies can submit their own standards for endorsement or further development as International standards by ISO. For example, this has been realised for: British Standard BS 5750 for Quality Systems which became ISO 9001, British Standard BS 7799 for Information Security which became ISO/IEC 17799 (and then ISO/IEC 27002), and British Standard BS 15000 for IT service management which became ISO/IEC 20000.

2.12.2 Professional Bodies

Professional bodies – for example The British Computer Society (BCS), The Institution of Electronic and Electrical Engineers, and The National Computing Centre (NCC) – will assign delegates to their respective national standards bodies as well as publish standards of their own. These may be standards which are refined by the application of specified development processes or published to supply a perceived need of members and then more widely accepted as the de facto standard for an activity⁵⁷.

2.12.3 Consortia

There is at least a perception that the traditional standards organisations are too slow to react to the need for standardisation⁵⁸. The standards bodies have met this criticism with mechanisms to 'fast-track' standard specifications through their approval process if a mature specification is available. They have also created classifications of document that do not have the same authority as a published standard but allow the promulgation of best practice

⁵⁷ Such as the DTI's *STARTS Purchasers Handbook*, The National Computing Centre, 1989 which was eventually subsumed into TickIT Guide managed by BSI (q.v.)

⁵⁸ See 2.3.

in the view of a significant organisation, or group of organisations. Examples of these are the Publicly Available Specifications (PAS) of the British Standards Institution (BSI) and the Workshop Agreement of the European Committee for Standardisation (CWA). This promulgation of consensus lies at the operational root of standardisation consortia which are created by organisations with a common interest agreeing on a mode of working to declare a working practice associated with a specific discipline or technology as standard to meet a particular commercial need. Examples of consortia include the Jericho Forum⁵⁹ established for standardisation in information security, the World Wide Web Consortium⁶⁰ to set Internet technologies, and OASIS⁶¹ to determine appropriate information interchange standards using XML.

Consortia are characterised by their structures of governance and policies and procedure for managing intellectual property which are perceived as less formal than the National and International standards bodies.

2.13 How are standards set?

A standard can be described as an agreed-upon convention, specification, or way of doing things (LeGSB, 2005). The process by way that convention, specification, or way of doing things is recorded or codified is the process of developing documented standards. It is the codification of knowledge or an aspect of knowledge management. This may be implicit in the conversion of tacit knowledge to explicit knowledge (Nonaka, Toyama, and Konno, 2000), or explicit in a formal process (BS 0:1997). The challenge is to maintain a process that can deal effectively with that tacit knowledge which may be 'non-verbalized, or even non verbalizable, intuitive, unarticulated' (Hedlund, 1994). The creation of standards, by standards bodies and consortia, to mitigate risk using knowledge manifests the processes of externalisation and combination (Nonaka, Toyama, and Konno, 2000) – Figure 11 and Figure 17. Externalisation is the process of converting tacit knowledge, which is difficult to communicate, deeply rooted in action, procedures, routines, commitment, ideals, values, **and emotions**, to the explicit, codified knowledge – that which can be expressed in formal and systematic language, shared in the form of data, scientific formulae, manuals etc. – of documented standards.

⁵⁹ <https://www.opengroup.org/jericho/index.tpl>

⁶⁰ <http://www.w3.org/>

⁶¹ <http://www.oasis-open.org/cover/xml.html>

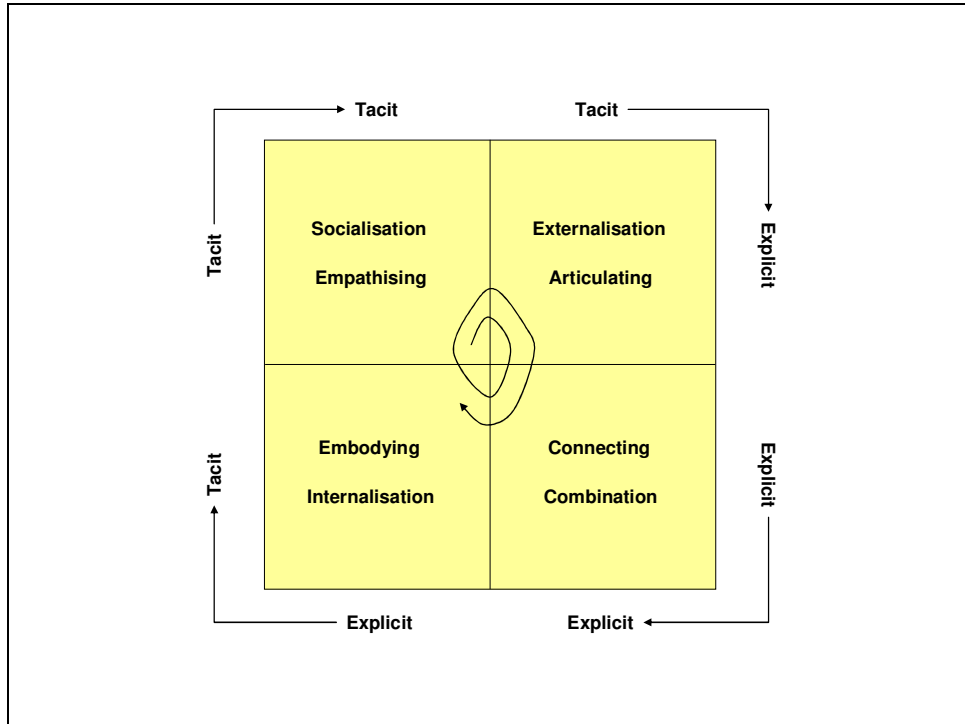


Figure 17: Maturing: Explicit to Explicit

Table 5 compares the processes whereby standards are developed to form a consensus document. The application of action research to test and refine one process exemplified by a standard consortium is described in Chapter 5. Chapter 5 includes a case study that looks at standards adoption in local government e-commerce, where e-commerce is defined as any information-based transaction according to the Cabinet Office report 'e-commerce@itsbest (1999).

Table 5: Standards development processes				
Stage	Standards Body Standard ⁶²	Standards Consortium Recommendation ⁶³	Standards Body Consensus ⁶⁴	Knowledge Management ⁶⁵
Proposal	A trigger for standardisation manifests itself and a New Work Item is proposed.	A trigger for standardisation is perceived and the need for a standard is proposed. This is formally recorded as a 'Request for a Proposal' (RFP). ⁶⁶	Experience of a successful method is proposed to the standards body for at least implied endorsement.	Originating ba This is typically represented by the coffee machine or water cooler interaction. Individuals share experience and opinion face to face.

⁶² British Standards Institution, *BS 0 A standard for standards*, 1997

⁶³ World Wide Web Consortium, Local e-Government Standards Body. The latter, which became the e-Standards Body, is the subject of a case study in Chapter 5.

⁶⁴ This process summary is modelled on the author's experience of CEN Workshop Agreements (CWA) and BSI's Publically Available Specification (PAS).

⁶⁵ Nonaka, Toyama, and Konno, 2000

⁶⁶ RFPs will usually be raised by someone who has an interest in the work of the consortium or by a member of the consortium. Some consortia are prepared to receive proposals in relation to all parts of their agenda, but prioritise those that support areas of activity of particular interest.

Table 5: Standards development processes

Stage	Standards Body Standard⁶²	Standards Consortium Recommendation⁶³	Standards Body Consensus⁶⁴	Knowledge Management⁶⁵
Review of the proposal	The proposal is reviewed by a Technical Committee and, if accepted, an author or team of authors is assigned to prepare a draft (who may or may not be members of the Technical Committee). To ensure that the current work is well understood, other complementary work is collated etc., a period of study may be designated to research the contents of the upcoming standard.	The RFP is reviewed by senior nominees within the consortium and will proceed to the development stage providing sufficient support for the topic is given.	A proposal to create a documented report of the good practice is made to the standards part with particular reference to funding the development of the report.	Dialoguing ba. The collective and face to face interactions begin to get some form as tacit knowledge is shared and articulated. Individuals with relevant knowledge and capabilities come to the fore.

Table 5: Standards development processes

Stage	Standards Body Standard ⁶²	Standards Consortium Recommendation ⁶³	Standards Body Consensus ⁶⁴	Knowledge Management ⁶⁵
Drafting and review of the draft	<p>One or more working drafts of the standard will be developed until the author(s) deem the work ready to submit as a Committee Draft. The technical committee will vote on the worthiness of the work to be accepted as a committee draft. Further development of the draft may be commissioned, creating additional committee drafts.</p>	<p>An initial draft of the proposed standards is collated by the consortium and is then referred to as a Request for Comments (RFC). An RFC is then released into the wider body of the consortium and the community for review. The consortium looks for expert and experiential comments as to the appropriateness of the topic and content of the standard.</p>	<p>The standards body appoints a secretariat to edit the report. A draft report of the method is compiled and reviewed at one or more meetings or workshops before experts in the field of the report are invited to review and return comments based on their experience.</p>	<p>Systemising ba. Collective and virtual interactions combine explicit knowledge.</p>

Table 5: Standards development processes

Stage	Standards Body Standard ⁶²	Standards Consortium Recommendation ⁶³	Standards Body Consensus ⁶⁴	Knowledge Management ⁶⁵
Testing	<p>When the technical committee deems that the standard contains all the relevant knowledge, presented as well as possible in the experience of the committee (and the author(s)), it will be made available as a Draft for Public Comment for a set period.</p>	<p>If the opinions recorded about the RFC are favourable, its status is elevated to a 'Draft Recommendation'. The draft recommendation is accorded an 'amber light status' and given a period during which use of the standard provides a further review. If the emerging standard is considered to be stable it will be deemed ready for approval and publication.</p>	<p>The report is distributed for comment beyond the initial list of invited experts, calling on stakeholders in the subject area to pass judgement on the contents of the report. This is the equivalent of a Draft for Public Comment.</p>	<p>Exercising ba. Individual and virtual interactions offer a context for internalization – the adoption of personal, tacit knowledge from the explicit knowledge resource (documented standards in this context). It puts into practice or action what dialoguing ba did through thought.</p>
Publication	<p>Comments from the period of Public Comment are reviewed by the committee and used to revise and create a Final Draft which, when voted for by the Technical Committee, becomes, the Published Standard.</p>	<p>Approved standards are typically published by storing them in a repository made available foremost to members of the consortium</p>	<p>The report is revised through the disposition of comments received. Again, meetings or workshops may be the method of interaction. When the report is deemed by the secretariat to comprise the consensus opinion of the stakeholders, it is prepared for publication.</p>	

Table 5: Standards development processes				
Stage	Standards Body Standard⁶²	Standards Consortium Recommendation⁶³	Standards Body Consensus⁶⁴	Knowledge Management⁶⁵
Promulgation	Published Standards enter the Catalogue of the standards body as the definitive recorded knowledge on the subject.	The consortium will engage in some sort of promotion and dissemination to encourage uptake of the standard.	The Standards Body will promulgate the report as part of its portfolio but with the demarcation that it is not to be regarded as a standard.	
Period of use.	Standards are resubmitted for review by the Technical Committee after a fixed period of time which may result in the standard remaining unchanged, being submitted for revision, or withdrawn.	The consortium will assign a period of use after which time the standard will be reviewed for its continuing suitability. The RFP/RFC process may be repeated to maintain the status quo, update the standard, or withdraw it.	The Consensus Document will remain on the Standards Body's catalogue until such time as it is either deemed to have lost its sponsorship, or that its popularity leads to its refinement as a fully endorsed standard.	

2.14 What is the status of the standards?

Standards are typically normative – those which must be followed to deliver the end result of the standard's objectives, or informative where they provide information to support a process or development or production of a product. The informative standards set out information which ought to be known but is not a mandatory element to assure the successful delivery of the end result. Some standards comprise⁶⁷ a mixture of normative and informative elements.

⁶⁷ For example the mandatory elements of ISO/IEC 27001 and the supporting guidance of the informative ISO/IEC 27002.

In the example model of the LeGSB (see the case study in Chapter 5), the highest priority standards are those which they adopt for use. In the nomenclature of LeGSB these are Certified Standards, a confusing term when viewed against the usual usage of 'certification' which normally refers to a certificate of compliance being awarded to an organisation or a product because it can provide evidence of conformance with the requirements of a standard against which it has been benchmarked. In the LeGSB model, normative standards are characterised by those relating exclusively to local government business and which have been 'certified' by the LeGSB process of consultation with its members and invited sources of expertise. These generally include standards of a very technical nature such as data definitions, XML schemas, ICT technical components and practice definitions.

LeGSB makes some effort to reduce the proliferation of standards in that it will adopt standards set by other recognised organisations, for example, BSI, ISO, eGU, OECD, which need to be inherited by local government, rather than look to develop their own version. This is a sensible approach which is also taken by other standards bodies, including BSI, and suggests that there is a conscious effort to avoid proliferation that concerns even the advocates of standardisation⁶⁸. Examples also include the detailed technical standards of data definitions, XML schemas, and ICT technical components referred to above, and bring in standards with wider applicability to information systems such as those for accessibility and security (non-functional quality characteristics). Because LeGSB recognises the rigour that these standards go through before acceptance by the recognised organisations, they are adopted through a simpler process than those emerging through use in their own discipline. This is similar to the liaison categories of the National and International standards bodies referred to above.

Another form of standard which permeates information systems – particularly those with Internet-enabled components – are recommendations of the World Wide Consortium (W3C) whose goal is to enhance the functionality and interoperability of the Web. Technologies or components of a technology are proposed for standard usage. A period of review by W3C is opened, the positive results of which are declared a recommendation. This is similar to the process of adopting standards for interoperability in central UK government under the mantle of the e-Government Interoperability Framework (e-GIF) which aims to manage the risk in interoperability by a catalogue of standards with a developing status of future consideration, under consideration, recommended, and approved. Some technologies may enter the 'observatory' for future consideration but be rejected during the approval process. (The Technical Standards Catalogue of the e-Government Interoperability Framework fulfils the BSI trigger of 'Will the published standard(s) ensure interoperability of businesses,

⁶⁸ See 2.3.

processes or products and services?’ and could be a framework to study interoperability standardisation specifically⁶⁹).

2.15 Differentiation: when is a standard not a standard?

Standards, as noted above, have agreement or approval under some process. This would seem to be accepted nomenclature, and not to be confused with ‘specification’ which is accepted to be informative. The status of specifications is similar to the third level of document declared by LeGSB which recommends Implementation Guides to help to convert the explicit knowledge of standards back to the tacit knowledge of practitioners who use them. LeGSB looks to include in this type of guidance on the implementation and usage of standards either set by LeGSB or by other organisations including examples, legal issues, and the financial considerations. This implementation guidance, fitting in with whether a standard is normative, has a simplified approval process before adoption, and carries the status ‘LeGSB Recommendation’ (not to be confused with the higher standard status of the W3C recommendation). So guidance may be referred to as informative documents that reduce risk in the implementation of standards. It may be valid to describe this as ‘best practice’, which may be documented as case studies. This is where conflicting views may be resolved. Implementers may disagree about how to implement a standard. The best practice and guidance can catalogue the acceptable (and note the unacceptable) implementations.

Another example of documents which are informative, and contain consensus opinion of stakeholders in the field the document is the CEN Workshop Agreement. (CEN is the European Standards Committee, a pan-European agency for standards setting.) As the name suggests, these are the reports of collaborative efforts and hold a similar status to the Technical Reports (TR) of the International Standards Organisation. A CWA or TR may be refined as a standard eventually but their informative nature allows for faster collation than their normative ‘standard’ counterparts. W3C also uses the grade of technical report. Similarly, the British Standards Institution publishes locally championed (usually by organisations with a particular field of expertise) ‘standardisation’ at the consensus level of the technical report. These ‘Publicly Available Specifications’ may be refined in time to become full standards but they are able to fill a gap in the standardisation portfolio, often by employing technical writers and a Delphi Technique-style panel to temper the content.

2.16 How much detail do standards provide?

Standards documentation – and by this I refer to the gamut of normative standards to informative specification – comprise a range of information levels within them. At the highest level there is the objective or policy statement which may be effected in different ways. A standard may comprise a number of normative policies which may be achieved in several informative ways, not necessarily prescribed by the standard. Informative standards may be

⁶⁹ In terms of Checkland and Holwell’s frameworks for learning (see Chapter 1 and Chapter 6).

embodied in codes of practice, the implementation of which produce the standard result or product or service benchmark.

These ways in which the policy may be effective are likely to be a network of processes, some of which may lie outside the area the standard focuses on. Processes may be documented as a succession of related procedures which may require implementers to develop local work instructions to take practitioners through the steps uniformly, depending on the level of expertise of the practitioners.

Just as the soft systems methodology recognises that different users will have different views of systems, so too does the body of knowledge in standards require a view of the support for particular technologies or communities. The *weltanschauung* or user view of a group of standards-related documents has been neatly labelled by LeGSB as a 'Blueprint' or a metastandard, of which e-GIF is an example. A blueprint is a collation of all known emerging standards and related information on a particular issue. Such metastandards are not only a source of convenience, they can also help focus further work to identify gaps and develop standards. Again, frameworks emerge as a source of learning about a problem.

2.17 Conclusion: leading to human vulnerabilities in information systems

Embracing standards as an explicit or implicit solution to a problem by treating risk is compatible with the common five-stage model of knowledge management (Khalil, Claudio and Seliem, 2006). These stages are knowledge acquisition (KA), knowledge documentation (KD), knowledge transfer (KT), knowledge creation (KC), and knowledge application (KP), where the documentation is exemplified by the publication of standards documents. There is also resonance with the classification method for standards that was defined during the research of a catalogue of standards and best practice advice for effective information assurance (Chapter 3) which shows that a standard (KD) may only provide a partial mitigation of a risk and that the knowledge documented therein may only be suitable for application (KP) by someone with suitable training or experience.

The poor regard for standards (*see 2.3*) when viewed as poor regard for espousing the appropriate behaviour in the face of risk, is indicative of the problem of preventing information security breaches as a result of a lack of correct human-information system interaction at the time of threat. Actors, customers and owners (Checkland, 1981) will still accept a wide band of risk depending on the perceived levels of stress the outcomes of the realised risk will cause (Coles, R. and Hodgkinson, 2008) and for some the risk is actually caused by measures put in place to treat it (Bryant, Davis et al., 2010). The emotional response to the stress drives the willingness to treat the risk using techniques which may be explicitly documented (Figure 11) but disregarded. It would be useful to have a methodology that could be used to learn where risk management in information systems relies on emotional literacy (Chapter 4) of the people involved and where technical constraints reduce

the risk to an acceptable level in terms of the impact of the realised risk (CESG, 2009). This will be useful to the stakeholders responsible for risk governance (*see 2.11*) as a means of decision support for taking action against unintentional error.

Three pieces of work have been particularly influential in the formulation of this thesis and the research methodology that was developed to investigate my ideas.

Taxonomy-based risk identification (Carr, Konda, et al., 2003) was the portal to other academic work on the components of information system risk (especially those associated with human factors and software) and introduced me to a sober representation of risk that is known, unknown, or unknowable in relation to the involvement of stakeholders in assessing that risk.

World in torment: a time whose idea must come (Beer, 1993) cemented the idea of drawing in literature on cybernetics and bringing out the attenuation risks of modelling and Ashby's laws of requisite variety and inter-recursive cohesion.

The six dumbest ideas in computer security (Ranum, 2005) sets out well the fundamental design flaws in computer systems that will remain as legacy until systems that have been designed with security in mind take over from them. This paper however suggests that locking down technology to avoid misuse is the only route to assurance. My hypothesis is that there is a wider source of good practice to be extracted from standards and the balance of locking down technology against the practice of educating and training users can be determined from the work described in Chapter 4.

CHAPTER 3. LINKING RISK TO STANDARDS

3.1 About this chapter

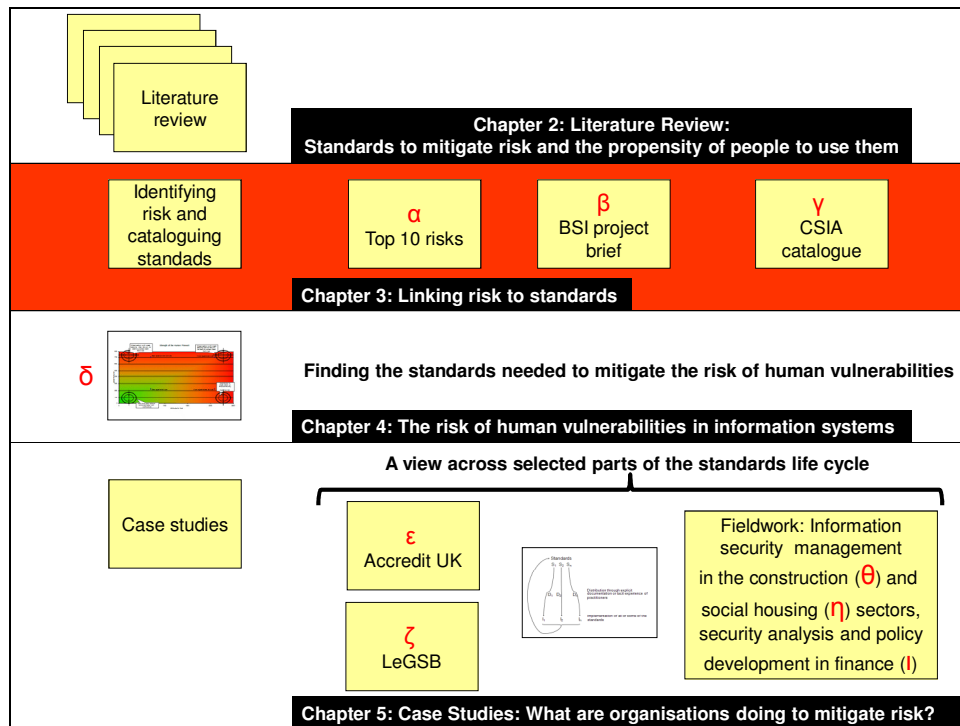


Figure 18: This chapter in the context of the thesis

This chapter describes three projects which address the research question, ‘How do you link risks to the standards that may mitigate them?’. These complementary projects are set out in Table 6 and described in detail below.

Table 6: Projects documented in this chapter	
Label	Project
Alpha α	An analysis of surveys for the Small Business Service of the Department of Trade and Industry where a ‘Top 10’ view of risks to information systems was derived. This highlights <i>what</i> the research problem is.
Beta β	Research and development of a project brief for the British Standards Institution (BSI), ‘Using Standards to Mitigate Risk in Information Systems’ which made the justification of <i>why</i> guidance is needed to promote standards to be promulgated as risk treatments.
Gamma γ	A project to establish a catalogue of <i>which</i> standards treat risks associated with information assurance.

3.2 Methodology

3.2.1 Choice and selection

The original research plan to analyse whether standards are efficacious in the treatment of risk was founded on the assumption that I would seek a consensus opinion that ‘Standards’ may be implemented to mitigate risk in information systems. This idea of taking a consensus view pervades the basis of the three research projects that are described in this chapter. It is also a recurring theme in my literature review (Chapter 2) which considers the formal recording of risk reduction techniques being linked to the reduction in risk with surety. Each of these projects comprised a period of desk research followed by the validation of that research by a Delphi-style panel of experts comprising a balanced mix of practitioners in the field of information security risk, both specialists and end-users. This is shown in Table 7.

Table 7: Research sources and validation			
	α	β	γ
	‘Top 10’ IS/IT Risks	BSI Project Brief	CSIA Catalogue
Source material	Multiple surveys of risks in IS/IT.	Software engineering body of knowledge (SWEBOK) and complementary standards.	Catalogues of standards in the field of information security and assurance.
Information extracted	Survey of surveys.	Specification of how the body of knowledge can be presented as a risk-treatment toolkit.	Populated taxonomy of publicly available guidance on information assurance.
Validation of results by:	End-user members of The National Computing Centre.	Subject matter experts from BSI panel IST/15 Software Engineering.	Information security experts.

The three projects may be viewed respectively as a granular exploration of the problem of risk in information systems (‘Top 10’ IS/IT Risks), an engine of engagement with the stakeholders who would benefit from a solution to the problems suggested by these risks, and a standard of standards – a metastandard – which provides the solution to the problem. The impact of the risks described in the first project (Alpha α) and which standards may be usefully applied from the third project (Gamma γ) to reduce risk to an acceptable level can be shown by the application of the methodology derived from the investigations into the human vulnerabilities in information systems (see Chapter 4).

A key objective of the survey of surveys was to establish some scope for the research overall. A list of prevalent (‘top ten’) IS/IT risks to small to medium sized enterprises was

requested by the Small Business Service (SBS) of the (then) UK Department of Trade and Industry (DTI). Discussions with the DTI's adviser settled the need to target ten risks in the list as a precursor to a possible larger study that may include the development of a risk assessment tool. The tool was commissioned and developed⁷⁰ soon after but using the 'Top 10' only. Feedback from the reviewers of the 'Top 10' list explained that they are not specific to SMEs as originally envisaged, but had implications for all information system users – owners, actors and customers. The limit of ten risks for this initial work was agreed so as to be able to market the information to the SME business community (defined by DTI as comprising organisations of less than 250 employees) in a popular format. It was recognised that this was not intended to be a definitive list of all risks but that the top-ten approach would have value as an introduction to the subject and that any other risk or risks outside of the selected ten could be the most critical for an SME carrying out a risk assessment.

The wider view of information systems risk within the 'Top 10' was maintained with the support of the British Standard Institution's (BSI) IST/15 committee which is responsible for developing and ratifying standards for software engineering. This assured consideration of information systems risk beyond the popular security triumvirate of confidentiality, integrity and availability (CIA) to include, for example, 'systems life cycle management, poor requirements definition, poor system design and inadequate testing' which may be the root cause of CIA breaches.

The National Computing Centre (NCC) had sent a delegate to attend IST/15 meetings since 1990 as a result of NCC's interest in good quality documentation. This led to my specifying the content of BS 7649⁷¹ for paper-based user documentation for application software, BS 7830⁷² for on-line user documentation for application software, and co-authoring a standard which combined the two (ISO/IEC 18019). The potential interest of BSI in this research was recognised and the research concepts were presented to IST/15. The result of this was an invitation to research and specify a project brief for consultants to develop a framework of the standards, information, and guidance required by industry to enable the efficient management, and opportunities for mitigation, of risk in information systems. This would include the most appropriate methods or deliverables in which this framework may be presented, covering (for example) a repository of risks and the details of standards that may be applied to mitigate them, and a Code of Practice for Using Standards to Mitigate Risk in Information Systems. As BSI's work would require exploitation of the project's deliverables for a financial return, the brief would be expected to specify the presentation of information

⁷⁰ www.businesslink.gov.uk/itrisk

⁷¹ BS 7649 British Standard Guide to the Design and Preparation of Documentation for Users of Applications Software.

⁷² BS 7830 British Standard Guide to the Design and Preparation of On-line Documentation for Users of Applications Software.

on-paper and on-line, by single purchase or by subscription and derived opportunities such as events and training⁷³.

This framework would have to be designed to be expandable and scalable to cover all relevant IT standards to ensure a sufficiently comprehensive approach to a variety of risk vectors. However, the initial focus would be those under the auspices of BSI Committee IST/15, which are expressly software engineering standards. IST/15 is well connected with other standardisation relevant to the research, in particular the committees which are responsible for IT service management and information security.⁷⁴

With this understanding of the identification of prevalent risk before specifying a methodology for detection and treatment, I established a project to survey contemporary surveys of information security risk. In this section I describe how a selection of significant risks was identified, with a view to investigating the standards that may be associated with the mitigation of that selection, and concentrating on collecting evidence that the standards contributed to that mitigation. The compilation of an initial list is described and then validated with the opinion first of a closed group of experts, and then with a broad church of information system users straddling the public and private sectors.

⁷³ These later manifested in:

- Information Asset Management, ½ day workshop, January 2010, (Maidenhead)
- Internal Audits of Business Continuity, One day workshop, *October 2009, (London)*
- Information Security in the Public Sector, Training Programme for the Chinese Ministry of Finance, *July 2009, (Manchester)*
- IT Governance, workshop for the British Standards Institution, *May 2009, (London)*
- Assessor Training – accrediting new assessors for AccreditedUK, *April and May, 2009 (Manchester)*
- IT Governance workshop, *February 2009 (Edinburgh), March 2009 (Cardiff)*
- Security: From Risk to Treatment, One day workshop, *April 2008 (NCC, Manchester), July 2008 (London), September 2008 (Manchester), February 2009 (London)*
- CS639/COMP60391/COMP61421 Computer (and Network) Security Module of the University of Manchester Advanced Computer Science MSc, 2004, updated 2005, 2006, 2007, 2008, 2009, 2010
- Dredge first, hedge later: Keeping risk business-focused (Aspects of information risk - being proportionate) *Construction Industry Computing Association (CICA) Workshop, 7 November 2007*
- Information Security Management: A standards approach, *One day workshop: March 2006 (NCC, Manchester)*

⁷⁴ The brief was not taken forward to be implemented when the BSI's publishing arm overruled IST/15 requesting the development and publication of the framework be carried out by a single author without the rigour of review by the committee members. This was reminiscent of the observations of control in standardisation programmes referred to in Backhouse, Hsu, and Silva, 2006.

Researching and selecting the ten risks - described herein (see Table 11) - met the difficulty in separating risk (strictly the effect, outcome, or loss) from the causes of the risk. It was considered that for the SME audience, it would probably not be useful to focus on the end results (the loss) alone as it may detract from attention that must be given, by the SME, to the timely reduction of the cause(s). To this end, the investigation did not distinguish between risk and the causes of risk.

Table 8: The method for selecting the 10 risks			
Stage	Activity	Description	Stage Deliverable(s)
1	Survey of surveys.	Collate the results of surveys about risk related to information systems.	Raw information about risks.
2	Identify a taxonomy of risk.	Arranged those risks and causes of risk in ten headings.	A taxonomy of risks from the surveys.
3	Define the top 10 risks.	Create a uniform style of description for each taxon to make it clear and unambiguous for reviewers.	A description of each of the top-ten risks.
4	Review the suggested 'top 10'.	The list was distributed to a selected 'panel' of experts for refinement.	Feedback from reviewers.
5	Adjust the top 10 using feedback from the review.	The opinion of the experts was collated to create a 'top ten' for submission to the SBS (who were working to a time-based agenda to deliver business-support information on the Internet).	A refined list of the top 10 risks.
6	Refine and validate the top 10 further.	Distribute the list for review by members of The National Computing Centre ⁷⁵ the Institute for Information Security Professionals, and consultants in information technology security subscribed to the discussion group of a World Wide Web forum (www.itsecurity.com) ⁷⁶ . Revise the list with feedback from the consultation.	A list that has been compared to experience.

⁷⁵ an association of information system users.

The survey of surveys involved finding studies and opinions on risks to SMEs. To be inclusive but avoid bias, surveys were sought and found that had been carried out by, or commissioned by, a representative sample of organisations. This meant that the risks in the list delivered by this research were initially defined by creating an aggregated view of risk lists published by UK public sector bodies, UK and European Consortia, trade press, and private enterprise studies published by information systems suppliers, and suppliers of information security services. The surveys from private enterprise were regarded with a degree of caution as they appeared to serve as marketing materials for products related to risk mitigation. However, they were deemed suitable for consideration because they could be correlated with the more independent studies and did not draw direct lines of action between the survey results and the product offerings⁷⁷. Only a few product suppliers were found to have carried out their own research and most referred to the (then) DTI's own bi-annual security breaches survey⁷⁸.

The evidence for information security risk – using the ‘top 10’ as examples – provided evidence and encouragement for BSI to commission (in the first instance) a project brief for metastandardisation – a framework connecting risk with mitigating standards. Table 9 describes the methodology for the research and development of the brief which included the following stages above and beyond the expected project management activities:

⁷⁶ who added some additional free-form comment to the body of knowledge analysed for the research.

⁷⁷ Note how Computer Weekly, 29 June 2010, reported that passwords were the biggest risk to information security supporting its article with the case proposed by a vendor of two-factor authentication. (However, the bias from an equipment manufacturer does not necessarily mean that the supporting evidence is suspect.)

⁷⁸ Price Waterhouse Coopers, *Information Security Breaches Survey*, Department of Trade and Industry (DTI)/Department for Business Enterprise and Regulatory Reform (BERR), 2004, 2006, and 2008

Table 9: The method for setting the project brief for BSI

Stage	Activity	Description	Stage Deliverable(s)
1	Desk research.	Desk research of standards published and in development: use the defined scope of the standards to define the risks that they are recognised as mitigating.	A connection between standards and realised risk.
2	Peer review.	Peer review – throughout the project – by an NCC colleague as the core method of internal quality assurance.	Corrections and amendments to prepare the brief for review by BSI.
3	Describe the framework.	Writing a description of the framework, its background, and justification.	The main body of the project brief
4	Specify a code of practice for applying the framework.	Specifying the contents of guidance and advice about how to apply the framework in practice.	
5	Describe the project's deliverables.	Describing how the framework and its attendant products should be made available, including publications, electronic products, subscription services for updates, briefings, training, and possible certification schemes for those who may apply the specified processes in their management systems.	
6	Review by BSI	Review the project brief with BSI Committee IST/15 (Software Engineering) and update it with feedback received.	Corrections and amendments to prepare the final brief for implementation.

The project brief was needed to set out the fully researched and justified background for the framework. It would specify how that framework should be constructed for an initial sample comprising those software engineering standards under the auspices of the IST/15 and other critical standards including ISO 9001 (Quality System), BS 7799 – now more readily

referred to as ISO/IEC 27001 (Information security management) and BS 15000 – now ISO/IEC 20000 (IT Service Management).

Although it was not apparent at the time the brief was under development, the commercial interests of BSI were to overtake the intentions of implementing the brief⁷⁹ and the opportunity arose to realise the intentions of the brief in a separate project where the range of standards scrutinised was focused on information security and assurance. This third desk-based research project investigated a process for collating and navigating through the standards that may mitigate the risks associated with information assurance. The research addressed methodological enquiries which emerged from consideration of the main research questions. These are shown in Table 10.

Table 10: Methodological elements supporting the research questions	
Research question	Methodological element
1 Do implemented 'Standards' mitigate risk?	Can the knowledge of risks be reverse-engineered from 'Standards' to link the 'Standards' to the risks?
2 Can 'Standards' be made more accessible?	Can you group standards, best practice, regulations and law into risk treatments?
3 How do you link risks to the 'Standards' that may mitigate them?	Can standards and risks be linked in a route map? How can that route map be applied? ⁸⁰

One of the definite deliverables that was envisaged by the research was a 'standard of standards' to mitigate risk in information systems. If such a metastandard could be created, it would produce an answer to two of the three research questions: *Can 'Standards' be made more accessible?* – because the metastandard would be a catalogue of standards and place them in the context of their utility, and *How do you link risks to the 'Standards' that may mitigate them?* – because the taxonomy of the catalogue would be the connecting structure of risks and the standards that populate the catalogue.

The research and development of the metastandard was initiated by the Central Sponsor for Information Assurance (CSIA – part of the Cabinet Office – now *Information Security and*

⁷⁹ The commercial decision to prepare a book on standardisation and risk mitigation that would not be part of the IST/15 programme of work.

⁸⁰ Better shown in the 'human vulnerabilities' project (Delta δ) of Chapter 4

*Assurance*⁸¹) to establish any gaps in the good practice advice available to mitigate the risks to information systems as defined by the International standard ISO/IEC 27001 *Information security management*. The research and development was specified as a commitment by The National Computing Centre to deliver a Technical Report⁸² – similar to the established ‘Body of Knowledge’ document that records the standards that define good practice in software engineering (SWEBoK) – that catalogued the standards and documented good practice that provide the detailed treatment of the risk that the ISO/IEC 27001 controls are designed mitigate. Items included in the catalogue will be ranked for applicability and suitability. This lead to a gap analysis that showed what controls were missing from ISO/IEC 27001, and what guidance⁸³ was missing to provide the detailed advice (for both the extant and the missing controls). The Cabinet Office would then be able to consider how the gaps could be filled by encouraging new research or declassifying government documents that already recommend risk treatments and making them more readily available. (An example of this was a set of recommendations on the secure destruction of electronic records that required access to classified technical processes to effect the destruction.)

The research and development method followed the stages documented in Table 11.

Table 11: Research and development stages for cataloguing IA standards			
Stage	Activity	Description	Stage Deliverable(s)
1	Mapping risk treatments.	Map the 135 risk treatment controls of ISO/IEC 27001 Annex A and design or select a taxonomy to assist navigation through them ⁸⁴ .	A taxonomy of risk to information systems.
2	Mapping standards to the taxonomy.	Map the controls to standards and best practice known to The National Computing Centre ⁸⁵ for implementing those risk treatments.	An initial gap analysis as a first draft definition of the Risk Treatment ‘Body of Knowledge’.

⁸¹ And joining with the Office of Cybersecurity in September 2010.

⁸² Available from the author.

⁸³ The importance of including both social and technical controls was recognised.

⁸⁴ The suitability of the ISO/IEC 27001 taxonomy was considered.

⁸⁵ Sources were to include but not be restricted to: respected books, Chambers of Commerce, Consortia (for example: the Jericho Forum, SAINT, the Information Security Forum), Government agencies (for example nationally: ACPO, GESG, CSIA, DTI, NISCC, OGC, SOCA and internationally: ENISA, OECD/WTO). WARPs/CERTs etc., Professional Bodies (for example: BBA,

Table 11: Research and development stages for cataloguing IA standards

Stage	Activity	Description	Stage Deliverable(s)
3	Rank the effectiveness of the standards and expertise required to use them.	Design a scale for rating suitability and applicability of risk treatment information. Consider: The type of standard or guidance (is it process or product based?); Which risk treatments are well documented? Which risk treatments need more guidance? The scale would take an e-GIF-like approach ⁸⁶ to the standard/best practice/guidance. The ranking would be applied to award an initial suitability and applicability rating to each treatment ⁸⁷ .	Ranked catalogue of publicly available risk treatment guidance.
4	Define the availability of the guidance.	The taxonomy/ranking would also consider the availability of items from the Body of Knowledge.	Ownership and access rights to the catalogued information.
5	Consultation and review.	Consult a representative sample of organisations straddling the public and private sectors to check and supplement the early draft with their own knowledge ⁸⁸ .	Additional entries for the catalogue.
6	Apply feedback from the consultation.	Update first draft to incorporate responses from those on the contact list.	Updated catalogue.

BCS, CIPD, IISP, Intellect, NCC), Standards Bodies (for example: BSI, ISO/IEC, IEEE, IET, and NIST).

⁸⁶ That is: 'Adopted', 'Recommended', 'Under review', or for 'Future consideration'?

⁸⁷ The suitability and applicability ranking may be context based so that risk treatments are keyed to the risks where they will have the best mitigating effect.

⁸⁸ Reviewers were asked to include a critical suitability and applicability rating for recommended information (both for what they add and for what is already there) and request suggested 'not recommended' risk treatment information.

Table 11: Research and development stages for cataloguing IA standards

Stage	Activity	Description	Stage Deliverable(s)
7	Report writing.	Create a report in a format that is a hybrid of the e-GIF 'Technical Standards Catalogue' and CSIA's 'A review of UK Government and industry initiatives'.	Report for issue.
8	Define how the catalogue may be kept current.	Research and development to specify how the deliverables from the original work package will be kept up to date, relevant, and made available (such as - for example – web presence ⁸⁹ , CD ROMs, printed catalogues, analysis tool etc.).	A second, supporting report that defines delivery mechanisms to provide the initial documentation baseline, and maintain both the gap analysis and the documentation baseline on an ongoing basis.

The second report would recommend mechanisms for introducing new risk treatment guidance into the catalogue, withdrawing obsolete material and noting obsolescent items⁹⁰, and changing the status of catalogued risk treatments ensuring that they are labelled appropriately for suitability and applicability. The report recommended establishing an active network of public and private sector informants – based on the 'Delphi' panel of reviewers – who would be polled every six months for changes. Part of this six-monthly gap-analysis review would include researching experienced and expected risk realisation to identify available risk treatment information and the gap analysis of what needs to be developed.

3.2.2 Application of the methodology

Table 12 catalogues the sources of information that I assembled using my knowledge and experience of working in the field of IT for 20 years, supplemented with a search of Internet pages. The selection was limited to these when it was recognised that there was a significant overlap between the sources.

⁸⁹ Which could include recommendations for positioning as part of 'Getsafeonline' or the UK GovTalk repository and links from the sites of other IA stakeholders.

⁹⁰ Where selected risk treatments may not be relevant for current practice but awareness for legacy practice is necessary.

Table 12: Surveys reviewed for the survey	
Source	Description
Computerworld ⁹¹	Computerworld, the 'Voice of IT Management,' is a weekly U.S.-based hub of a 58-edition global IT media network, published by the International Data Group (IDG).
Council of Europe's Convention on Cyber Crime ⁹²	In view of the increasing use of new technologies, Member States pledged to combat high-tech crime and cyber crime in all its forms. The Council and Parliament adopted an action plan on promoting the safe use of the internet by combating messages with harmful and illegal content.
The Central Sponsor for Information Assurance (CSIA) ⁹³	The CSIA is a unit of the UK Government's Cabinet Office and works with partners in the public and private sectors, as well as its International counterparts, to help safeguard the nation's IT and telecommunications services.
The Department of Trade and Industry (DTI) ⁹⁴	The Department of Trade and Industry (DTI) aimed to increase competitiveness and scientific excellence to generate higher levels of sustainable growth and productivity in modern Britain. It encouraged successful business start-ups, including small and medium-sized enterprises, with practical support through Business Link. This included help and advice on best practice, training, employment law, and new technology. The DTI also helped British firms to export their products to overseas markets. In 2007 its responsibilities were split between the Department for Business Enterprise and Regulatory Reform (BERR) and the Technology Strategy Board (TSB).
Gen-i ⁹⁵	Gen-i helps organisations in New Zealand generate greater value from their IT and telecommunications spend, while managing the transition from legacy networks and systems to converged technologies.

⁹¹ www.computerworld.com

⁹² www.europa.eu.int

⁹³ www.cabinet-office.gov.uk/csia

⁹⁴ www.number-10.gov.uk

⁹⁵ www.gen-i.co.nz

Table 12: Surveys reviewed for the survey	
Source	Description
The Real Time Club ⁹⁶	The Real Time Club comprises 150 entrepreneurs from the IT community who meet for discussion, debate and dinner on a regular basis and has done so continuously since 1967. Speakers are leaders of sectors including Finance, Business, Education, Computer/Telecommunications industries and Government. It publishes an annual consideration of risks faced by the 'IT industry' under the banner of the 'ICT Banana skins'.
The National High-Tech Crime Unit (NHTCU) ⁹⁷	The National Hi-Tech Crime Unit was part of the UK's National Crime Squad and launched in April 2001 as part of the national hi-tech crime strategy announced by the Home Secretary to Parliament in November 2000. The NHTCU was the first UK national law enforcement organisation tasked to combat national, and transnational, serious and organised computer-based crime which impacts upon the United Kingdom. It became part of the Serious Organised Crime Agency (SOCA) in 2005.
PC/Computing magazine ⁹⁸	PC/Computing is a periodical from Ziff Davis Publishing for knowledgeable personal computer users who are interested in general news and trends in addition to the technological aspects of computing.
SilentRunner Inc ⁹⁹	Silent Runner Inc., a manufacturer of computer security equipment, and part of Computer Associates.
Unisys ¹⁰⁰	Unisys is a worldwide information technology services and solutions company delivering expertise in consulting, systems integration, outsourcing, infrastructure, and server technology.

⁹⁶ www.realttimeclub.org.uk

⁹⁷ www.nhtcu.org

⁹⁸ www.zdnet.com/

⁹⁹ ca.com

¹⁰⁰ www.unisys.com/

Table 12: Surveys reviewed for the survey	
Source	Description
The National Computing Centre ¹⁰¹	The National Computing Centre is the UK's IT membership organisation, serving corporate, vendor and government communities. NCC champions the effective use of IT to maximise the competitiveness of its members' businesses. This is done by providing impartial advice and support, best practice and standards and personal and professional development. NCC is a social enterprise.

To make sense of the rich vein of primary research, I looked for representative groupings of particular kinds of risk in the collated body of research with a view to selecting a taxonomy of ten headings. I selected groups of risk from the surveys and used a mind mapping tool to sort the individual risks from the surveys until the groupings settled into 10, level 1 categories. These headings are presented here in alphabetical order. It was noted that amongst the sources of the reports, no indication was given as to the relevant severity of the risks, with the exception of the DTI's security breaches survey (DTI/Price Waterhouse Coopers, 2004).

Table 13: Common groups of risk from the surveys		
	Risk or the cause of risk	Definition
1.	Complacency, lack of awareness or understanding, or accepting too much risk.	Unless the chance of a risk can be reduced to zero – at which point it may be argued that it is no longer a risk – there must be some level of acceptance. This may be a deliberate act or through ignorance.
2.	Fraud, identity, theft or sabotage of data or systems.	The value of information assets may be measured in several different ways varying from the focused total cost of ownership of hardware and software (Gartner Group, 1987) to including the calculation of the value of intangible assets such as intellectual property (Stewart, 1997). This may be extended to very personal losses through the targeted theft of very specific items of identification that allow inappropriate access to bank accounts.

¹⁰¹ www.ncc.co.uk

Table 13: Common groups of risk from the surveys		
	Risk or the cause of risk	Definition
3.	Governance, legal and regulatory compliance.	The collapse of major organisations through fraudulent financial reporting prompted attention to the internal controls that manage operational risk (Armstrong, Rhys-Jones, Dresner, 2004) so the implied requirements of good governance are now a statute in the US ¹⁰² and benchmarks for corporate regulation in the UK (Cadbury, 1992; Higgs, 2002; and Turnbull, 1999). Banking has also introduced its own risk management framework ¹⁰³ .
4.	Holes punched through established defences (home-office deperimeterisation).	Onion-skin models (Alexander, 2007) for access to information systems become less effective with the autonomy given to legitimate users. People, other systems, or software applications that are allowed permission into the defined periphery may allow inappropriate traffic through its perimeter and cannot easily be differentiated from legitimate activity (NCC, 2004 [2]).
5.	Inadequate resilience/business continuity management.	Business continuity plans should not be expected to pre-empt every eventuality (Armstrong, Rhys-Jones, Dresner, 2004) or emergent risk but rather provide a framework of mitigating action based on the probability (risk) of incidents from risk assessment or treatment plans.

¹⁰² *Public Company Accounting Reform and Investor Protector Act 2002* (commonly referred to as Sarbanes-Oxley). Section 404 requires board level certification of an organisation's financial activity and the effectiveness and status of the organisations internal controls.

¹⁰³ The second *Basel Accord of the Bank of International Settlements* (Basel II)

Table 13: Common groups of risk from the surveys

Risk or the cause of risk		Definition
6.	Malicious Software.	There are several variations on the theme of malicious code. Worms permeate computer systems, changing code and erasing files. They are difficult to trace and stop. Macro viruses hide within applications files such as spreadsheets or word processor documents, and their damage can extend well beyond the application. Trojan Horses, like their legendary namesake, hold hidden problems within an otherwise innocent looking file. They break down defences to enable unauthorised access to the network.
7.	Systems life cycle management, especially requirements definition and testing.	In 1988, research (Price Waterhouse, 1988) commissioned by the UK Department of Trade and Industry, estimated the annual loss to the UK economy resulting from defects in domestically produced software sold on the open market to be £600 million. A complementary report (Logica, 1987) indicated that quality risks in software development could be mitigated by implementing ISO 9000 (which was BS 5750 at the time and is now ISO 9001) for Quality Systems and being independently certificated for it – a major endorsement that implementing a standard can mitigate risk. The information technology certification scheme designed to encourage this peaked at a little over 1700 certifications and had dropped to less than 1300 by 2005 ¹⁰⁴ .
8.	Unacceptable use by or through staff, contractors, partners.	This category of risk has similar properties to the category of 'Fraud etc'. (2 above). It refers to the deliberate or accidental misuse of appropriately granted privileges with both innocent and malicious intent by those with permission to be where they are.
9.	Unauthorised access.	In contrast to the granting of appropriate access in the category of 'Holes etc.' (4 above), this class of risk is relatively short, but only in as much as the opportunities for its realisation are clearer: access is gained to places where it should not have been.

¹⁰⁴ www.tickit.org

Table 13: Common groups of risk from the surveys

Risk or the cause of risk		Definition
10.	Wireless networks.	Although there are only two examples here, it was originally considered that the popularity of reporting concern over wireless communication and the blanket banning of their use in some significant circumstances (NISCC, 2002) was important to reflect here.

My intention was to restrict the list of ten risks to a clear, general taxonomy which would be as inclusive as possible within the constraint of ten items. This would avoid a reader, who did not see a risk which they considered important, failing to give the list adequate credibility. An example of this was the intention to class the popular concern about wireless networks as a manifestation or example of ‘tunnelling’ through other risk-mitigating activity. However, the pervasive occurrence of the concerns over wireless data transfer – apparent in many conversations (Chapter 4) and in the survey of surveys – indicated that it would be important to maintain this as a distinctive class of risk, at least in the initial sorting so that sufficient prominence could be given to that risk in the final taxonomy. The components of the collected survey were sorted into these classes as shown in Table 14. These are quoted verbatim from the corpus of surveys following a short definition of each. (The first validation of the ‘top ten’ with the panel of experts supported this view of the original classification scheme; wireless network risk became an example rather than a category.)

Table 14: Risks from the surveys sorted into the groups

Description		Examples
1.	Complacency, lack of awareness or understanding, or accepting too much risk.	<p>Concealment of attacks.</p> <p>Flawed risk assessment – i.e., 'who would want to attack us? – Not only are large multinationals targets, but SMEs are also an attractive target for hackers.</p> <p>Assumption that virus protection is adequate security – Virus protection is seen today as an essential security measure for SMEs in New Zealand. Unfortunately for most of these businesses this is their ONLY security measure.</p> <p>No method of detecting a security breach or compromise – While there may be a prevention security system measure in place, more often than not there is NO detection measure. This is the equivalent of a bank locking its doors but having no alarm system installed.</p> <p>Invalid belief that information security is a firewall – Setting security policies in a company does not provide the same protection as a company firewall. If applicable, these should both be implemented as part of an overall security system.</p> <p>No procedures for handling security incidents – When a security incident occurs there should be a set procedure outlining all possible actions, responsibilities and alternatives for the company.</p> <p>Placing more importance on ease of use or cost, rather than security – Many New Zealand businesses underrate the importance of security measures and settle for 'user friendliness'.</p> <p>Don't believe that all sites for shopping are safe. Two very popular security methods are the Secure Electronic Transaction (SET) or Secure Socket Layer (SSL). These methods have security issues that are more trustworthy when shopping online.</p> <p>Inadequate security policies and procedures.</p> <p>Personal websites are easily hacked into. If there is valuable information on a website, make sure to have a firewall in place.</p> <p>VPN Tunnel Vulnerabilities – If a hacker worms his way into the VPN he can have free and easy access to the network.</p>

Table 14: Risks from the surveys sorted into the groups

	Description	Examples
2.	Fraud, identity, theft or sabotage of data or systems.	<p>Theft of data. This can include proprietary information and intellectual property such as customer lists, research and development, financial data and personal information.</p> <p>Corporate web site spoofing attacks. A spoof website claims to be the legitimate site of a particular organisation and is set up to look like the original.</p> <p>Financial fraud, through deception and identity theft, for example:</p> <ul style="list-style-type: none"> • Sabotage of, or damage to, data or networks. • Personal ID card fails. Phishing. <p>Adoption of federated architectures for identity and access management will accelerate.</p> <p>Browsers can give out information about people by the settings they choose. They start with names and e-mail addresses usually, and these are sold to companies.</p> <p>Computer related forgery. Computer related fraud.</p> <p>Credit reporting agencies will become more involved in managing the consequences of identity theft.</p> <p>Criminals can impersonate you and get valuable information about you. Use digital signatures for authorization.</p> <p>Data interference. Don't let personal information get out to the public. Once it is publicized, it will be sold to companies. If personal information is stolen, report it to your credit card companies, banks, and other personal agencies.</p> <p>E-mail is not private. Encryption and decryption is recommended for high security e-mails.</p> <p>Enterprises will revisit role-based access control for identity and access management.</p> <p>Internet relationships are not always private. People can hack into chats and files; so don't send private information online.</p> <p>Internet sites sell personal information. Report privacy issues to government agency. Get a free e-mail account from a site like Yahoo or Hotmail to give out if you have to.</p> <p>Never give out a bank account number under any circumstances. If someone gets this number, they can empty the account with no authorization.</p> <p>System interference. Theft of data.</p> <p>There are many different scams online. Shop at only sites that are reputable, and use a credit card to buy online. Most credit companies will charge people for only the first \$50 charged, if their number is stolen.</p>

Table 14: Risks from the surveys sorted into the groups

		Table 14: Risks from the surveys sorted into the groups	
		Description	Examples
3.	Governance, legal and regulatory compliance.	Application software breaches will lead to 'lemon laws'	<p>Copyright and similar rights offences</p> <p>Copyright law litigation.</p> <p>Data protection too onerous.</p> <p>European Software Licensing</p> <p>Extra-territorialism.</p> <p>Illegal interception.</p> <p>IPR Enforcement Directive</p> <p>IT Governance.</p> <p>Offshore outsourcing hits UK</p> <p>Online child pornography</p> <p>Outsourcing put on hold.</p> <p>SCO suit succeeds</p> <p>System suppliers in court.</p> <p>The Disappearing IT Director</p>
4.	Holes punched through established defences (home-office deperimeterisation).	Application risks.	<p>Music and video browsers – These automatically connect the user to related web sites - all without the user's permission.</p> <p>Peer-to-Peer Applications – In a peer-to-peer environment, it has an implied trust between servers.</p> <p>Using a modem while connected to the LAN.</p>

Table 14: Risks from the surveys sorted into the groups

		Table 14: Risks from the surveys sorted into the groups	
		Description	Examples
5.	Inadequate resilience/business continuity management.	Damage to reputation. Denial of service ¹⁰⁵ Disaster recovery found wanting. Diversionary Tactics ¹⁰⁶ Legacy systems halt. National Grid fails. Non-resilient systems. Not making or testing backups. Physical accidents or attacks. SPAM halts the Internet. Systems failure. Websites damage brands.	
6.	Malicious Software.	Virus attacks. 2003 brought a variety of new viruses targeting a number of software weaknesses. Trusting insecure messages, for example, e-mail or phone calls. Phone calls or e-mails can easily be tapped or hacked into, for example, the 'love bug' virus was a good example of a virus using people's e-mail address books to send the virus on. Blended attacks. Worms and viruses have become more complicated and now a single one can execute itself or even attack more than one platform. Computer viruses ('worms' or 'Trojans'). Cyber attack styles will become virulent. E-mail attachments. Workers opening an attachment could unleash a virus or a worm to the network of their employer. In most cases just opening the e-mail and not even clicking on the attachment can open the virus. Opening unsolicited e-mail attachments. Viruses.	

¹⁰⁵ Whereby attackers prevent legitimate users of a service from using that service.

¹⁰⁶ Security administrators are busy 'putting out fires' that hackers have set in the servers of targeted companies.

Table 14: Risks from the surveys sorted into the groups

	Description	Examples
7.	Systems life cycle management especially requirements definition and testing.	<p>Lack of independent verification of system integrity. Outsourcing to an independent security specialist can provide vital checks of the system.</p> <p>Having reactive rather than proactive security processes. Businesses should not wait for any of their own organisation's processes to be breached – security plans should already be in place to prevent the occurrence, for example, companies should have a disaster recovery plan in place in case of a fire.</p> <p>Systems demographics disasters.</p> <p>Users versus IT professionals.</p> <p>Enterprises will turn to proactive 'defence-in-depth' as business needs drive security.</p> <p>Errors in systems software or hardware design.</p> <p>Microsoft's SOAP. The Simple Object Access Protocol (SOAP) doesn't have any security specifications built in it, SilentRunner warns.</p> <p>Not installing security patches for browsers and mail clients.</p> <p>Out-of-date systems and software.</p> <p>Virtual directory technology will increasingly become a strategic component of identity integration projects.</p>

Table 14: Risks from the surveys sorted into the groups

Description		Examples
8.	Unacceptable use by or through staff, contractors, partners.	<p>Unauthorised access to, or misuse of, the company web site, such as accessing secure areas or storing illicit material on the servers.</p> <p>Disgruntled IT employee.</p> <p>Criminal use of the Internet.</p> <p>Implicit encouragement of staff bypassing security measures. Strict procedures are required which must be followed at all times.</p> <p>Downloads from Web Sites. By misusing the Internet in the workplace by downloading games, movies and music; it opens the network to attack and sucks up valuable bandwidth.</p> <p>Inappropriate use.</p> <p>Installing screensavers and games.</p> <p>Misuse of devices.</p> <p>Renaming Documents. An employee could save a job under a different name and e-mail it to someone that shouldn't see the information. Even though the company might have monitoring software, it might not pick up something like this since it's under a different name.</p> <p>Supply Chain and Partners Added to the Network. Administrators might access the network for a partner company and then, when the job is over, forget to close the access.</p> <p>Trusted networks involving business partners and others will grow as sources of risk.</p>
9.	Unauthorised access.	<p>Unauthorised access to, or penetration of, corporate systems, such as hacking or gaining access through social engineering.</p> <p>Hackers unite.</p> <p>Hacking.</p> <p>Illegal access.</p> <p>Organized attacks by Internet desperados will increase.</p> <p>Unauthorised access.</p>
10.	Wireless networks.	<p>Wireless systems setback</p> <p>The mobile realm will continue to grow as a Petri dish for security incidents.</p>

Four risks – or causes of risk – remained after this initial sorting and needed careful consideration as to whether excluding any of the examples may invalidate the taxonomy. The four risks: ‘drive by wire accidents’, ‘cyber terrorism’, ‘unexpected attacks’, and ‘knowledge economy fails’ had at least the common attribute that they originated in the same survey – ICT Banana Skins report. Although excluding them from the taxonomy for this reason was not acceptable – because it would question the acceptability of the consideration of that whole survey, it was decided that each could be justifiably excluded for its own deficiency without damaging the reasoning that had led to the creation of the ‘first cut’ top ten list.

Table 15: Excluded risks	
Risk or cause of risk	Justification for exclusion
Drive by wire accidents	A specialised technology.
Cyber Terrorism	Acts of cyberterrorism are adequately covered by ‘component risks’ in the rest of the taxonomy.
Unexpected attacks	Too broad a heading. Risk assessment may be regarded as sufficiently mature a discipline so that the ‘expected’ outweighs the ‘unexpected’. Many effects of the ‘Unexpected attacks’ are likely to be adequately covered by ‘component risks’ in the rest of the taxonomy.
Knowledge economy fails	Information systems are not constrained in the generation of information for sale alone but form part of larger business models.

This collated top ten list was distributed by e-mail to an internal IT infrastructure manager and web hosting provision manager (responded), an IT security expert and former adviser to the Commonwealth Games (responded), the former IT director of an insurance company (responded), a visiting professor of computer security and forensics (no response), the technical director of a penetration testing and computer forensics company (no response), systems engineer for a major technology vendor (responded), anti-virus expert (no response), the technology adviser for a telecoms provider (responded), the technical director of security testing specialist (no response), two lawyers (both responded), a pan-government systems accreditor (no response), and the public sector programme manager from a government department (responded).

The responses from the experts comprised general support for the extracted ‘draft’ list, comments on how the risks in the draft were prioritised, and some additional risks that they, or their clients had had to deal with. Most of the ‘additional’ risks were not new but rather fitted into one of the top ten categories. The respondents recognised this. Taking the comments and additional risks into account, the final list in Table 16 was established.

Although the respondents had not all shown which of all the risks they considered the most widespread, this rough order of prevalence was teased out of the correspondence:

Table 16: 'Delphi' panel response	
Risk or cause of risk	
1.	Sabotage of data or systems, malicious software.
2.	Systems life cycle management, poor requirements definition, poor system design and inadequate testing.
3.	Unacceptable use by or through staff, contractors, partners, and former employees.
4.	Breaches in established defences, poor/changes to configuration without risk analysis.
5.	Governance weaknesses, lack of legal and regulatory compliance.
6.	Unauthorised access, fraud, identity theft.
7.	Loss of key resource – staff/supplier relationships.
8.	Complacency, lack of awareness or understanding of risks, or accepting too much risk.
9.	Inadequate resilience, poor business continuity management.
10.	Lack of professional, affordable IS/IT risk mitigation specialists to advise on and implement risk reduction plans.

This collated list was then validated further by engaging with the information system user community represented by members of The National Computing Centre (NCC). Recognising that users need to engage in dialogue with vendors and that vendors are also a grouping of computer user, there is also a category of membership for vendors. These are both included in the NCC's membership and were used as a second sounding board following the refinement of the list with feedback from selected stakeholders in risk management. NCC was providing membership services to over 700 subscribing organisations¹⁰⁷ and the top 10 list of risks was sent to 1135 member contacts within these organisations with a request to review them against the five questions shown below. Typical member contacts have job titles such as IT Manager, IT Director, or Head of IS. The membership base is cross-sector with a sectoral breakdown shown in Table 17 to illustrate the broad view of risk considered for this research:

¹⁰⁷ Survey of NCC's membership, 2004. Membership is on an organisational basis with an annual subscription.

Industry	%		Industry	%
Production	21.3		Government	24.0
Transport and Communications	4.0		Health and Education	5.3
Finance	8.0		Other Services	13.3
Business Services	13.3		IT Suppliers	9.3
			Other	1.5

Although in terms of size, NCC Member organisations are predominately of medium to large in terms of size of the overall organisation (*see Table 18*), a member's IS function itself has an SME service model for its size in relationship to the rest of the organisation¹⁰⁸ and so was considered as an eligible sounding board for validating the opinion in the survey of surveys.

IT staff	%
Up to 10	28.0
11 to 25	20.0
26 to 50	18.7
Over 50	30.7
Not given	2.6

The members were e-mailed the list which had been validated by the expert panel. The e-mail message included a request to consider the following five questions:

- (1) Are these risks those which concern you most?
- (2) What risks are not listed that should be?
- (3) Which of these risks – from the list or those which you have added – have been realised in your organisation?
- (4) Have you any other information, opinion, or experience which you would like to contribute?

¹⁰⁸ Which led to the adaptation of the Accredited UK standard (*see Chapter 5*) for IT Department Accreditation in 2009.

- (5) What have you done to mitigate these risks – from the list or those which you have added?

Members were also offered the opportunity to receive the draft paper which explained how the initial list was extracted from the 'survey of surveys' and reviewed by the panel of experts to derive the list that was released for the wider consultation. Several respondents requested the paper but did not voice any opinion in reply to the five questions.

Responses were received from an automotive components supplier, a borough council, 3 computer services departments from universities and management colleges, a provider of services into the construction industry, an information assurance consultancy, local government, a passenger railway franchise, a privatised government agency, a software developer for the financial services industry, a unitary authority, and a utilities company. Respondents offered broad support to the list and in some cases, showed how they would prioritise the list either by concern or by those risks that had been realised in their organisations. These results were used to inform the project brief for BSI (project Beta β) and the catalogue for CSIA (project Gamma γ).

Project β was divided into two stages: planning and research. The planning stage set out the structure of the work to be completed during the research stage. This comprised outlining the background and justification to be included in the project brief, its scope and its structure. The objective of the project brief was to set out the background, justification, scope, and structure of a framework showing how standards can be used to manage risk and the industry benefits with the potential for complementary initiatives (such as new standards for risk management) to put the framework in context. The project brief covered the research needed to identify which standards to include and provide some quantitative information on the scale of guidance that would be required and the number of standards to cover. The brief also suggested what information the target audience would need, the content and the potential shelf-life of such information because technologies, methods of deployment and associated standards continue to change. For this point it was suggested to break the information required by industry down into modules, such as 'stable' and 'developing' and to take into consideration the frequency of any change.

The brief detailed the methods and formats that could be used to deliver the framework, and the best methods of getting the information to the target audience, including the presentation of the information and navigation through it. As the framework was likely to be extensive – resembling the Software Engineering Body of Knowledge (IEEE, 2004) – the brief also recorded how an overview of the information may be derived and how the framework could be supported by complementary products that can be based on, or derived from the code of practice.

Another instruction in the brief was to 'reverse engineer' a risk register from standards and apply the probability of an occurrence of respective risks to temper the attention given to them. The resulting risk guide would assist users with different views and priorities (the

weltanschauung of the soft system method) to select the best practice that should be in place to mitigate at least the known risks in the information systems life cycle (as modelled by ISO/IEC 15288 *System life cycle processes*). The intention to develop the framework from the brief was superseded by the application of its overall concept in researching a catalogue of information assurance risk and standards which – according to my literature review (Chapter 2) – could mitigate those risks. This research was carried out on behalf of the Cabinet Office whose interest lay in reducing such risks in the public sector in particular.

The desk research for the catalogue (γ) was applied as planned with some struggle to involve some of the contributing organisations. This reticence to be involved was evidenced in two aspects. Firstly an association of information and communication technology suppliers who is seen as the authoritative body representing the good proactive views of those organisations took a step back and offered no guidance of their own but referred to other sources. Secondly, two organisations that publish standards and good practice took a good deal of convincing that their work was only going to be referenced in the catalogue and would not be made freely available as a result. The benefit of exposing the existence of their own research and development to a potentially new fee-paying audience was not immediately understood and it took some dialogue before it was agreed that participation in this research had a potential return for both organisations.

The core of the catalogue manifested as a series of tables. Each table covered a control from ISO/IEC 27001 Appendix A¹⁰⁹. These are directly derived from, and aligned with, those listed in ISO/IEC 27002 (17799):2005 Clauses 5 to 15 where each control objective is designed to address a category of risk.¹¹⁰ Each control objective is categorised, in the catalogue, as applicable to three areas of context: people treatments, process treatments, and technology treatments

¹⁰⁹ The standard notes that the list of controls is not exhaustive and an organisation may consider that additional control objectives and controls are necessary.

¹¹⁰ Changes to the structure of the Catalogue would be triggered by changes to ISO/IEC 27001 Appendix A or changes to ISO/IEC 27002 (which may take time to be reflected in ISO/IEC 27001), or the recognition of new controls which may not be covered by the ISO/IEC 27000 series.

Subclause of ISO/IEC 17799	Source/identification	Description/title	Suitability
7.1 Responsibility for assets			
7.1.2 Ownership of assets	BS ISO/IEC 19770-1:2006	Software asset management. Processes	B2
	National Computing Centre, Guideline 231	Asset Management Across The Distributed Enterprise	B2
	National Computing Centre, Guideline 278	Software Asset Management	B2

Figure 19: A sample from the catalogue tables

In this application of the risk taxonomy of ISO/IEC 27002 (see Figure 19), a control objective may appear in one or more categories. Each item of published risk treatment advice is then assigned to the relevant controls (for each control objective) and may appear more than once within the catalogue, in one or more of the three areas of context – to address risks or the causes of risk associated with people, process, or technology respectively. The suitability of each piece of advice applies to the thoroughness of the advice for addressing the risk in the relevant context for the level of expertise needed to apply it. Hence, the same advice may appear in different tables with a different ranking based on the context of the risk.

Because the catalogue would be subject to the risk of becoming too narrowly focused or carrying obsolete or at best obsolescent recommendations, the involvement of cross-sector researchers and practitioners was considered core to the method compiling the catalogue and subsequently keeping it up to date. I also noted in the report for the Cabinet Office that accompanied the catalogue that it is only of value if it is accessible and used. However, the risk of only engendering a narrow awareness of the catalogue is also mitigated by the same principle: engagement with organisations with the objective of promulgating IA best practice. This process is based on the work done to compile the first issue of the catalogue. The methodical process of creating the catalogue – that was recorded for the purpose of updating it too – follows.

A directory of organisations active in the field of publishing IA standards and best practice guidance was compiled¹¹¹ by reviewing standards and best practice publications (including websites) and noting the sources of information and the publishing bodies. The directory was validated by the Cabinet Office. Each organisation on the directory was contacted, requesting a listing of its relevant publications that may be classified as IA standards and

¹¹¹ The intention in the longer term would be to establish an 'IA Standards and Best Practice Observatory' with organisations who would commit to regular involvement.

best practice guidance¹¹². This is where I asked for access to copies of the standards and best practice guidance for review for classification in the catalogue. Some organisations saw this as a threat to their income, expecting that a reference in the catalogue was part of Cabinet Office mandate to issue the documents free of charge beyond their membership. The fears of this risk were allayed in correspondence that explained that the 'publicly available' label of the catalogue referred to information that did not carry the government's protective marking; it was not suggesting that it could not be distributed to a 'restricted' audience of fee payers. During the gathering of information from these sources, I also noted how the catalogue could be kept up to date efficiently recording the existing of updating services where available (which would be subject to relevant agreement of the information owners). These included the BSI PLUS service which, although available to BSI members who buy selected standards, may be negotiated for cataloguing information only, and the free e-mail notification of the (American) National Institute for Science and Technology (NIST) Special Publications (which themselves comprise a significant amount of free information).

The lists of standards and best practice guidance issued by the participating organisations were reviewed to categorise each item in terms of its applicability for inclusion in the catalogue by reading with the background question of whether it addresses a risk that ISO/IEC 27001 sets out to control, and if so how does it do that? Is the risk controlled by attention to people aspects (such as educating users to counteract the human vulnerabilities in information systems – see Chapter 4), controlled by defining a process to follow and so avoid or reduce the risk, or promote a technology to ameliorate the risk. A positive response to this categorisation would lead to the inclusion of a document in the catalogue. It was then subjected to the more granular review of its suitability for mitigating the risk (assuming its guidance is correctly implemented) either partially or in its entirety, and the level of expertise expected of those implementing the instructions of the documentation. A ranking matrix for each item of standards and best practice guidance is shown in Table 19. The starting point for the classification was the information owners' suggested ranking.

¹¹² In the sustained model of the regular publication of the catalogue, the request would have focused on the nomination of new or revised risk treatments that they publish, the validation of existing information in the Catalogue (either confirming its current relevance, its redesignation as obsolescent or obsolete), and a suggested ranking (to be taken into consideration during peer review).

Table 19: Ranking of the risk treatments in the catalogue				
		How directly applicable is the guidance to the risk that it could mitigate?		
		A thorough approach	Significant guidance	Some help
		A	B	C
No expertise	1	A1	B1	C1
Some expertise	2	A2	B2	C2
Expert knowledge needed	3	A3	B3	C3

The format for the catalogue was established so that future editions would record changes to the previous edition of the catalogue in an annex to the main document. To comply with the intention of the catalogue being a ‘gap analysis’ for the Cabinet Office and so highlight opportunities to seek out (for declassification) or develop more guidance, the catalogue was scrutinised for controls that do not have treatments of at least B2, being the core classification of providing significant guidance without demanding much expertise to follow it.

I questioned the completeness of the ISO/IEC 27002 taxonomy because of the risk of a taxonomy excluding useful standards and best practice that would mitigate risks that did not fit with it. However, all the documents that I found or were suggested to me had a place in an ISO/IEC 27002 taxon¹¹³. This classification was strengthened further by the agreement of the reviewers who carried out a peer review of the draft catalogue and only suggested a few additions of documents that should have been included and no change to the positioning of any entries in the catalogue. This compilation and review process was documented and repeated to issue a second version of the catalogue six months later. The second version of the catalogue expanded its field of reference for trawling standards and best practice. The work for this catalogue had been commissioned from The National Computing Centre and as a result, attention has focused on the information systems standards associated with storing and processing information and with the risks concerned with the state of the data or information in transit. It did not include publishers of standards that specifically covered the field of telecommunications amongst its target ‘observatory’ organisations. This is an example of the potential shortcomings in not treating risk associated with a taxonomy based classification (Carr, Konda, et al., 2003). A view of the wider field of publications – telecommunications and computing – was applied for the second edition of the catalogue.

¹¹³ This finding is further validated by a recent (2009) rearrangement of the ISO/IEC 27002 controls by the Dutch national standards body which does not introduce new classes into the standard’s taxonomy.

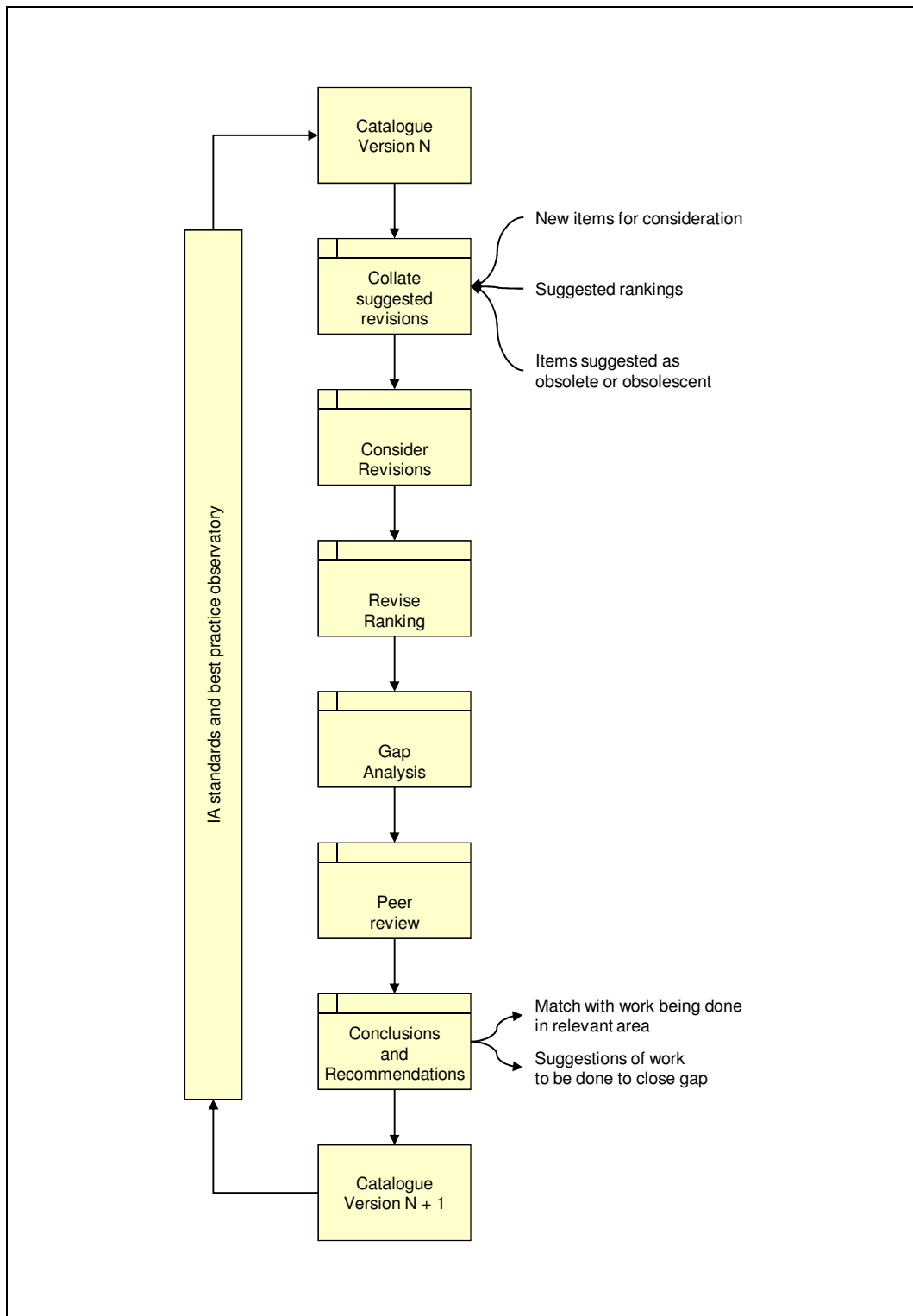


Figure 20: Creating and updating the catalogue

CHAPTER 4. PROJECT DELTA δ : THE RISK OF HUMAN VULNERABILITIES IN INFORMATION SYSTEMS

4.1 This chapter in context

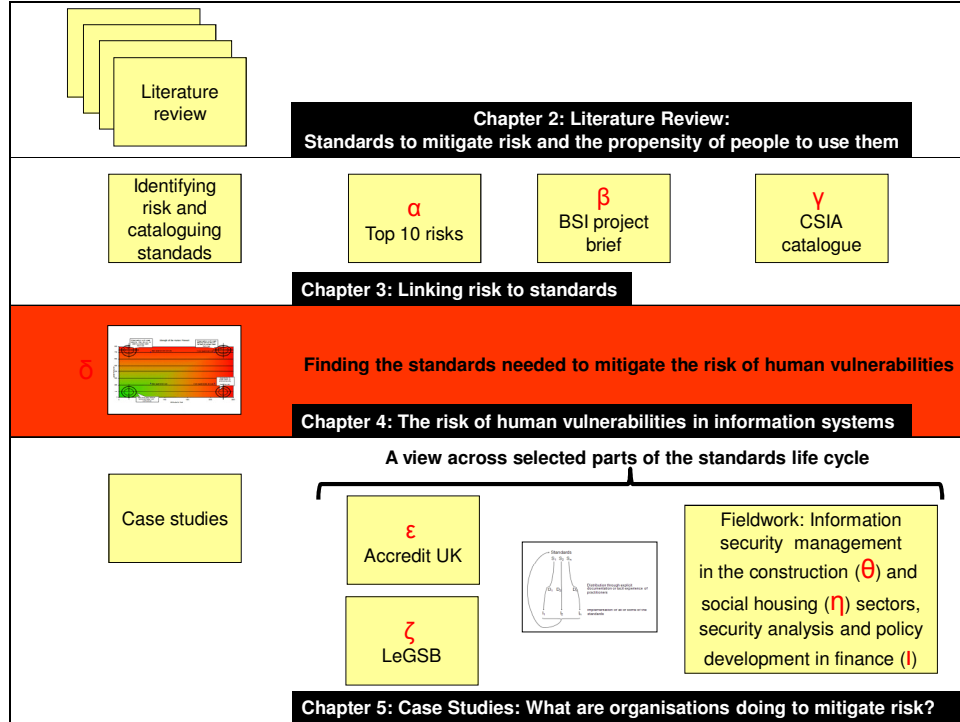


Figure 21: This chapter in the context of the thesis

In the opening chapter of this thesis I described the motivation for the research and in chapter 2, the literature review, explained the supporting background to the research from academic literature and industry reports, and the wider motivation for work based on the socio-political concerns that are apparent. The preceding chapter – 3 – described the desk research carried out to identify the risks and the standards that are to be considered by my core hypothesis that standards mitigate risk. The literature review of chapter 2 and the cataloguing work described in chapter 3 show that data and information security on computer networks is increasingly important to individuals seeking assurances of privacy and anonymity, and to governments and commerce seeking assurances of legitimacy, accuracy, and control, with the survey of surveys pointing towards concern over information system security risks caused by people. This chapter describes the part of my research that tested the feasibility of a survey methodology to detect *who* are the human vulnerabilities in information systems so that appropriate treatments – captured in documented standards - can be selected and applied to reduce the risks from these vulnerabilities to an acceptable level. The project was carried out with the support of the Innovation Platform of the Technology Strategy Board which was looking at new ways to reveal human vulnerabilities in information systems, and improve organisational risk cultures.

4.2 What is a human vulnerability?

My study refers to a human vulnerability (in an information system or any of its component parts) as the vector through which a loss of any single or combination of confidentiality, integrity and availability may take place. This is independent of the quality of the information system (see 4.4 below). It also makes no assumption that the source of risk may be malicious or accidental. An insider threat is defined by CERT (Cappelli et al., 2009) as a 'current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems'. A useful definition structure is offered by I3P¹¹⁴ which differentiates non-malicious insiders from malicious insiders where the latter 'is one motivated to adversely impact an organization's mission by taking action that compromises information confidentiality, integrity, and/or availability'. Deliberate actions – or violations – particularly as a result of disgruntled employees are seen as a significant vector (Cappelli et al., 2005). This study – in its scrutiny of both the organisation and the individual – takes account of the organisation's circumstance as part of the environment that will have an effect on the individual's motivation and affect the risk of disgruntled employees but similarly does not downplay the damage that may be done through mistakes of, say, an end-user which are the result of poor software design. So the research described in this chapter considers the seriousness of the effect of the risk or loss and deliberately excludes considering whether it is the result of a mistake or a violation, although this is useful information for the detection of where a loss may occur. The research concentrates on detection with a view to mitigation by releasing knowledge from relevant standards. This may result in improved working practices in the operation of an information system of longer term changes in the design of systems software (see 4.4).

4.3 Finding an acceptable level of risk

The proposal was that wherever risk needs to be managed, that need is second to achieving an acceptable level of risk. Could there be a benchmarked, technology-agnostic approach of discovering and treating risk that could match the risk appetite in different situations and appreciating where – if anywhere – the common level of acceptability (Dresner and Wood, 2007) applies? If that risk stems from human vulnerabilities, how do you identify them? If you can identify them, what can you do to reduce exposure and improve the risk culture? I have made the assumption that information security risk may be managed by strong security policies – as defined by standards – and that human vulnerabilities may undermine those policies. This agrees with the body of knowledge that was analysed for this project which

¹¹⁴ The Institute for Information Infrastructure Protection – a consortium of academic institutions, national laboratories and non-profit research organisations addressing cyber security challenges affecting the critical infrastructures.

records particularly insider threats from human vulnerabilities as bypassing information security controls that are defined by specific organisational information security policies.

This chapter considers the use of information systems by '*organisations*' which may be identifiable by location or some form of branding, and '*communities*' which may, like the organisations, have shared goals and values. For the purpose of detecting human vulnerabilities, a view of where the information system is in use is needed to gain an understanding of where the boundaries of risk lie. As a benchmark of acceptable risk, the risk appetite of an organisation or – where no organisation is clearly defined – the *community* using the information system was selected. The project investigated a technique for placing individuals and organisations on a scale of risk with a view to identifying actions that would move them to their preferred position (on the scale) if change were needed with respect to the business impact of the risk if realised¹¹⁵. The following chapter – 5 – comprises case studies that took an empirical view of the literature review (Chapter 2), the cataloguing work of Chapter 3, and the appreciation of the need to account for the human vulnerabilities in information systems (this chapter) when implementing a security management system (as defined by ISO/IEC 27001) looking at how standards emerge to treat risk and how well information security policies – as realisation of part or parts of standards – are implemented as risk management controls.

Data collection in the development of a catalogue of risk treatments (Chapter 3) shows that security risks in information systems are greater in number than other types of risk. This may be because the definition (BS 7799-2:2002) of security risks relates to a wide range of losses affecting confidentiality, integrity, and availability (a definition of security that is sometimes extended to include non-repudiation of the transaction – or transformation – under scrutiny. Examples of the risks realised through human vulnerabilities in information systems include theft of customer information by a member of staff who passed it to a third party who used the information to conduct credit card fraud and where, before leaving employment, a member of staff e-mailed a list of minors' personal details, in relation to a sports club, to himself (NCC, 2004).

I was interested in finding a method that identifies the people most likely to introduce a risk, or who would see a risk realised in an information system. Would they know what to do to mitigate a risk? If they could mitigate that risk through treatment, would they recognise risk in time or be prepared to implement the amelioration? I propose that wherever it is that risk needs to be managed, that need is second to the overall need to achieve an acceptable level of risk, whether that be a message passing over a telecommunications network or a user logging onto a computer to receive that message. Elimination of all risk is impractical and unreasonable to expect. So, this research project was fundamentally concerned with

¹¹⁵ Outside of HMG where the business impact tables of 'HMG IA Standard No. 1, *Technical Risk Assessment* Issue No: 3.51, October 2009' is the standard to be maintained, there is no common model of the effect or outcome of risk realisation.

finding a technology-agnostic way of discovering and treating risk that could be taken up as a consistently repeatable approach to matching the risk appetite in different situations and appreciating where – if anywhere – the common level of acceptability applies.

4.4 Software and systems quality

This project makes no assumptions about the quality of the software (which may be measured by applying the characteristics and metrics framework of the ISO/IEC 25030 series). It does make the assumption that there will be design flaws in the software that will require alert users to take countermeasures and will cause others to err through incompatibility between the characteristics of security and usability. These less enlightened users may place too much trust in the correct function of the system or rely on blame to be transferable to it (Flechais, Riegelsberger, Sasse 2005) at best working in an attitude of positive expectation that one's vulnerabilities will not be exploited (Riegelsberger, Sasse, and McCarthy, 2005). This work is needed because there will be active failures through both technical and social vulnerabilities (Flechais, Sasse, and Hailes. 2003) – the realisation of security risk will result from slips (attention failures), lapses (memory failures), mistakes (rule or knowledge failures – intended actions which lead to unintended results), and violations (actions that intentionally breach the security of the systems). I define a security risk as the cause of a loss of any single or combination of confidentiality, integrity, or availability.

It is important to take this work in context. The temptation to label users as 'the weakest link' (Sasse, Brostoff, and Weirich 2001) should not lead to a belief that user education will be a panacea (Ranum, 2005). It should however be used to suggest that the portfolio of standards may be applied to treat the risks from the detected human vulnerabilities. These treatments may include user education but only from the perspective that any education will only be effective if users believe in the risk (Sasse, 2003), and cost effective, secure systems design (Flechais, Sasse, and Hailes. 2003) which sets policies and targets to assure risk management within the context of the software in use (the policies and targets being the regulators of the protection of information in the system). Reworking the software will be desirable but is unlikely to have the speed of return that is needed – standards beyond those for good development practices will be required, as well as enticing the implementation of the good practices which are already known.

4.5 Methodology

It is frequently reported that the most prevalent risk to information security is the people involved in the development, deployment, and use of information systems¹¹⁶ (NCC, 2005). There is a challenge to find those who do not pay sufficient attention to risk and the very *human* nature of losing their sense of emotional literacy in an effort to achieve personal goals or just to get the job done (Hillson and Murray-Webster, 2007). Ignoring risk may have

¹¹⁶ *Information Security Breaches Survey(s)*, Department of Trade and Industry/Business Innovation and Skills, 2006, 2008, 2010

no malicious intent but it may have significant consequences well beyond the immediate environment of the individual. Even shocks that can trigger appropriate emotions at one time may be relatively short lasting. For example, would-be Liverpool football club spectators who wanted to break into the Champions League final against AC Milan (23 May 2007¹¹⁷) where a lack of available tickets had led to their exclusion from the ground. The emotions governing their desire to see the game overcame their appreciation of what had happened at a match between Liverpool and Nottingham Forest when 96 people died after supporters tried to enter an already overcrowded stadium (15 April 1989¹¹⁸). The challenge is to maintain an awareness of the risks to many when individuals distance themselves from the consequences of their actions. Information systems not only need to provide opportunity to share and transform information they also need to remind users of the outcomes of their actions of using the system. For example, what consideration do people give to the consequences of publishing holiday photographs or personal information on a 'Web 2.0' social network (House of Lords, 2007) and how much thought does a user give to continuing e-mail correspondence using the 'Reply-to-All' function? At the other extreme, how many are prevented from making decisions or taking actions which would be unlikely to lead to a risk being realised? There is a tendency for overcompensating day-to-day; to become obsessed with the high impact, low probability risk. For a comprehensive approach, sensitivity to the *weltanschauung* of the stakeholder is required as it has been observed: risk is in the eye of the beholder. This spectrum of 'risk attitude' is shown in the diagram by David Hillson and Ruth Murray-Webster (*Figure 22*).

¹¹⁷ <http://news.bbc.co.uk/sport1/hi/football/europe/6669039.stm>

¹¹⁸ <http://news.bbc.co.uk/1/hi/uk/7992845.stm>

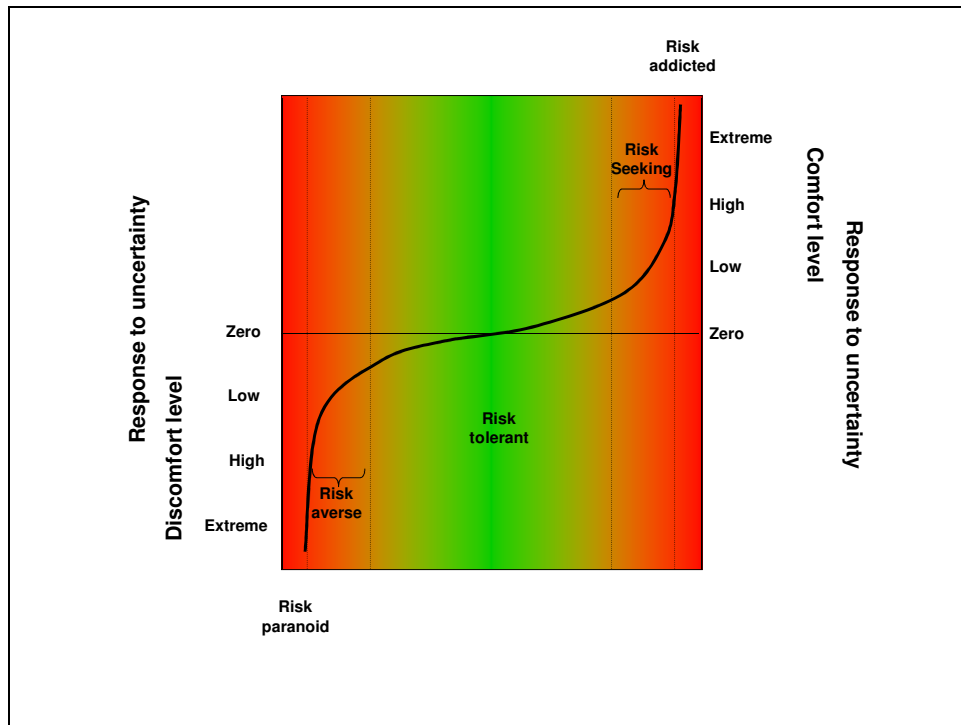


Figure 22: The risk attitude spectrum (Hillson and Murray-Webster, 2007)

I considered the general concept of risk from the two aspects of how risks may be categorised and whether there was a model that described how one might react to risks which determined how acceptable (that is, the level of acceptability) a risk, or a group of risks, may be? Risk acceptance, the decision to accept a risk, depends on risk criteria (PD ISO/IEC Guide 73:2002). No differentiation was made between risk and the causes of risk. I considered the general concept of risk according to two aspects: how risks may be categorised, and a model that describes how the reaction to risk determines how acceptable a risk, or a group of risks, may be. The decision to accept a risk depends on risk criteria. The categorisation of risk was based on CMU SEI's taxonomy (Carr, Konda, et al., 2003), which describes risks as having one of three characteristics: **known risks** that are well understood and will surface time after time in a risk assessment; **unknown risks** that did not make it into the risk register because the assessment did not call on the right kind of expertise; and **unknowable risks** that could not have been reasonably predicted even with a wide enough representation from the contemporary knowledge base. These characteristics may be represented in a quadrant (Figure 23) to show the direction risk assessment should take to dredge up as many risks as honest governance drives^{119 120}. For example, the risks of

¹¹⁹ Initially being concerned with capturing any risk without considering likelihood or impact - quantitative rather than qualitative analysis. I use the term 'honest' to suggest a degree of risk literacy where risks – however distracting – are not ignored to get the desired result from a risk assessment.

¹²⁰ For example, the risks of placing transient content onto social networking websites (http://news.bbc.co.uk/1/hi/uk_politics/6929161.stm, 03 August 2007) may result in advertisements

placing transient content onto websites may result in advertisements (for example) appearing with other material with which the advertisers do not want to be associated. Assessing such risk calls for the knowledge of the content owners that such a technology is available and could be used and for them to define what is acceptable to them and to the website designers and programmers to recognise where constraints can or cannot be made. It may be an instance where a risk is accepted or the facility rejected on account of the risk. An extrapolation of this example is the lack of control afforded to an advertiser placing adverts on a social networking site and the freedom of users to define content outside the close control of the website¹²¹.

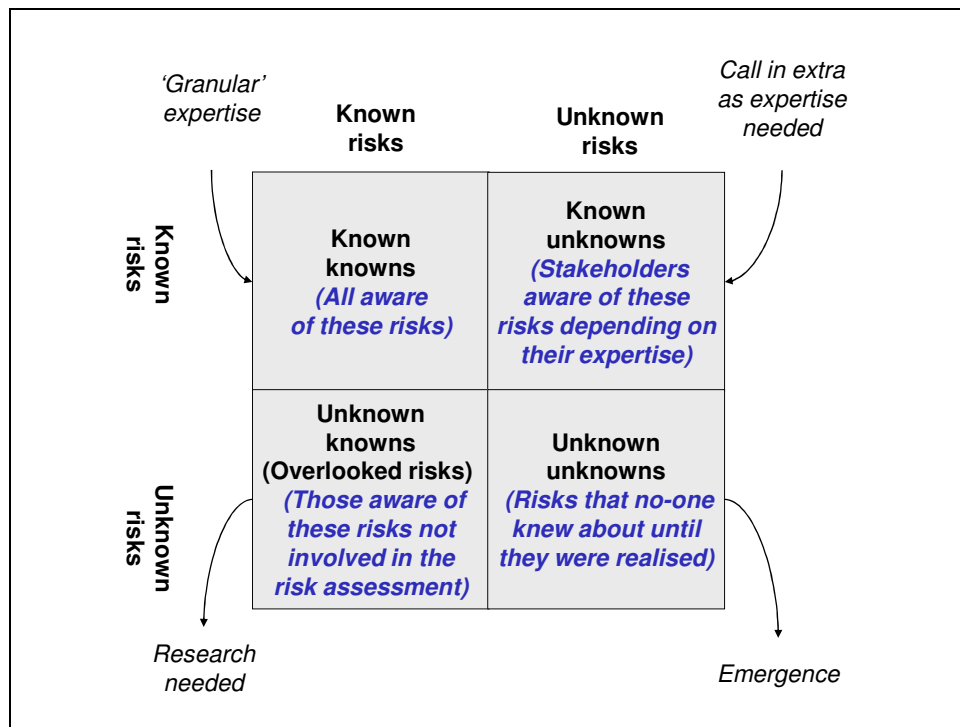


Figure 23: Risk criteria

I looked at how the prevalence of a type of risk may be considered during an assessment of an appetite for risk and suggested that the link between the type of risk and its acceptability is the trust engendered by how well that risk is treated. That is to say that there is no requirement to go to the extremes of being complacent about the risk or calling a halt to any activity which may be affected by the realisation of that risk; some pragmatic, affordable precautions can usually be taken. The risk is recognised but so is a treatment that has a reasonable risk of successfully treating it. Risk treatment is the application of one or more

appearing with other material with which the advertisers do not want to be associated. Assessing such risk calls for the knowledge of the content owners to define what is acceptable to them and to the website designers and programmers to recognise where constraints can or cannot be made. It may be an instance where a risk is accepted or the facility rejected on account of the risk.

¹²¹ http://news.bbc.co.uk/1/hi/uk_politics/6929161.stm, 08 August 2007

risk countermeasures that reduce that risk to an acceptable level. These may include prevention (to stop the realisation of the risk), reduction (to reduce the effect when it occurs), transference (make the *treatment* someone else's problem – for example, outsourcing), and contingency (where you must be ready to do something if it happens). Acceptance is reached when you decide that you have done enough so that you can live with the residual risk. Observing that the risk countermeasures could be described separately in this way, I mimicked the layer models of telecommunications and information technology networks (Figure 24 and Figure 25) that identify how two communicating entities may transfer information and created a tiered model of risk acceptability that may show where two entities who want to work together without risk contagion can do so with some confidence. My model for the reaction of risk and its level of acceptability is the balance of risk appetite (represented by the controls within an organisation or community) and the risk attitude of the individuals – how much, and in what way do they feel responsible for protecting the information they deal with.

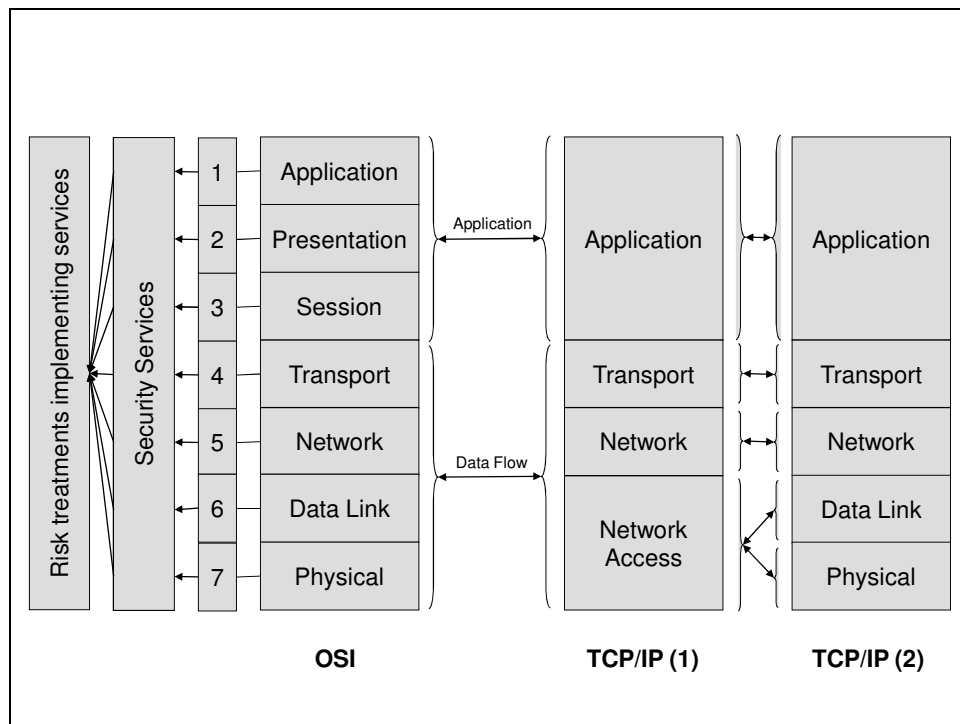


Figure 24: Communications models

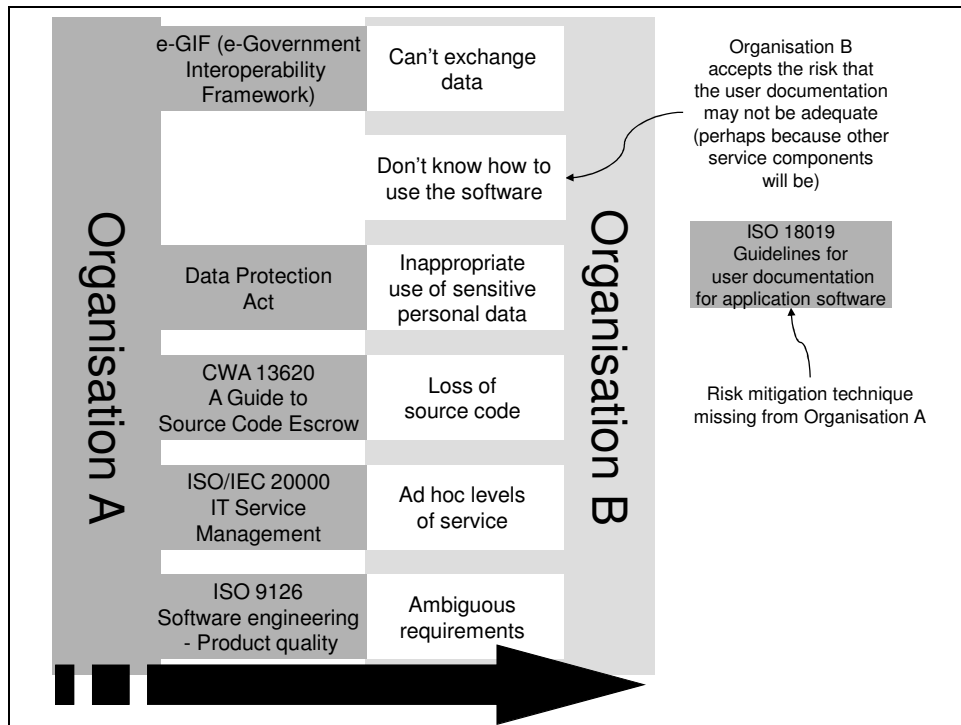


Figure 25: Creating a zone of common acceptance using standards to treat risks

This is an extension of the Taxonomy-Based Risk Identification archetype and it also builds on a tripartite model of core (or fixed) risks, interactive risk, and emergent risk. Core or fixed risks, as with the SEI model, are the known risks which are those that one or more personnel are aware of – if not explicitly – as risks, at least as concerns. For the individual, these are from your *weltanschauung*. For example, if you are interested in telecommunications then you are focused on telecoms risks; if you are not, then you are lacking in your profession¹²². Professional knowledge of the risks in information technology may, for example, raise the potential problems related to the integrity of data input. When core or fixed risks are dredged up, stakeholders are siloed and are likely to have a degree of confidence that complexity can be managed because there are more 1:1 risks and treatments relationships. Clearer treatment should lead to trust.

Interactive risks are similar to the unknown risks of the SEI model. They are those risks that would surface (that is, become known) if personnel were given the right opportunity, cues, and information. These are less likely than core or fixed risks. They are predicted by the cooperation of different disciplines. For example, will technology affect the process it is meant to ease? Or by allowing for both the physical and environmental considerations for IT,

¹²² The first draft of the Catalogue of Publicly Available Information Assurance Guidance (Project γ ; *Chapter 3*) was criticised for being too focused on Information Technology at the expense of guidance pertaining to telecommunications. The response to this criticism was to include telecommunications standards in the revised catalogue but to justify its predecessor on the basis that it had been commissioned knowingly from The National Computing Centre and so an 'IT bias' was to be expected.

stakeholders are together but working with less confidence because of the increased complexity. Known unknowns are registered when the right disciplines come together. Unknown knowns remain uncovered by not including a wide enough set of expertise. There are more many-to-many risks and treatment relationships. Trust depends on the complexity of risks and treatments that need to be put in place.

The third type of risk is the emergent risk that is equivalent to SEI's unknowable risks. These are the risks that, even in principle, none could foresee. Hence these risks – the management of which are potentially critical to success – are beyond the prediction of any risk identification method. Their unpredictability may be the result of the interaction between several 'core or fixed' risks and/or 'interactive risks'. That is, this may not be the result of something new but rather combinations of 'known' risks. Similarly these may result from the unplanned effects of risk treatments or a combination of risk treatments.

Consideration of the prevalence of a type of risk during an assessment of risk appetite brings out a link between the type of risk and its acceptability in the trust engendered by how well that risk is treated.

The objective of this research was to determine whether the attitudes of individuals to risk may be usefully correlated to the acceptable level of risk that is expected by the 'risk culture' in which they work. Knowing this to be true, and how so, is a foundation for understanding what training, improved awareness, or other mechanisms (namely applying standards as regulators (Beer, 1993) or controls) are needed for changes in risk culture or to maintain a current, appropriate risk culture. This was to be tested by creating a scale of measurement for attitudes to risk. A questionnaire was constructed to determine where on the scale a user should be placed and whether they sit within, or outside, the attitude that is acceptable to the owner of the network. The creation and refinement of the questionnaire and the evaluation of the responses determines the application of the method as a practical tool to evaluate the appropriateness of implemented policies (or standards) for risk management in information systems. The feasibility study was organised into 8 stages:

Stage	Activity	Description	Stage Deliverable(s)
1	Acquisition of data	Acquire a database of risk and treatment as a body of knowledge from which to derive <i>bona fida</i> experience of risk and loss from exposure to human vulnerabilities.	Body of knowledge about risk and treatment on which to base the questionnaire.

Table 20: Research stages for the human vulnerabilities detection methodology

Stage	Activity	Description	Stage Deliverable(s)
2	Questionnaire design	Analyse the database to create a way of gauging user reactions to risks and treatments. The levelled answers would build up a picture of the users' sensitivity to risk and loss in information systems.	Questionnaire for structured user engagement and on-line to measure attitude to risk relative to the organisational culture.
3	Design analysis method	Use the NCC Survey of the 'Top Ten IS/IT Risks' to design the outline ranking scale that could indicate the measures of human vulnerability within information systems.	Ranking scale with which responses will be analysed.
4	User engagement	Deploy the questionnaire (<i>Figure 27</i>) with a sample of 'network' (system) stakeholders around the UK, from the wide membership of The National Computing Centre.	Completed user questionnaires.
5	Collate the results	Collate results to create a body of knowledge to test the premise that the level of risk culture can be detected and improved if necessary, and that 'weak links' may be identified for tailored attention.	Collated results ready for analysis.
6	Evaluate the results	Compare the results with the ranking scale developed during stage 3. Look for patterns to inject the necessary controls, training, or awareness campaigns, check the effectiveness of the campaigns, and take remedial action for further improvement.	Algorithm or formula which would show the relative risk that users pose.
7	Design a tool to identify Human Vulnerabilities	Use the evaluation and the knowledge to design a sustainable tool.	High level programme and tool design specification.

Table 20: Research stages for the human vulnerabilities detection methodology			
Stage	Activity	Description	Stage Deliverable(s)
8	Develop feasibility report	Prepare and deliver a report describing the findings of the research and confirming the feasibility of the developing tool.	Feasibility study report.

4.6 Application

4.6.1 Acquisition of data

The acquisition of data comprised assessing a corpus of security (Appendix A) research that connected realised risk to human vulnerabilities responsible for the loss, engineering questionnaires based on the experience recorded therein, and then using the questionnaires in interviews with the objective of validating a way to predict likely human vulnerabilities using the vectors recorded in that body of research. The literature considered the context in which people use information systems over networks which are expected to be secure and the recording of vulnerabilities caused by ignorance and deliberate acts¹²³.

To determine how to detect human vulnerabilities, this special literature survey – carried out in addition to the review described in Chapter 2 – was focused on the security expectations/context in which people use networked information systems. The literature was reviewed with the questions from Table 21 in mind.

Table 21: Project y literature review	
1	Is there a classification/taxonomy of human vulnerabilities?
2	What are the achievable aspirations for the method of detection?
3	Is it reasonable to look for vulnerabilities caused by (say) ignorance?
4	How can deliberate acts be predicted?

The collected research showed certain recurring characteristics in incidents that resulted from human vulnerabilities, particularly those branded by the label of ‘insider threat’.

¹²³ This relates to a Royal Holloway University of London (RHUL) psychology research project and may be an opportunity for some future collaboration. The RHUL Information Security Group programme is designed to investigate the human factor in online security threats. The investigation looks at Internet users' vulnerability to fraudulent schemes, viruses and hacking, as well helping to stop so much of the information theft that could so easily be avoided with the right knowledge.

In deliberation of the way that (say) a user may be 'marked down' as a risk because of their access to highly sensitive information, I sought to create a balance using 'normalising' factors. A 'happy' employee should not be branded as a risk by the questionnaire unless it points to (say) a significant likelihood of some accidental realisation of a risk with significant impact. Referring to the corpus (Appendix A) I selected 'risk vectors' to test for including the type of employment contract (for example, full or part time, contractors, partners, consultants, 'Temps', and even former employees) and the likelihood of layoff. Consideration was given to being in a high risk group¹²⁴ including any intrinsic risk in their role/position – particularly any paths to do bad things; how much is open to them? For example the threat from 'critical information technology insiders' (Shaw, Ruby and Post, 1998) such as computer professionals may be broken down into characteristics of: computer dependency, ethical 'flexibility', reduced loyalty, entitlement, and a lack of empathy¹²⁵. Excluded from the feasibility study – to enable a pragmatic limitation on the information to be analysed - but noted for future consideration were length of service and the greater psychological or temporal components including latent risk (related to the activity supported by the information system), the propensity to risk, and the variation in how people will behave.

Understanding who is a 'human vulnerability' may be important for the organisation as an entity. However, if the investigation and the application of the results are applied with insensitivity, then the effects on morale could be devastating. The importance of understanding that security awareness must form part of the induction to any information network community (which suggests that this technique may be applied to measure what needs to be done and suggest appropriate awareness measures to support the desired risk culture¹²⁶) was also noted. For example, allowing access to facilities that are not only unrequired but also dangerous suggests an abrogation of responsibility¹²⁷.

¹²⁴ For example, 86% of breaches caused by insiders were from holders of technical positions.

¹²⁵ Empathy is one of the five attributes of information system service provision established by The National Computing Centre's benchmarking special interest group [1996]. The five attributes are: Empathy – How caring and individualised is the attention from the IT practitioner?; Responsiveness – Does the IT practitioner provide a helpful, prompt service?; Reliability – Is the service from the IT practitioner reliable and accurate?; Assurance – Does the knowledge and courtesy of the IT practitioner staff instill customers with trust and confidence?; and, Tangibility – How do customers perceive the communications, appearance of IT equipment, related materials and the IT practitioner's competence and professionalism? (Grafton, Bytheway, and Edwards, 1997)

¹²⁶ I have recently applied the techniques in this chapter to assess the 'before' and 'after' status of delegates at information security awareness briefings. The results show the efficacy of the technique with an increase in the appreciation of the risks and the attention that users must pay to them in order to avoid them or reduce their impact.

¹²⁷ cf. Manufacturing cars that can travel at twice the highest legal speed limit! IT requirements elicitation studies may benefit from understanding why developers allow or include a feature just because it can be done.

A key 'rule' of the method was to recognise that 'opportunity makes a thief'¹²⁸. This was built into the questioning as a 'cold' policy to mean that anyone – absolutely anyone – who can access an information system will be tarred with some element of risk as to the damage they can do, or may be cajoled into doing. No intended character judgement is made – security is regulated by controls (BS ISO/IEC 27002:2005 BS 7799-1:2005). Although 'trust is not a control'¹²⁹ it will still be the basis for a final decision as to whether the security culture is balanced with the sociotechnical controls that manifest in security policies. Reliance on trust is dependent on ensuring that the security policy is neither excessive nor unfair with that trust being regulated by avoiding punishment and benefiting from reward (Flechais, Riegelsberger, Sasse 2005). The approach to promoting the security culture varies with the extent to which the organisation must go to make the recognised security practices that are encapsulated in standards part of its *modus operandi*. The activities around this promotion will be governed by the organisation's idiosyncrasies (Figure 11).

The formulation of the initial questions considered the granularity of the component vectors (and the completeness of the set of vectors) and derived the scoring mechanism to take into account competing/conflicting vectors so that being 'tarred' with one risk vector may allow you to recoup ground if not 'tarred' with another. That is, I recognised how the interdependencies of risk combine to increase the potential impact. The impact definitions of data type\from NIST SP 800-60 [2004] and the GIPSI¹³⁰ catalogue/table were considered for this. For example, does the target of the evaluation have access to trade secrets, human resource information, or significant financial information? However, a balance was sought using 'normalising' factors. A 'happy' employee should not be branded with a risk label from the questionnaire unless the answers point to (say) the likelihood of some accidental realisation of risk.

Much useful information and points of focus were extrapolated from the research literature associating realised risks with those responsible. For example, is an information system user disgruntled with the network owners or perhaps the network itself? And does the user have good potential to deliver the work required but is a risk because of poor supervision? Vulnerability vectors were isolated from the literature, working on the assumption that the more vectors examined, the greater predictive accuracy the method would have. A selection of vectors was compiled into questions for the one-to-one interviews and (in less detail) for

¹²⁸ Francis Bacon

¹²⁹ Gerry O'Neill, former head of information security risk for Barclays Bank plc and Emeritus Chief Executive Officer of the Institute of Information Security Professionals

¹³⁰ General Information Assurance Products and Services Initiative (GIPSI). These became the Business Impact Tables of *HMG IA Standard No. 1, Technical Risk Assessment*, jointly published by CESG (The National Technical Authority for Information Assurance) and the Cabinet Office.

the on-line 'rapid' survey¹³¹. The method was challenged not to become a vulnerability itself by promoting the overall balance between organisational and individual attitudes and appetites for risk that may hide the detail of a specific risk vector. This can be seen by the clusters of similar, overall results from this study's aggregated results from very different component scores (Figure 30). Part of the challenge in extracting a sensible set of risk vectors was a focus of the body of research on deliberate acts¹³². The papers were scrutinised to identify risks realised through non-deliberate action too as a balance. Vulnerability vectors included a categorisation of the type of person interacting with the information system, the availability to that person of a path to realise a risk (such as access to confidential information or the ability to damage required operating capacity of a network), and the attitude to risk of the individual. These may include (for example), threat-pair vulnerabilities (as defined in Stoneburner, Goguen, and Feringa 2002, Table 3-2) or potential disgruntlement at not being allowed (say) to use company equipment for personal downloads.

The method was designed to complement the technical and quasi-technical countermeasures deployed for use against well known outsider threats such as hackers or the malicious software of criminal programmers. Technical measures would include intrusion detection and prevention systems, antivirus or spyware detection and removal programs and firewalls (both hardware and software). Quasi-technical measures comprise a technical implementation which may, for example, use technology to distract a criminal from gaining inappropriate access to a computer network such a honeypot which may imitate a legitimate network or part of a network with otherwise redundant information stored thereon. The common characteristics were isolated and are represented by the formula in Figure 26 which is explained below:

<p>Vulnerability = Environmental circumstances + Personal circumstance + Path(s) + ICT literacy + Risk literacy + Emotional literacy</p> <p>Where</p> <p>Risk Literacy = Knowledge of risk + Knowledge of treatment + Willingness to deploy treatment</p>

Figure 26: Calculating the depth of a human vulnerability in an information system

¹³¹ A rapid survey is a web-based questionnaire methodology used by the National Computing Centre. Each survey is developed by a team comprising a market analyst, web developer and marketing representatives, and subject matter expert. The on-line survey was used to complement the in-depth interviews because of the quality of information gathered in previous on-line surveys – in particular *Risk Management in IT* (2003) and *The Security and Information Risk Survey* (2007).

¹³² For example, the vulnerability markers identified by Cappelli, Moore, and Trzeciak, 2005.

The context in which a type of person or organisational role is assessed for being a human vulnerability has the two aspects of environmental circumstances of where they use information systems (often a workplace), and a set of personal circumstances or profile. The environmental circumstances were considered in the questions (and the rules designed to evaluate the results) by taking into account the environment and context in which an individual is operating. The method recognises that where a user engages with a network, the context of use will depend on the profile of the user in terms of their ICT skills, the tasks that the user expects, or is expected, to achieve¹³³, the equipment such as hardware or software that gives the user access, the physical and social environments in which engagement takes place, and the stability of the organisation in terms of its existence or propensity for change.

4.6.2 Questionnaire design

The challenge of the questionnaire was to make it practical to use whilst covering a broad enough range of risks and risk treatments to be meaningful. There was also a challenge to restrain any bias in the questions by leading the interviewees or survey respondents to give an answer that they felt was the one that was wanted rather than the reflection of risk appetite or attitude no matter how inappropriate to circumstance.

To effect this independence, the questions were formulated without referring directly to the subject areas, covering the undisclosed topics of authentication, authorisation, availability, confidentiality, integrity, non-repudiation, and trust. Anecdotal feedback from NCC workshops¹³⁴ in information security management suggested that security induces more cognition and comprehension when it is presented as its three components of confidentiality, integrity and availability – particularly the latter where it can be positioned as an enabler rather than a constraint. The attitudes to examples of these components were used to test directly the individual attitudes to risk in the questions (see Table 22).

A two-part questionnaire was compiled as a prototype of what an on-line analysis of risk appetite and attitude might comprise. Questions were divided into 'Measuring organisational/community appetite', and 'Testing personal attitude to risk'. These were reduced to two questions (with subparts) for the on-line survey to ensure that it could be completed quickly.

¹³³ For example, appropriate risk taking for a private individual accessing personal e-mail with a mobile device is not likely to be appropriate for another user engaging with a network managing a safety-critical SCADA system. However, common areas that would secure the use of both would appear in the attitude tests for all users.

¹³⁴ Including 3 October 2002, 8 February 2005, 22 March 2006 and 6 June 2007. The first three dates were open workshops; the fourth date was a private activity for one of the interviewees of this feasibility project

There were two types of question in these two categories: contextual questions to put a set of the responses into perspective, and questions where responses can be scored to give a comparative basis for the evaluation of the questions on risk appetite (the organisation or community) or risk attitude (the individuals). In the on-line survey, questions about the organisations' risk appetites were designed to have single answers rather than the two-part questions of the in-depth interviews¹³⁵.

To understand the organisational (or community) appetite for risk, the following contextual question was asked in the interviews to see if knowledge of the individual made a difference in corporate decision making. *If you had a staff member who you knew to have experienced/is experiencing the following, would you alter how they were managed? (For example, restrict access capabilities, or monitor their use of the network more closely.)* With the examples being staff who had 'Missed a promotion, salary rise, project, or opportunity of interest', 'Is/has been a candidate for redundancy', and 'Is "stable" in his/her personal life' This created a bridgehead between the organisational appetite and individual attitude.

To enhance the understanding of the organisation in relation to its experience of information security, the questionnaire asked other contextual information in the interviews:

- Has your organisation experienced an information/information system security breach in the last 12 to 18 months? (Yes/No)
- If an information security breach was experienced, was it malware infection, staff misuse, attacks or hacks into unauthorised areas, theft or fraud involving computers, systems failure or data corruption?

The answers to these questions were of particular interest as a test to an underlying assumption that a high proportion of organisations would have had risks realised as security breaches (DTI/Price Waterhouse Coopers, 2006). An organisation which reported itself to be free of security breaches was probably not sufficiently aware of its situation or wanted to deliberately withhold information for fear of embarrassment. One organisation turned down the request to take part in the interviews for fear of the latter.

An additional question was added for the end of the interviews to investigate if the organisation's perception of risk to its information systems increased or decreased as a result of the security incidents discussed during the interview and those which had been prevalent in the news at the time¹³⁶. Interviewees were asked if their awareness of risk

¹³⁵ For example, the in-depth interview would ask about the content of a policy and then consider the quality of that policy's implementation. An interviewee could record the existence of a policy and the effectiveness of its implementation. The rapid survey would record the content of the policy and its effectiveness would be implied by detail in the option selected.

¹³⁶ Such as a building society being fined £980,000 for a laptop theft, the 'hacking' of TKJ (TK Maxx) and the theft of 45 million credit card records, or the result of storms in the UK (January '07) which led to deaths and travel disruption? (It was with a certain sense of irony that this prototyping of the

increased, decreased, or had not changed. A fourth option, 'Time to reconsider our exposure' was allowed too.

Two opportunities were given to interviewees to answer the scored questions: each interviewee was asked how they thought the analysed member of staff would feel if certain risks, and their effect on the organisation, were realised (Table 22) with the responses tabulated (Table 23). If the respondent could not answer for an individual but could talk generally about staff, the same set of questions was asked in that context¹³⁷. The interviewer was recommended to consider asking these too if time allowed after answering the questions about a specific individual.¹³⁸

Perhaps the most significant component of the questioning was not related directly to the quality of an organisation's security policies (perceived or thoroughly implemented). The method built on other methods such as the historical survey (DTI/Price Waterhouse Coopers, 2006) or preparing a semi-predictive state of readiness to handle information securely¹³⁹. This component is the approach to risk that an individual may take when faced with a particular problem. For example, how likely is a user to e-mail confidential information to the wrong person? Would they rely on the corporate back-ups or proliferate uncontrolled information that is stored 'just in case'? The examples considered are shown in Table 22 and the response set for analysis is shown in Table 23.

method took place during the July floods of 2007 which presented the realisation of a major risk to information systems whose data centres were inundated.)

¹³⁷ With the same scoring template applied to the responses.

¹³⁸ Time did not allow for this but one of the interviewees who completed the questions directly onto the interview sheets included answers for both.

¹³⁹ Such as HMG Infosec Standards 1, 2, and 6, and BS ISO/IEC 27001:2005 BS 7799-2:2005.

Table 22: Questions of attitude

Example of a security issue:	Component of security at risk:
Confidential e-mail might be sent to the wrong person/people	Confidentiality
IT equipment is exposed to coffee spills, knocks and drops.	Availability
Data typed in on one day cannot be easily restored from a back up if lost.	Integrity
Security awareness suggests that measures are common sense measures and don't need to be mandated.	Trust
Cables may be unplugged and moved and new cables plugged in to get on with work quickly.	Availability
Pen drives (USB sticks) are convenient, efficient and made secure by their removability.	Confidentiality
Legal documents are better provided in hard copy because the legal admissibility of e-mail is doubtful.	Non-repudiation
Our organisation gives access to all the IT equipment and files that you need.	Authorisation
Users may share logon details if it helps job-sharing or simplifies processes for the organisation.	Authentication
A tested plan minimises the impact of a serious incident, e.g. a fire, storms, loss of key staff.	Availability
Information about our customers can be shared with our partners and contractors.	Trust

With the following options for responses:

Table 23: Attitudes to risk	
Attitude	Interpretation
Threatened	'Here's a risk that the user ought to keep an eye open for.' That is, feeling threatened can be positive; it encourages awareness. It should not, however, be an inhibitor to efficiency.
Unfamiliar	If they don't know about it they won't take any deliberate action to reduce the risk.
Uncommitted	They know about the risk but don't think about it. Perhaps they feel it's not their problem.
Comfortable	They know about the risk but make a deliberate decision to accept it without treatment on their part ¹⁴⁰ .

¹⁴⁰ Which may be a reasonable response for those with adequate trust in their environment's information security management system.

4.6.3 Analysis method

Each response to a question had a numerical score associated with it – a value that represents the risk that that vector exposes the information system to. These scores are shown below in Table 24 and Table 26 with reasoning for the scores in particular cells explained as footnotes. The higher the score allocated, the higher the perceived risk. For example, it was deemed riskier to have no policy for the use of personal ICT than to have a documented policy restricting its use. The judgements on what may or may not be the better practice were based on the catalogue of recommended risk treatments in BS ISO/IEC 27002:2005 BS 7799-1:2005. A response to a question describes the quality of risk treatment in the organisation. Each reply is given an initial score ranging from 0 (representing no significant risk) to 3 (representing the most significant risk). That initial score is adjusted according to the quality of the countermeasure in place to treat the risk. It is increased if the countermeasure does not meet the expectations of BS ISO/IEC 27002:2005 BS 7799-1:2005. It is then weighted for significance according to the ranking of the 'Top 10 IS/IT Risks' (NCC, 2005). The scores are based on the assumptions that having a good, documented policy is a risk treatment and so protects the organisation from risk; a maturing information security management system (ISMS) suggests less risk than an organisation in and an 'Initial' or 'Ad hoc' state of maturity (Crosby, 1979); a higher score indicates less control of risk and hence a greater appetite for *known* risk (assumed from the greater exposure they leave themselves open to). In this model, appetite for risk may be *involuntary* because it is measured not on perception or feeling but rather evidence that acceptable risk controls are in place – a low score suggest that the organisation has deliberately or coincidentally implemented significant controls from BS ISO/IEC 27002:2005 BS 7799-1:2005 – and as a result has satisfied a lesser appetite for known risk.

Table 24: Application of scores to answers about their organisations/communities

Topic		Contribution to appetite	Tested statement or question	Responses ¹⁴¹								
Classified by Top 10 number	Accounting for the Top 10 ranking factor			A: This is the risk 'value' or 'factor' ¹⁴²				B: ¹⁴³ Information security management maturity (How established is the policy in the organisation?)				
				Yes	Sometimes	No	Don't know	Documented, communicated and audited	Documented, not followed up	Documented but not followed up	Implied	No policy
Organisational context/ Environmental circumstance	N/A	A	The organisation is undergoing, likely to undergo, or may be rumoured to be undergoing some merger or acquisition or internal reorganisation.	3	2	0	2	N/A	N/A	N/A	N/A	N/A
Organisational context/ Environmental circumstance	6	B*18	Information risk is regularly addressed ¹⁴⁴ in projects, operations/IT service delivery, and at board level.	1	2	3	2	A/4	A/3	A/2	A	

¹⁴¹ Scores are awarded/ranked according how the answers fall into the top 10 categories. For example, if staff may change their PC configurations, risk 3 is exposed.

The organisation's attitude to risk is apparent by the 'Hardness' of their Policy Set.

¹⁴² Does the organisation/community take the approach of 'laissez faire' or lock down?

¹⁴³ 'B' is the risk 'value' or 'factor' 'A' adjusted for ISMS maturity

¹⁴⁴ 'addressed' means that there is some form of risk assessment and an implemented plan to treat the risks that are not acceptable to the organisation.

Table 24: Application of scores to answers about their organisations/communities

Topic		Contribution to appetite	Tested statement or question	Responses ¹⁴¹							
Classified by Top 10 number		Accounting for the Top 10 ranking factor		A: This is the risk 'value' or 'factor' ¹⁴²				B: ¹⁴³ Information security management maturity (How established is the policy in the organisation?)			
				Yes	Sometimes	No	Don't know	Documented, communicated and audited	Documented, not followed up	Implied	No policy
Path	3	B*23	Staff may use their own IT equipment for business use (PCs, telephones, PDAs, USB sticks/pen drives)	3	3 ¹⁴⁵	1	2	A*4	A*4	A*4	A*4 ^{146 147}
								A*4	A/3	A/2	A
Path, motive, system role	1	B*28	Staff are screened for background, qualifications, during selection and during changes of employment and their access to information tailored accordingly. ¹⁴⁸	1	2	3	2	A/4	A/3	A/2	A

¹⁴⁵ Because any usage is a risk

¹⁴⁶ It won't matter if there is no policy because it's a bad thing; will some infer better practice? (A positive risk.)

¹⁴⁷ A bad policy that can't be scored less just because it's documented.

¹⁴⁸ Does the interviewee know that there's a British Standard for screening staff (BS7858:2006)? What if an animal rights campaigner works for a furniture company? Not a significant issue but if that company made lab equipment...?

Table 24: Application of scores to answers about their organisations/communities

Topic		Contribution to appetite	Tested statement or question	Responses ¹⁴¹								
Classified by Top 10 number	Accounting for the Top 10 ranking factor			A: This is the risk 'value' or 'factor' ¹⁴²								
				B: ¹⁴³ Information security management maturity (How established is the policy in the organisation?)								
				Yes	Sometimes	No	Don't know	Documented, communicated and audited	Documented, not followed up	Documented but not followed up	Implied	No policy
ICT/systems Literacy	3 ¹⁴⁹	B*23	Staff have their work monitored for accuracy for a period until competency through experience is assured or other validation mechanism is deemed sufficient.	1	2	3	2	A/4	A/3	A/2	A	
Path, process	3	B*23	Alterations to how company equipment is set up can only been done through qualified staff.	1	2	3	2	A/4	A/3	A/2	A	

What if a trusted employee had financial problems and access to company resources which could be sold to alleviate them?

¹⁴⁹ A sound selection process is an established defence which may be undermined by not carrying that care through into the induction processes.

Table 25 introduces a measure of the caution an organisation may or may not have, to individuals who may have their emotional response to risk affected by corporate or personal circumstances and asks how – if at all – do respondents adjust their behaviour to others who may become vulnerabilities.

Table 25: Adjustment of risk treatment to account for behaviour.								
Management of destabilising activity	If you had a staff member who you knew to have experienced/ is experiencing the following, would you alter how they were managed?(for example, restrict access capabilities, monitor their use of the network more closely)							
	A ¹⁵⁰ Laissez faire or lock down?				B ¹⁵¹ Information security management maturity (How established is the policy in the organisation?)			
	Yes	Sometimes	No	Don't know	and audited and communicated Documented, followed up but not Documented	Documented	Implied	No policy
	Missed a promotion, salary rise, project or opportunity of interest?							
Is/has been a candidate for redundancy?								
Is your staff member's personal life 'stable'?								

With the methodology set to measure the organisation's risk environment, the second axis of the evaluation was designed to test the personal attitude of an individual to risk. For administrative purposes, the affiliation of the people associated with breaches in an organisation could be identified by organisation and subject identifier so this traceability was removed at the earliest part of the processing to assure confidentiality.

¹⁵⁰ This the risk 'value' or 'factor'

¹⁵¹ This the risk 'value' or 'factor' adjusted for ISMS maturity

The types of security issues experienced by the organisation was questioned but respondents were asked to limit their experiences to a 12 to 18 month period which would increase the likelihood of more accurate remembrance and keep all interviewees talking about the same time period to suggest a similar potential exposure to the prevalent risks. This was in keeping with the Top 10 IS/IT Risks survey (Chapter 3) which was used for weighting responses. This survey gave a heavier weighting to risks that had been experienced directly over risks which were of concern because of the reports of others.

Having established the context of the information system in use, the questions focus on profiling the individual using attributes of those individuals recorded in the literature as to whether they have a greater or lesser propensity for being the source of a realised risk.

Table 26: Analysis of an individual

Components of risk	Situations are scored according to the exposure or likely vulnerability recorded. This is derived from research literature (for example, more paths, more technical expertise is where insider/human threats/vulnerabilities are realised).	Yes	Sometimes/partially	No	Don't know (Knowledge gap)
		3	2	0	1
Path/ opportunity to bypass path ¹⁵²	Would you rate your staff member's ICT technical skills as high?	3	2	0	1
	Does your staff member have day-to-day access to sensitive/confidential information?	3	2	0	1
	Is your staff member able to affect the integrity of information?	3	2	0	1
	Can your staff member affect availability of information assets to others?				
	Hardware?	3	2	0	1
	Operating system(s)?	3	2	0	1
	Application(s)?	3	2	0	1
	Data(s)?	3	2	0	1
Attachment to organisation	Is your staff member a shareholder?	1		3	2
	Is your staff member a full/part-time employee?	1		3	2
	Is your staff member a contractor, partner, temporary staff?	3		1	2
	Does your staff member receive pension fund contributions or other significant benefits from the organisation?	1	2	3	2
	Are you describing a former employee?	3		0	
Compliance	Has your staff member been involved with any non-compliances with organisational processes raised by internal audit?	3	2	1	2
	Is your staff member familiar with your 'Data Protection Act' responsibilities?	1	2	3	2
	Can you be totally sure that all the software your staff member uses has corresponding licences?	1	2	3	2
Knowledge	If you don't know the answers to the above, why don't you know? ¹⁵³				

The aim – and resulting complexity in the analysis – is the adjustment for policies where these policies are known (and whether they are implemented). For example USB sticks may not be a threat because there are no working 'ports' to connect them to, or because the data

¹⁵² An example comparison: if the risk appetite is low or 'OK' then high skills may be less of a threat than low skills in an organisation where the risk appetite is high (that is, fewer controls).

¹⁵³ Asked so that the researcher can consider if the response 'colours' the 'Don't know/Knowledge Gap' factor.

held are not confidential, or the malware countermeasures are strong enough to prevent programs uploading from portable devices.

Table 27: Scores for Table 30		
	'Free thought' or policy status unknown	Managed by policy ¹⁵⁴
Threatened	1	3
Unfamiliar	2	1
Uncommitted	2	2
Comfortable	3	1 ¹⁵⁵

In the on-line survey where there is no interviewer to intervene with further in-depth questions, the methodology considers a 'grey scale' where a policy is in place but enforcement of that policy may not be strong. So, to use the USB example, caution may still be required with an element of trust. For example, trust that malware prevention is up to date **or** that all USB ports are disabled. Then, **who** are you feeling worried about – your own misuse or that of others? If an area of risk is managed by a strong, followed up policy, the actor or customer in the information system shouldn't feel threatened.

¹⁵⁴ Therefore shouldn't feel threatened – don't allow one's performance to be impaired by 'unnecessary' worry.

¹⁵⁵ The subject of the evaluation should have some risk awareness to avoid carrying (say, information) out of the safe zone.

Table 28: Explanation of scores for Table 27			
Scores¹⁵⁶	1	2	3
Threatened	Acceptable/good attitude without controls in place	Unacceptable attitude with controls in place ¹⁵⁷ (but not actually vulnerability).	Unacceptable attitude without controls in place.
Unfamiliar	Acceptable attitude with controls in place	Not a good attitude but with a hope of improvement – better that uncommitted	May suggest a decision to accept the risk 'without' care.
Uncommitted	Rarely acceptable. May be acceptable in a highly controlled environment with negligible risk		Likely to be a vulnerability of some sort – perhaps not in regard to the issue at hand.
Comfortable	This is good if there are tested controls in place [to manage risk]		This is bad if there are no controls in place [to manage risk]

¹⁵⁶ Higher scores suggest a less desirable situation.

¹⁵⁷ Higher (worse) score because although the risk is managed, one can assume that performance may be impaired by being unnecessarily concerned.

Table 29: Second party evaluation of the individual (scored for 'Free thought' or policy status unknown)							
Component of risk	How do think the analysed member of staff would feel if the following risks, and their effect on the organisation, were realised?¹⁵⁸	Threatened¹⁵⁹	Unfamiliar	Uncommitted	Comfortable	Top 10 Category	Top 10 Weight
Confidentiality	Confidential e-mail might be sent to the wrong person/people	1	2	2	3	6	18
Availability	IT equipment is exposed to coffee spills, knocks and drops.	1	2	2	3	5	20
Integrity	Data typed in on one day cannot be easily restored from a back up if lost.	1	2	2	3	5	20
Trust	Security awareness suggest that measures are common sense measures and don't need to be mandated.	1	2	2	3	6	18
Availability	Cables may be unplugged and moved and new cables plugged in to get on with work quickly.	1	2	2	3	3	23
Confidentiality	Pen drives (USB sticks) are convenient, efficient and made secure by their removability.	1	2	2	3	3	23
Non-repudiation	Legal documents are better provided in hard copy because the legal admissibility of e-mail is doubtful. ¹⁶⁰	1	2	2	3	2	26
Authorisation	Our organisation gives access to all the IT equipment and files that you need.	1	2	2	3	7	16
Authentication	Users may share logon details if it helps job-sharing or simplifies processes for the organisation.	1	2	2	3	7	16
Availability	A tested plan minimises the impact of a serious incident, e.g. a fire, storms, loss of key staff.	1	2	2	3	5	20
Trust	Information about our customers can be shared with our partners and contractors.	1	2	2	3	6	18

¹⁵⁸ See the following table if the respondent cannot answer for an individual but can talk generally about staff or members of the community who interact with the information system.

¹⁵⁹ This is trying to make an honest record considering how the likely attitude may affect the organisation; it is not meant to be Orwellian 'thought police' dictating how one should feel!

¹⁶⁰ This may be an area of high risk when secure IT systems remain safe whilst paper documents proliferate and are lost.

Table 30: Second party evaluation of individuals in general in the community or organisation (scored for 'Free thought' or policy status unknown)							
Component of risk	Do you think that your staff care about the following?¹⁶¹	Threatened	Unfamiliar	Uncommitted	Comfortable	Top 10 Category	Top 10 Weight
Confidentiality	Confidential e-mail might be sent to the wrong person/people	1	2	2	3	6	18
Availability	IT equipment is exposed to coffee spills, knocks and drops.	1	2	2	3	5	20
Integrity	Data typed in on one day cannot be easily restored from a back up if lost.	1	2	2	3	5	20
Trust	Security awareness suggest that measures are common sense measures and don't need to be mandated.	1	2	2	3	6	18
Availability	Cables may be unplugged and moved and new cables plugged in to get on with work quickly.	1	2	2	3	3	23
Confidentiality	Pen drives (USB sticks) are convenient, efficient and made secure by their removability.	1	2	2	3	3	23
Non-repudiation	Legal documents are better provided in hard copy because the legal admissibility of e-mail is doubtful.	1	2	2	3	2	26
Authorisation	Our organisation gives access to all the IT equipment and files that you need.	1	2	2	3	7	16
Authentication	Users may share logon details if it helps job-sharing or simplifies processes for the organisation.	1	2	2	3	7	16
Availability	A tested plan minimises the impact of a serious incident, e.g. a fire, storms, loss of key staff.	1	2	2	3	5	20
Trust	Information about our customers can be shared with our partners and contractors.	1	2	2	3	6	18

¹⁶¹ These are the questions to be followed if the respondent cannot answer for an individual but can talk generally about staff. If the questions about the individual were answered, interviewers were briefed to consider asking these too if time allowed.

And finally, the general questions to investigate the reaction of the interviewee to external events were asked.

Table 31: For consideration of how the appetite score of the organisation/community may be affected by the respondent¹⁶²					
Has your perception of risk to your information systems increased or decreased as a result of the following . . .		Increased	Decreased	No change	Time to reconsider our exposure
perception of risk	As a result of the security incident/breach involving the subject above?				
	As a result of any other security incident/breach in your organisation?				
	As a result of hearing of a laptop theft which led to Nationwide Building Society being fined £980,000?				
	As a result of the 'hacking' of TKJ (TK Maxx) and the theft of 45 million credit card records?				
	As a result of storms in the UK (January '07) which led to deaths and travel disruption?				

The responses to the on-line survey were similarly scored by assigning a rising scale of values depending on the risk associated with the lack of compliance with BS ISO/IEC 27002:2005 BS 7799-1:2005, weighted from the ranked categories of The National Computing Centre's Top 10 IS/IT risks (Table 32 and Table 33).

¹⁶² Originally included to provide deeper interest but not to contribute to the scoring.

Table 32: Scores for responses to the On-line survey analysis of an Organisation's appetite for risk								
							Model Appetite	
	communicated and audited	Documented, followed-up	Probably understood to be the company practice, but no written formal documentation	No policy/ Not our policy	Weight	Good	Bad	
Information risk is regularly addressed in projects, operations/IT service delivery, and at board level	0.25	0.33	0.5	3	18	4.5	54	
Staff may use their own IT equipment for business use (PCs, telephones, PDAs, USB sticks/pen drives)	0.25	0.33	0.5	3	23	5.75	69	
Staff are screened for background qualifications, during selection and during changes of employment and their access to information tailored accordingly.	0.25	0.33	0.5	3	28	7	84	
Staff have their work monitored for accuracy for a period until competency through experience is assured or another validation mechanism is deemed sufficient.	0.25	0.33	0.5	3	23	5.75	69	
Alterations to how company equipment is set up can only been done through qualified staff.	0.25	0.33	0.5	3	23	5.75	69	
							28.75	345

Table 33: Scores for responses to the On-line survey analysis of an individual's attitude to risk							
	Threatened	Unfamiliar	Uncommitted	Comfortable	Weight	Model Attitude	
						Good	Bad
Confidential e-mail might be sent to the wrong person/people	1	2	2	3	18	18	54
IT equipment is exposed to coffee spills, knocks and drops	1	2	2	3	20	20	60
Data typed in on one day cannot be easily restored from a back up if lost	1	2	2	3	20	20	60
Security awareness suggests that measures are common sense and don't need to be mandated	1	2	2	3	18	18	54
Cables may be unplugged and moved and new cables plugged in to get on with work quickly	1	2	2	3	23	23	69
Pen drives (USB sticks) are convenient, efficient and made secure by their removability	1	2	2	3	23	23	69
Legal documents are better provided in hard copy because the legal admissibility of e-mail is doubtful	1	2	2	3	26	26	78
Our organisation gives access to all the IT equipment and files that you need	1	2	2	3	16	16	48
Users may share logon details if it helps job-sharing or simplifies processes for the organisation	1	2	2	3	16	16	48
A tested plan minimises the impact of a serious incident, e.g. a fire, storms, loss of key staff	1	2	2	3	20	20	60
Information about our customers can be shared with our partners and contractors	1	2	2	3	18	18	54
						218	654

4.6.4 User engagement

User engagement – managed by the process recorded in Figure 27 – was seen to be an area of risk to the research itself in terms of consistency of results, particularly as it could be skewed by the participant's willingness (or unwillingness) to talk about examples of risk realisation that would be deemed personally embarrassing or embarrassing for the organisation. To manage this risk in the method, the interviews were carried out to this

method for consistency and using senior interviewers – rather than students – to build on the implied trust that ensues from dealing with a qualified individual. Where organisations who were invited to take part (in the in-depth interviews) but would not participate, is described below. The supplementary on-line questionnaire was posted on the website of The National Computing Centre. The questions were aimed to pick up on the end-user perspective of human vulnerabilities rather than the technical risks and to support the more comprehensive, in-depth interviews. Therefore, technical staff were treated as end-users and their technical skills accounted for in the vulnerability vectors that were investigated.

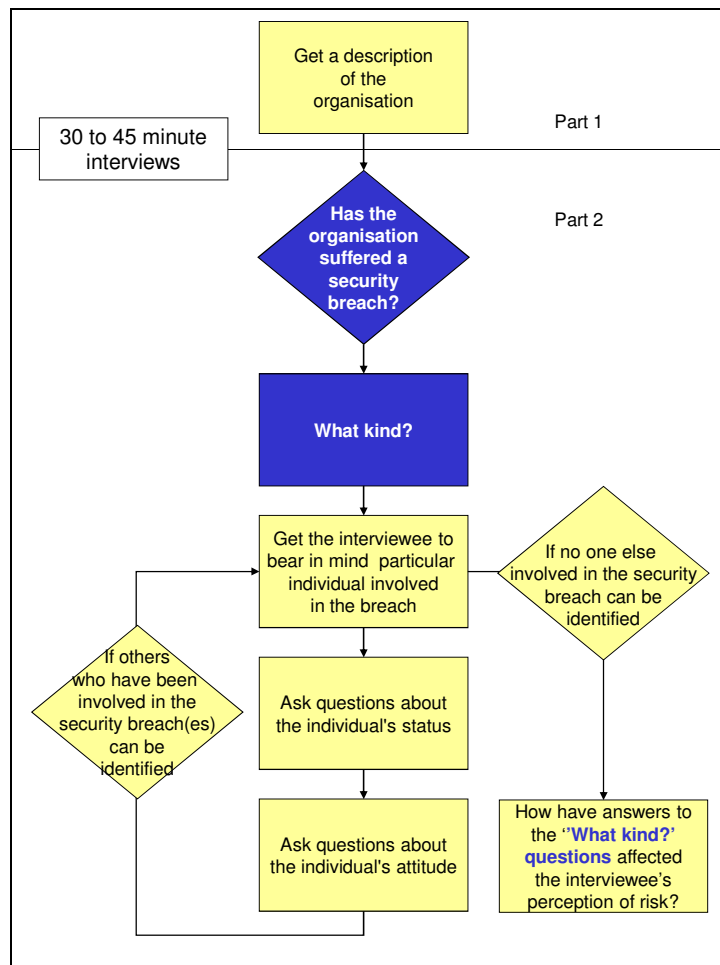


Figure 27: Interviewee engagement process

To scrutinise the type of individual whose risk appetite may affect an information system I selected the taxonomy of IS/IT roles used annually in The National Computing Centre benchmark of 'Salaries and Employment Trends in IT' (see Table 34). Because of the limited contact time with interviewees and the number of different roles that they would have to select from to describe the potential *human* vulnerabilities to be studied, the NCC benchmark model was simplified to IT management; those involved in systems analysis, design, development, and testing, user and technical support; IT operations/service delivery; and end-users.

Table 34: IS/IT roles			
Management	Systems Analysis and Development	User Support	Operations
Head of IT/IT Director	IT Consultant	Help Desk Team Leader	Senior Operator/Shift Leader
IT Manager	Project Leader/Senior Analyst	Help Desk Staff	Operator
Systems Development Manager	Systems Analyst	IT Trainer	Trainees
Operations/Data Centre Manager	Business Analyst	PC/User Support Analyst	Non-graduate IT Trainee
Network/Communications Manager	Senior Systems Developer	Technical Support Group	Graduate IT Trainee
User Support Manager	Systems Developer (over 3 years)	Senior Technical Support Staff	
Technical Support Manager	Systems Developer (under 3 years)	Technical Support Staff	
Client/Account Manager or Service Delivery Manager.	Systems Testing Engineer	Systems Administrator	
Contracts Manager		Database	
QA/Testing/Systems Change Manager		Controller/Administrator	
Project Manager		Web Administrator	
		Communications and Network Support Group	
		Network	
		Controller/Administrator	
		Network/Communications Analyst	
		Network/Communications Support Staff	
		Technician/Engineer	

Part of the inherent risk (sic!) of collecting information for this type of analysis is in the accuracy of the responses and hence the quality of information collected. *Table 35: Options for investigation*, shows how segregating the respondents considered the quality of information by providing some independent judgement. This control is centred on having someone profile the respondent to questionnaire first. This improves quality of the analysis of the responses based on the assumptions¹⁶³ that the supervisor and the individual will not collude, or that the response should not be an opportunity to transfer risk from supervisor to individual. (Again, quality assurance would expect the supervisor to undergo the same scrutiny¹⁶⁴.)

¹⁶³ That is, acceptable risk.

¹⁶⁴ Quis custodiet ipsos custodes – Who will keep watch over the guardians?

Table 35: Options for investigation				
Options	Questions answered by:			Relative quality of data expected¹⁶⁵
	(a) Questions about the Organisation	(b) Questions about general network users/ stakeholders	(c) Questions about specific individual(s)	
1	Supervisor/ Security or Risk officer	Supervisor/ Security or Risk officer	N/A	2
2	Supervisor/ Security or Risk officer	N/A	Supervisor/ Security or Risk officer	3
3	Supervisor/ Security or Risk officer	N/A	Specific individual	4
4	Supervisor/ Security or Risk officer	N/A	Profile information by the Supervisor, Security or Risk officer; Purely risk attitude questions by the specific individual	5

As the study was timebound, interviews were limited to the supervisory actor. There was not enough time to include more than one representative from each organisation.

The targets for evaluation were selected from the membership database of The National Computing Centre. Several 'direct marketing' e-mails were sent, supported with a more detailed article in NCC's *ITadviser* magazine. First priority was to contact respondents who expressed an interest following the e-mail campaign. After this first tranche was contacted, the types of organisation who had agreed to take part were reviewed and a list drawn up of industry sectors that were under-represented or where a second example may validate (or otherwise) the results of the first. Those identified in these first two tranches were then contacted by telephone for appointments.

4.6.5 Results

Telephone interviews lasted between 45 minutes and an hour (longer than the expected 30 to 45 minutes). Interviewees demonstrated a willingness to discuss their experiences in detail. The intentions of the research were discussed. Although the original plan was to

¹⁶⁵Ranked 1 = low, 5 = high.

conduct all the interviews by telephone, some of the interviewees preferred to complete the questionnaire documents themselves. This self-examination worked and well and acted as a prototype of the remote questioning of the on-line environment in the planned, fully developed methodology. The informative results of the on-line survey also provided this proof-of-concept with a greater number of respondents.

Several organisations who were invited to take part (in the in-depth interviews) would not because (for example):

- 'I respect what you are doing' but am too busy completing work before a holiday
- They have a policy of not taking part in research.
- The research period (June-July) is the busiest time of year for rolling out new information systems.
- 'I fear that it would ultimately be unwise for <a type of organisation> to reveal their appetite for risk. Think about the fear of being quoted in subsequent litigation, for example: the difference between a big appetite for risk and recklessness is a fine one.'

It is interesting to observe in that last response, this considered policy was not followed by another member of staff from the same organisation who took part in the on-line survey as did several other people from the same *type* of organisation. The implied connections between 'branches' of this type of organisation suggest that they would have a common policy against divulging this type of information. This is an example of the complexity being compensated for in this analysis of human vulnerabilities. That is, one person in the organisation has a good attitude to risk which holds him back from taking part in the study. Another has a good attitude to risk which encourages him to contribute. The contributor is compliant with their policy which does **not** prevent taking part; the non-contributor actually formulates his own policy.

Output from the detailed user engagement comprised the two-part questionnaires completed by one of three researchers, and the two-part questionnaires completed directly by the respondents to the invitations to take part in the research. The responses comprised tick-box responses to the questions and some commentary added to inform about the context of the response, or partially filled in tick-boxes and notes about the background and context of the responses to the questions which could be used to complete the tick-boxes, and in some instances, tick-box responses only. The on-line survey provided a greater volume of responses for analysis using the scoring mechanism. This was carried out using packaged SPSS analysis software¹⁶⁶.

¹⁶⁶ From SPSS Inc.

13 organisations from the following domains took part in the detailed investigation:

- Charity
- Construction
- Education
- Entertainment
- Government Agency
- Health
- Housing
- Insurance
- Law
- Local Government
- Software Development
- Utilities Related

As part of setting the context of the interviews, interviewees were asked to list information security breaches their organisations had experienced during the last 12 to 18 months. This ensured that interviews were grounded in experience rather than conjecture. The assumption was that for a respondent to discuss exposure to risk, they – or their staff – should have had some exposure to realised risk rather than basing their responses on conjecture. It also strengthened the responses to questions which were scored on the results of previous research where human vulnerabilities had manifested. The catalogue of realised risks below indicates that our interviewed sample has a significant contribution to make to the research. Their responses are not based on ‘what if?’ scenarios and can therefore be assessed without regarding the emotional literacy of the respondents (Hillson and Murray-Webster, 2007). There is no requirement to adjust their scores for (say) vested interest in the outcome of a possible breach. For example, as security manager, they may be tempted to downplay a threat for which they should have effective measures in place.

Participation in the on-line survey was primarily by invitation. NCC members and contacts were e-mailed an invitation to participate in the research. A further reminder e-mailing was dispatched to members one week before the survey closed. The survey was open for responses from 13 July 2007 to 14 August 2007 (just over four weeks).

From the 13 detailed interviews:

- 4 had suffered a malware infection
- 8 had encountered staff misuse
- 1 had detected an attack or ‘hack’ against the authorised network privileges
- 6 reported theft or fraud involving computers
- 5 had suffered systems failure or data corruption

Some of the respondents gave more detail about the security breaches they had experienced:

- Testing procedures were not followed before software was released into production¹⁶⁷.

¹⁶⁷ With the developer’s privileges being downgraded as a sanction.

- A member of staff sent a sensitive internal report to a Sunday newspaper.
- A senior member of staff was of the opinion that more information was required for their job and obtained it by gaining unauthorised access to a financial database¹⁶⁸.
- Several distributed denial of service attacks were experienced with at least one being directly attributed to blackmail.
- An IT staff member worked to a personal agenda, unaligned with corporate objectives but with a spirit of 'knowing best'; systematically ignoring back-up procedures.
- When a 'phishing' incident raided the bank account of an employee taken in by messages received through the company e-mail, performance was impaired by the individual's subsequent concern even though the loss did not directly impact on the corporate resource (that is, a loss of company funds).
- Some respondents mentioned small losses to data integrity or minor losses of data which presented small but almost acceptable – from a perspective of risk – inconveniences.
- Occasional problems with change control affected the availability of some network resources for one respondent.
- The police were involved with the misuse of a laptop for storing pornography (and the employee in question was dismissed).
- Confidential documents were stored in a less secure area than they should have been. No evidence was found of unauthorised access other than by the finder who came across them by accident.
- An outsourced IT 'partner' granted permissions to staff to which they were not entitled.
- One organisation suffered an unintentional denial of service when a legitimate customer set up a monitoring routine that polled their services to check availability. The server involved could not cope with the additional load of the monitoring.

The following paragraphs describe the responses from the interviewees to the risks questioned, against the topics in Table 22. This started with e-mail going astray as very much a human vulnerability, given the ease of sending e-mails and the tendency of users to send e-mails hastily (particularly in reply). This means that the consideration traditionally given to composing a letter is not applied. Anecdotes were told about usability features such as the autocompletion (of names) and 'Reply to all' functions which reduce the sender's verification of e-mail metadata before it is sent (Armstrong, Rhys-Jones, Dresner, 2004).

¹⁶⁸ This is an example of unauthorised access but without malicious intent.

Respondents suggested that damage to hardware was of little concern to users so their responses fall into the greater (weighted) risks. This may be related to an increased awareness of the anecdotally reported paradox of concern for the physical medium being stronger than concern for the intangible data stored on it¹⁶⁹. I expected some moderate concern over users' own activities but realised that this may already be reduced to an acceptable risk by some countermeasure. For example, changes to IT equipment being restricted to dedicated IT staff¹⁷⁰.

Availability – a system characteristic covered originally by the business continuity clause in the ISO/IEC 27001 standard and more recently in its own dedicated standards (BS 25999-1:2006; BS 25999-2:2007; BS 25777:2008) – is where business could not be continued as a result of a realised risk. I expected a high level of perceived risks in the event of an incident invoking a business continuity plan although this was not voiced in the concerns at the NCC workshops. This is indicative of the human vulnerability of complacency identified in the top 10 risks (NCC, 2005). In contrast to this, a good sense of the consequences of risk realised by inadequate back-ups was reported. *Most* organisations felt the measures in place would manage the risks and that their users concurred with this.

Removable media – channel for the risk of data loss – had the interviewees almost equally split between those who cautiously allow removable media such as pen drives and those who have put in measures against them. One exception – from the insurance industry – expressed concern because of a perceived lack of implemented controls.

The two questions examined the difficult-to-quantify concept of trust – the idea that network users should not be inhibited to use a network if they are aware of security measures being in place. That is, they should not be naturally risk averse rather than show a commensurate degree of caution during their interaction in the information system.

Reports about individuals' attitude to legal risk tended to score highly (that is, the risks were greater) in most of the interviews. This suggests the strength of the interview format because this level of response could have been predicted given the frequent doubt and uncertainty of callers to The National Computing Centre help desk. Although statistics for this are not

¹⁶⁹ In the developing methodology this could point us towards refining the question or scoring it differently because it could suggest *good* risk awareness.

¹⁷⁰ This balance of risks and treatments for areas taken for granted was observed during the certification to BS ISO/IEC 27001:2005 BS 7799-2:2005 of a major corporate organisation the Spring/Summer of 2010. The auditing certification body was content with the risk assessment for new risks but raised a note of non-compliance for the standard because the organisation had not included the well known risks that had been effectively treated before the formal ISMS had been developed. The risk assessment before the auditor's scrutiny suggested that only new and emerging risks were being dealt with and no credit was being given to areas where risk had already been reduced to an acceptable level. For example, a new data centre built three years earlier was designed so that any water-carrying pipes were routed away from the server racks for fear of leaks.

collected, a review of e-mail responses to incoming enquiries show that they are about legal issues regarding information systems (such as contractual issues with service providers, data protection, and the desire to ensure that any monitoring of communications is carried out legally).

More anecdotal feedback from discussions at NCC workshops suggests that there is often confusion between authentication (proving who you are) and authorisation (what you are allowed to do [on a computer network]). Interviews suggested that authentication information may be shared for positive motives. One respondent reported a breach where unauthorised access was gained with the genuine belief that restrictions were not taking account of his business case for access.

The responses for both the in-depth interviews (Figure 28) and the on-line survey (Figure 29) were benchmarked against 4 model answers which were derived by completing the questionnaires with worst and best case results (not pertaining to any organisation in particular). These 4 combinations were:

- Good appetite in the organisation/good attitude amongst individuals
- Inappropriate appetite in the organisation/good attitude amongst individuals
- Inappropriate appetite in the organisation/inappropriate attitude amongst individuals
- Good appetite in the organisation/inappropriate attitude amongst individuals

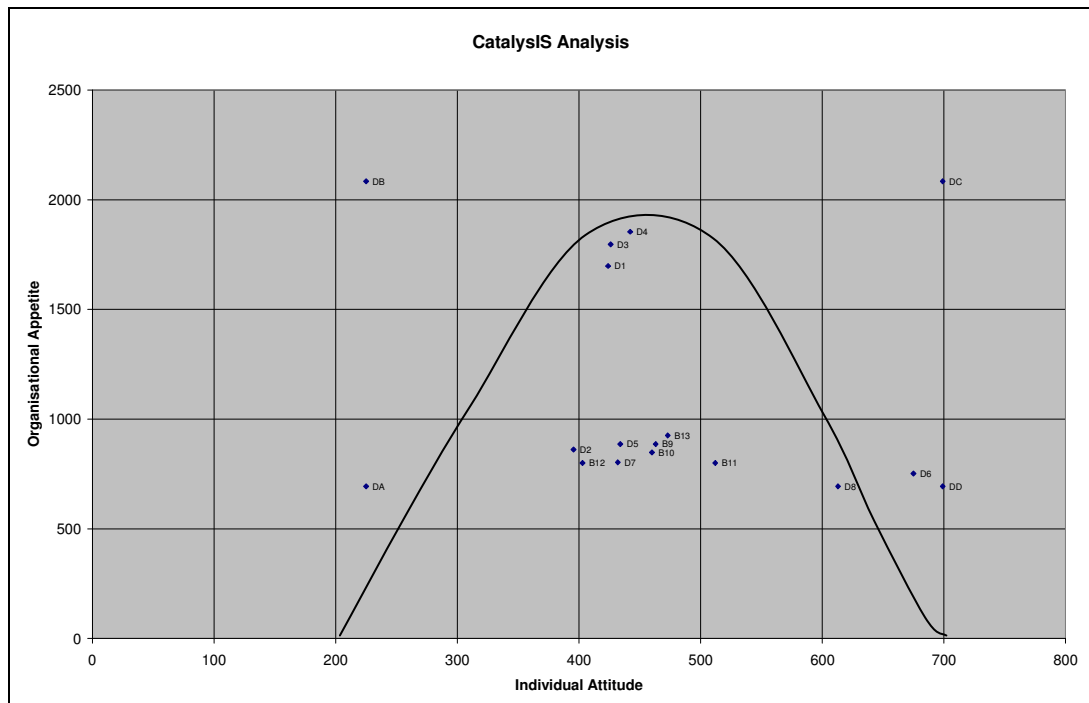


Figure 28: In-depth interviews: organisational appetite compared with individual attitude

Although limited to 13 points, a normal distribution of responses can be seen to be emerging. This evaluation is supported by a similar pattern being discernible for the on-line

responses. The on-line survey – although based on fewer questions – used the same weighted scoring structure as the in-depth interviews. This realisation of a normal model implies that the question structure and scoring of the methodology’s questions have merit for detecting an anomaly – a human vulnerability.

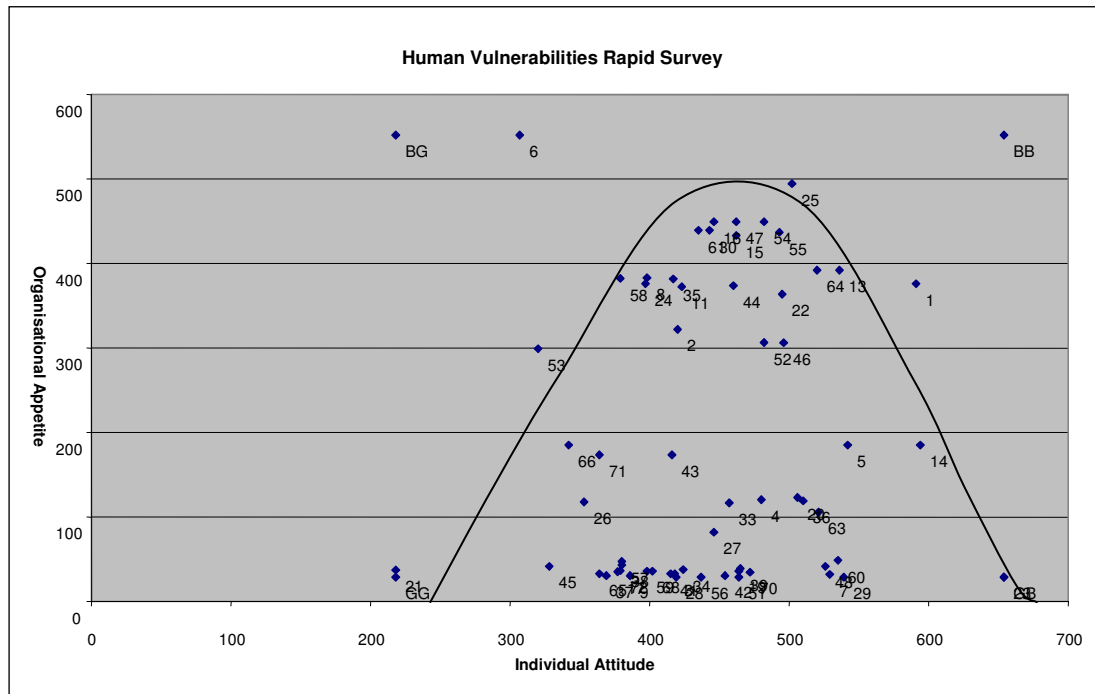


Figure 29 A comparison of organisational appetite with individual attitude from the on-line survey

82 responses to the on-line survey were received by the closing date of which 73 were useable responses - duplicate or hardly completed responses were not collated for analysis. The basic analysis includes all 73 responses, however, analysis by Size, by Scores and Weightings includes 72 responses (one respondent did not indicate the number of end-users in their organisation so they could not be included in analysis by size).

The number of end-users in the organisation was used as a measure for the size of the organisation. Almost half (46%) of the respondents to the on-line survey are from organisations with over 1,000 end-users. However, it must be remembered that these are a self-selecting group.

In questions about organisation or community, respondents take a serious view when it comes to only qualified staff altering how company equipment is used. 58% of respondents indicated that this is documented, communicated and audited. Over half of respondents indicated this was a formal policy. In smaller organisations (under 100 end-users) 50% indicated a formal policy, however, a quarter said they had no written formal policy and the remaining quarter had no policy at all.

It is interesting to note the high proportion of organisations that have no policy on screening staff for background qualifications during selection and changes of employment and once in

position only a few monitor their work. This tallies with the general unawareness (amongst those interviewed in-depth) of an up to date standard for screening.

With the introduction and accessibility of new devices to the general public, there has been an increased trend of staff (end-users) being allowed to use their own IT equipment for business use. For some organisations this has been a problem in terms of a policy for supporting this equipment. For this survey respondents were asked if they had a formal policy. It appears black and white – they either have a documented and formal policy or no policy at all.

Information risks are regularly addressed in projects, and in operations/IT service delivery at board level and are formally documented, communicated and audited by 47% of respondents, as part of their security policy. Larger organisations are more likely to report this as a formal policy. A quarter of responding organisations do not have any formal written documentation but it is understood to be company practice.

Very few respondents expressed the opinion that the ICT technical skills of their end-users is high (11%). The majority of respondents (64%) think the ICT skills of end-users are 'sometimes' high. It may be that this current picture – across all sizes of organisation – is the one that respondents want; after all they may not want or find it more challenging on their IT team if all their end-user ICT technical skills were 'high' thus increasing the likelihood of risks caused by unofficial intervention.

Respondents also indicated that end-users are more likely to have access to sensitive or confidential information at least sometimes rather than never.

It is encouraging to see that the message about Data Protection responsibilities seems to be getting through, with very few respondents indicating that they had end-users unfamiliar with the policy. All organisations with fewer than 100 end-users said that all their staff were familiar.

It is interesting that of all the questions in this section only the question about software licences reported some 'don't know' responses. Organisations with up to 1,000 end-users were more likely to report that all the software used by their end-users has a corresponding licence. Only a third of responding organisations with 1,000 to 5,000 end-users were confident that all the software used has corresponding licences, and 40% indicated that they 'sometimes' have a corresponding licence.

Looking at risks and how end-users would react and understand the effect on the organisation, it is clear from the results that respondents view end-users as more threatened when it comes to issues with their day-to-day work-related tasks. They were more likely to feel threatened by the following: confidential e-mail sent to the wrong person (68%), data cannot be easily restored from a back up if lost (55%), sharing logon details (49%), and customer information can be shared with their partners and contractors (50%). However, respondents indicated that end-users are more likely to feel comfortable with unplugging and

moving cables (34%), that pen drives are secure by their removability (46%), that the organisation gives access to all the IT equipment and files that they need (55%), and that a tested plan minimises the impact of a serious incident (50%).

They are more likely to report end-users are unfamiliar (39%) with the legal admissibility of legal documents in hard copy rather than by email.

Respondents are more likely to indicate their end-users were ‘uncommitted’ when it came to IT equipment being exposed to potential damage (37%), and security measures are common sense and don’t need to be mandated (34%).

4.6.6 What may be derived from these results?

Two key observations may be made on the frequency of scored responses shown in Figure 30: that the scores for the organisational appetite tend towards bimodal distributions, that is, individuals are scoring their organisations at extremes on the scoring scale, and that the scores for the risk attitude of individuals tend towards normal distributions, that is, individuals tend to rate themselves as being in the middle of a scale range.

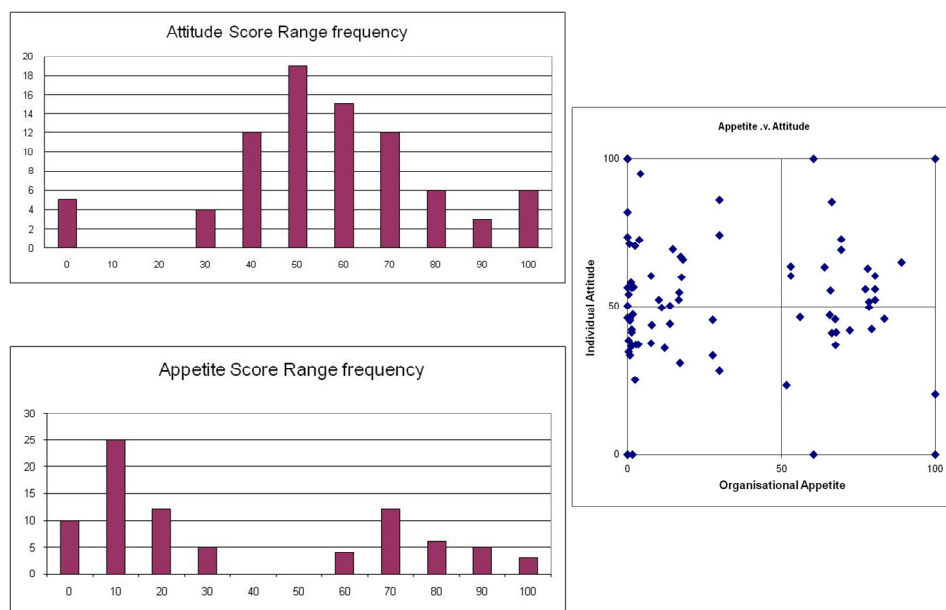


Figure 30: The frequency of scored responses (scores rescaled to 0 – 100 range)¹⁷¹

The bi-modal distribution of the risk appetite score is likely to be the effect of the highly differentiating questions about the use of uncontrolled (from the aspect of security policy) IT equipment. Where such use was permitted, a risk without reasonably expected security countermeasure greatly increased the risk score for a ‘big’ appetite for risk. Organisations generally had this under control *or* allowed it.

¹⁷¹ The higher the score, the greater the risk.

The aggregated score of all risk vectors contributing to the measure of an organisation's risk appetite – real or implied – only showed significant variations when uncontrolled (for example, personal ICT was in use for official business). I have described the *attitude* as *real* or *implied* because I am measuring this from an objective comparison of what the organisation expects to do about a risk. Therefore its appetite may be affected by a light policy implying that it has a big appetite in allowing exposure to certain risks. This pattern supports the scoring method for the methodology because the ranked scoring makes an area of risk (uncontrolled ICT) stand out.

The stability of the organisation – represented by for example uncertainty of employment prospects that are felt around the time of mergers and acquisitions – may result in divided loyalties, loss of corporate knowledge or leakage of information to inappropriate destinations (the export of a customer details database for example). This factor is therefore included in the risk profile. An organisation that is undergoing change to do with the allegiances of its stakeholders is likely to be at greater risk of an information security breach than its 'stable' counterpart. This was usually found to have a major change as the result of a merger or acquisition or no expected change at all. A notable exception was a Health Service department which, although clearly excluded from the expectation of takeover, considered reorganisation to be endemic and therefore expected to suffer from that instability.

Organisations with no reasonable expectations for major change of this sort (that is, likely mergers, acquisitions or root and branch reorganisation) scored zero risk for this question. This 'zero' score was allowed to reduce the complexity of the feasibility study. A full tool would ask for more detail to assure a completely realistic response¹⁷².

Most organisations felt that they had board-level risk governance actually in place. This is perhaps unsurprising considering that the survey sample was derived from The National Computing Centre database and that respondents came from reasonably active member organisations. This suggests that those listed in the database may already show some attention to IT risk though there is a desire to receive the regular knowledge transfer packages from the National Computing Centre to benchmark or improve practices.

The interviewees were all senior ICT staff with typically 15 to 20 years of experience. I believe that this profile of the interviewees endorses the high quality of this survey's content because of their awareness of risk issues and their confidence in sharing information about their organisation's approach to risk that others – without whom a relationship had been established – may have proven reticent to elaborate on. Interviewees referred to the need to

¹⁷² An additional feature of a tool based on this methodology could be to ask more detail for such questions so that the tool could recognise periods where risk is greater – a risk profile lifecycle. This is similar to risk management decisions made by Channel 4 television who have regular penetration testing of their website over a period of months. However, when broadcasting shows with a high interactive Web element, this penetration testing is carried out at least weekly.

address risk at board level and how standards for this are set by corporate regulations (Chapter 2).

BS ISO/IEC 27002:2005 BS 7799-1:2005 makes clear recommendations for the security-led control of ICT equipment. Where rules for these controls may be enforced within the jurisdiction¹⁷³ of the organisation, it is unlikely that the corporate controls will be kept sufficiently up to date on personal ICT equipment.

The prevalent restriction of having people with specific ICT roles as the only one allowed to implement ICT installation and change is a strong control with the caveats of the vulnerabilities of skilled insiders (Shaw, Ruby and Post, 1998). This highlights the need to focus on human vulnerabilities as the path to information systems breaches. One respondent referred to the opportunities to deliver some of their products and 'services' on-line had opened new paths for the fraudsters already prevalent in their industry but the new technology also presented its own technical solutions with no net gain or net loss being apparent as a result (but much more work).

Because the methodology is looking for human vulnerabilities in information systems, I have regarded the potential of screening and monitoring of staff as a powerful tool for matching information system users with the roles and access commensurate with their background, situation and skills (with a good human resource development programme to develop users accordingly). This is exemplified by the highly publicised¹⁷⁴ need to carry out CRB checks (as would be required for certain network users in the sample of survey respondents). The risk treatment (BS7858:2006) for ineffective screening – which goes into greater detail than the outline recommendations of BS ISO/IEC 27002:2005 BS 7799-1:2005 – was revised and reissued within two years of its original publication rather than the 3 to 5 years or more that is usual for similar standards.

Monitoring was reported unanimously by respondents as being an issue for the consideration of line managers and although it did not seem to be in use, the potential for it to be used remained. This was reinforced by interest from two of the respondents in having their monitoring processes vetted for compliance with the Regulation of Investigatory Powers Act (RIPA)¹⁷⁵. Notably one of these responses has an active programme of making their operating environment a 'good place to work'; their objective is partly to reduce any temptation for inappropriate use of the network by engendering personal commitment to the organisation. There is a lesson to be learnt here with the application of what the methodology may detect. Its use should not be one of monitoring and control but rather measuring and encouragement.

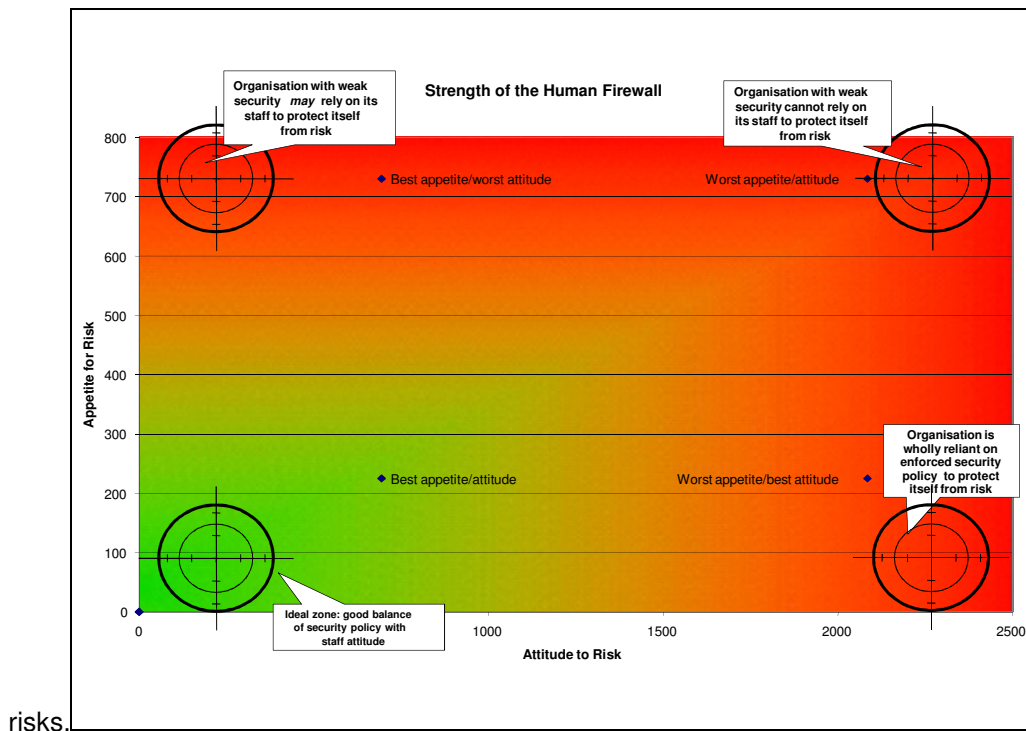
¹⁷³ That is the 'electronic airspace' or sovereign territory.

¹⁷⁴ Including <http://news.bbc.co.uk/1/hi/health/6678827.stm>, and <http://news.bbc.co.uk/1/hi/wales/mid/6386431.stm>

¹⁷⁵ One of whom has subsequently had this done.

4.6.7 A tool to identify Human Vulnerabilities

To create a tool to identify where an organisation's culture signifies human vulnerabilities in its information systems, the tables with questions were transposed into a spreadsheet with the responses marked in the relevant table cell. Each cell had the corresponding score from the tables assigned to it so that an x in the response cell called in the relevant weighted score. Two sheets per organisation were created: one with the totalled appetite score from the questions about the organisation's risk appetite, and one with the totalled attitude score from the questions about the risk appetite of individuals that the organisations representative had described. The totals from the two sheets were plotted on a graph where the x axis represented a scale showing the individual's attitude to risk and the y axis represented the organisation's appetite for risk (Figure 31). The range of the scales on the two axes was set by the model answers comprising the good and inappropriate appetites and attitudes according to the worst and best case results. Higher scores represent greater exposure to risk. A green-red background was created for the graph to highlight the relative



risks.
Figure 31: The proforma chart of appetite and attitude scores

The chart was tested with the results of the 13 in-depth interviews showing that it was sufficiently reliable to be used in the field.

4.6.8 The application of the method in establishing improvements in risk awareness

4.6.8.1 The test environments

None of the field work case studies (Chapter 5) required the deployment of the methodology however its value, usability, and accuracy have been shown in two recent projects. In the

first (December 2009 to March 2010), I was tasked to train an IT department in information security awareness at a level that fitted with their responsibilities as system designers and implementers handling sensitive information up to Business Impact Level 3¹⁷⁶. This programme was requested by the organisation's information security officer so that he could discharge its obligations under government requirements for mandatory information assurance training. Information assurance is defined by CESG as 'the confidence that information systems will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users'. The training was designed specifically for the IT department. This realised the responsibility of system developers to create systems where usability would not be compromised by the poor design of the security controls (Flechais, Sasse, Hailes, 2003). Each session comprised a presentation with an exercise to test the risk awareness of the staff. It is worthwhile noting that the IT department agreed to the training under sufferance as it was not seen to be a priority.

In several training sessions the questions measuring risk attitude were completed at the start and end of the session and benchmarked against the original answers. The results were used to see if the training had improved the attitude of those attending by increasing their awareness of risk and what was considered as acceptable treatments for those risks. (

The 'look and feel' of the spreadsheet implementation from the feasibility study was improved so that it could be displayed publicly during exercises involved with the improvement of information security in an organisation.

4.6.8.2 How the tool was deployed

The IT department comprised 83 staff who were involved with the development, support, and maintenance of information and communication systems for the organisation, and administrative support for the department. The staff attended the training sessions in groups of 12 or less with little or no knowledge of why they were required to attend. Each session started with an explanation followed by a review of their information security attitude. This was taken with the risk appetite measure for the organisation (which had been calculated by interviewing the information security officer using the questions about the organisation's status, and the content and quality of deployment of the organisation's information risk management policies. His responses were added to the spreadsheet, leaving the questions about the local attitude to risk to be asked during training sessions with the IT department. This plot was made with the version of the questions used by the in-depth questionnaire so that the trainees could not only see where they were placed in relation to themselves before and after the training but also with respect to other organisations. An example from one session is shown in Figure 32. The objective was to show the collective risk attitude of each group.

¹⁷⁶ That is, *confidential* according to HMG Infosec Standard No. 1 (CESG, 2009).

4.6.9 Training content

The training session for each group contained material to educate attendees in the basics of information assurance, teach them how to apply proportionate treatments to information risk, and help them appreciate the stakeholders who will make risk treatment effective. This was exercised with a fictional case study about handling sensitive information to which the controls of BS ISO/IEC 27002:2005 had to be applied to link risks with policies and countermeasures.

4.6.9.1 Results

Seven sessions were run which included most of the department in the training. As the programme was run, it became more and more challenging to deliver the sessions with some of those attending being distracted by their perception that the training was a low priority in relation to their day-to-day responsibilities. Priority was given to delivering the presentation material and encouraging participation in discussion and the risk treatment exercise. Only three of the seven sessions completed the benchmarking exercise. The results are shown in .

Table 36: Before and after training – measures of risk attitude

		Session 1	Session 2	Session 3
	Appetite Score	Attitude Score	Appetite Score	Attitude Score
Training session: first measure	301	324	486	287
Central Government	424	1698	1698	1698
Construction	396	861	861	861
Law	426	1797	1797	1797
Registered Social Landlord	442	1854	1854	1854
Local Government	434	886	886	886
Insurance	675	752	752	752
Education	432	803	803	803
Software	613	694	694	694
Utilities	463	886	886	886
Gambling	460	848	848	848
Local Government	512	800	800	800
Charity	403	800	800	800
Healthcare	473	925	925	925
Training session: second measure	301	209	137	137

4.6.9.2 Analysis of the results

In all sessions, the coordinates of the group under scrutiny were moved further into the heart of the green zone of the chart. Figure 32 shows the improvement measured from the first session. It is worth noting that the organisation scored well from the outset with regard to both risk appetite and risk attitude. This is likely to be because of the nature of the organisation's work which require it to habitually regard security as important as part of its business which often requires it to enforce security for others. This is further exemplified by the existence of the full time information security officer and the mandate for the information security awareness training.

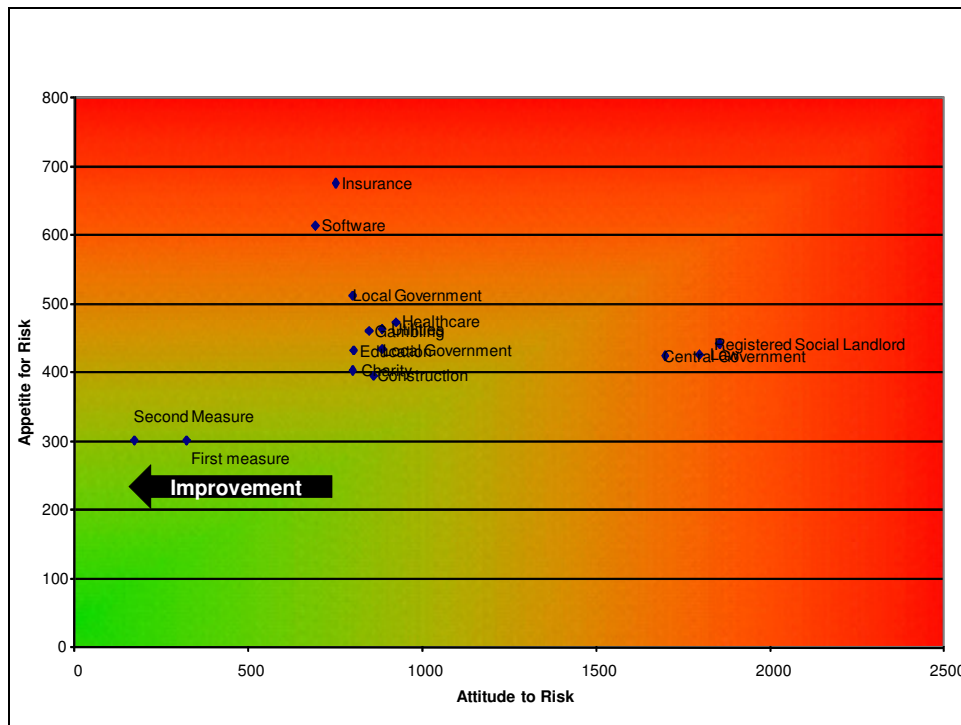


Figure 32: Improvement in risk and treatment awareness measured in the first session of training

4.6.10 A second test of the tool

Another test of the tool was used for a government agency (June/July 2010). This test was better because I completed all the results to input into the tool independently following several days of structured interviews of representatives from the agency’s field workers and their management, local authority liaison, human resourced department, and their policy, communications, and strategy divisions.

The results of these interviews were recorded in a report making a set of recommendations for improvement. Implementation of the recommendations was begun at a workshop of top security management staff from the agency who concurred with the point on the chart where their agency and colleagues were placed.

4.6.11 The feasibility study report

Two reports were written. The first was a short report to fulfil the mandatory requirement of the funding grant. This covered the technological and socio-technical innovation of the work, its economic, environmental and societal benefits, supply chain impacts, and opportunities for further development and exploitation. The later considered further research and development, trialling the tool and for delivering project benefits and diffusion commensurate with the investment. The second, detailed report is mostly encapsulated in this chapter with the analysis of the project’s outcomes, and future work as described in Chapter 6 of this thesis.

CHAPTER 5. CASE STUDIES: WHAT ARE ORGANISATIONS DOING TO MITIGATE RISK?

5.1 About this chapter

This chapter extends the literature review of Chapter 2 by describing a rich set of action research case studies that show how standards are developed and selected – for example from the body of knowledge described in Chapter 3 – and implemented to treat risk in information systems. The case studies are a catalogued in Table 1. In the literature review, I discussed the methods of how standards are set and the differentiation of the standards as set, and the standards as implemented. These case studies track the parts of the life cycle of standards in development and standards in use that demonstrated some of the realisation of that process.

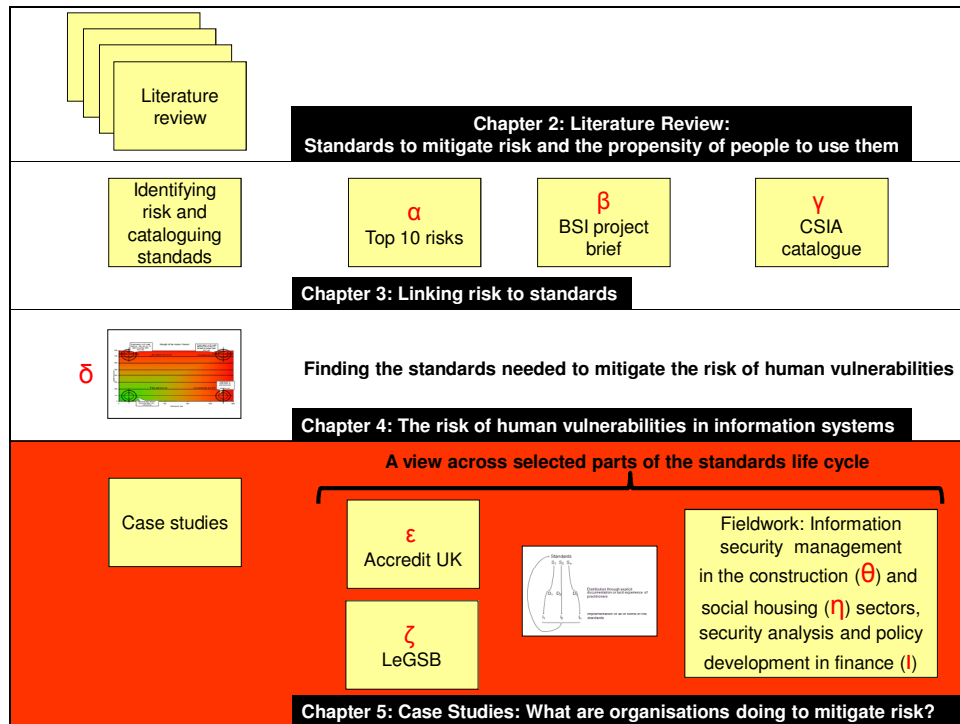


Figure 33: This chapter in the context of the thesis

In this chapter I describe the methodology and the recommendations of the action research. In Chapter 6, I discuss how these recommendations are examples of how standards are adapted to mitigate risk whilst retaining their characteristics and desired degree of uniformity.

5.2 Why were these case studies chosen?

The case study projects (Table 37) were selected as the theatre of observation to look across the standards lifecycle. Projects investigated the setting and selection of standards (Accredit UK – ϵ , LeGSB – ζ) and the deployment of standards in three different

organisations (a housing association – η , a construction firm – θ , and a financial services firm – ι). This action research set out to observe the process suggested in the literature review (Figure 11); that tacit know-how is codified as explicit knowledge in standards, released by the organisation implementing a standard. Yet despite the idiosyncrasies in the way that this is done, compliance with the standard is still respected. The organisation takes on board, explicitly or implicitly, the policies set out by the respective standard with the organisations own idiosyncrasies that make the implementation of that standard particular to that organisation. The overall ‘standard’ of the standard remains intact (Figure 14). This is closely connected with the methodology of Chapter 4 where the risk appetite of the organisation is measured according to the *quality* of policies implemented to protect its information. (This is shown on the risk appetite axis of the scatter diagrams in Figure 28 and Figure 29.)

Table 37: Case studies documented in this chapter	
Label	Case Study
These case studies comprise (a) two projects about the development of standards for information systems:	
Epsilon ϵ	The development of the Accredited UK (AUK) General Segment – a standard to manage the risk in the supply of ICT by small to medium-sized ICT suppliers ¹⁷⁷ .
Zeta ζ	Work with the Local e-Government Standards Board (LeGSB ¹⁷⁸) to define a process for the development and adoption of standards, and to pilot a process to ‘certify’ the acceptance of standards.
(b) three pieces of fieldwork which analyse where standards are applied to treat risk:	
Eta η	Recommending an information systems risk (security) strategy in a housing association.
Theta θ	Supporting a construction firm in its identification of risk and the selection of controlling treatments to mitigate them.
Iota ι	A review of risk management (information security) policies in a financial services firm delivering pensions and actuarial products.

¹⁷⁷ A segment is an ICT discipline such as network design and installation, software development, or ICT consultancy. Each discipline is expected to manage risk by carrying out its own specialist activities *and* a set of activities that are carried out in every ICT business. It is the latter set of common activities that are defined in the ‘General Segment’.

¹⁷⁸ Eventually becoming the e-Standards Body (e-SB)

5.3 Developing standards to treat risks: defining a collective methodology for investigation

This section of the chapter considers two action research projects which directly involved managing or influencing different parts of the standards development life cycle. They are significant parts of the research because they show how standards are developed in response to a particular risk (such as Accredited UK and the purchaser's risk of selecting a supplier of inadequate competence) and how existing standards may be selected as risk treatments for specific problems (such as testing Local e-Government Board's ratification process for standards that it wished to endorse). The methodology (Table 38) emerged from the creation of a way to observe the take up of standards in three organisations (a housing association, a construction firm, and a financial services firm delivering pensions and actuarial products.)

Table 38: The development of the action research methodology for this study

	Method	Methodological reasoning	Relevant project
1	Facilitate a series of stakeholder meetings to understand the requirements of a standard from the point of view of those who will implement it and those who will benefit from its implementation. Draft the standard in response to the contents promoted by the two views and use the same stakeholder group to review the emerging standard until its text is agreed.	The definition of standards (Table 5) involves stakeholders who must implement the standard, those who will benefit from the implementation of the standard, and those who may be charged as the independent facilitators who reconcile the viewpoints into a synthesised, agreed way of working. This is required to increase the likelihood of the standard being accepted by those who apply it and those in the thrall of its results.	ε The development of the Accredited UK (AUK) General Segment – a standard to manage the risk in the supply of ICT by small to medium-sized ICT suppliers.

Table 38: The development of the action research methodology for this study

	Method	Methodological reasoning	Relevant project
2	<p>Propose – or invite proposals for good practice to be set as the standard way of working for a specified scope.</p>	<p>Where there are a number of candidate standards, each needs to be assessed for the fit with its practicality to implement and the likelihood of its implementation being accepted.</p>	<p>ζ Work with the Local e-Government Standards Board (LeGSB) to define a process for the development and adoption of standards, and to pilot a process to ‘certify’ the acceptance of standards.</p>
3	<p>Suggest how information security practice – as defined by the ISO/IEC 2700n series of standards – can be applied to mitigate information security risk.</p> <p>Analyse the current practice of each organisation by touring a sample of their premises and interviewing a cross-section of management, administration and delivery staff. Benchmark the findings against the recommended practices in ISO/IEC 27001 and ISO/27002 and recommend improvements.</p>	<p>A benchmark against a well-defined standard and one or more recommendations for change from the current activity of the organisation to those which would mitigate risk is that it allows a structured process for creating an observatory on the effects of standards implementation. The changes to activity are identified by the assessed risk to the organisation with respect to the implemented policy that would protect against that risk.</p>	<p>η Recommending an information systems risk (security) strategy in a housing association.</p> <p>θ Supporting a construction firm in its identification of risk and the selection of controlling treatments to mitigate them.</p> <p>I A review of risk management (information security) policies in a financial services firm delivering pensions and actuarial products.</p>
4	<p>Analysis</p>	<p>Investigation of the results to look for supporting evidence in answer to three research questions.</p>	<p>The succession of projects as the work they record spans different parts of the standards lifecycle.</p>

Accredit UK is a standard that was proposed by The National Computing Centre to increase the commercial success of small-to-medium ICT businesses¹⁷⁹ in the regional development zone that is overseen by the Advantage West Midlands agency. The objective of the standard is achieved by making the purchasing process successful for both the supplier and the customer by managing the risk in the supply of ICT. Compliance with Accredit UK results in assuring the successful implementation of ICT supply activities that have been recognised as good practice by suppliers and purchasers. Businesses that do not carry out the activities to the acceptable levels defined in the standard are suspected of not having a sufficiently positive risk of successfully supplying ICT to the satisfaction of their customers or where the continuing maintenance and support of the ICT is uncertain as a result of potential instability in the ICT suppliers' business.

There were two methodologies that were assessed for the research and development of a standard that would be acceptable to its stakeholders. Four stakeholders (or stakeholder groups – see Table 39) were identified for involvement in the development process to assess fitness for purpose of the project's deliverables and outcomes.

Table 39: Key stakeholder groups for the Accredit UK project	
Group	Profile
Advantage West Midlands (AWM)	The development agency part funding the development and roll out of the standard to SME ICT businesses and their suppliers.
The National Computing Centre (NCC)	The research and technology management organisation that invested resources into the development of the standard.
SME ICT suppliers	Businesses who wanted to apply a mark of quality to their business to increase the confidence of current and prospective customers.
Purchasers of ICT	Public and private sector organisations who want reliable ICT from suppliers who deliver value for money.

Two methodologies were proposed to create and deploy a standard and certification framework which would benchmark the ICT suppliers against the adequacy of their risk management controls in running an ICT business in their respective field. Both methodologies would apply action research in the formulation, refinement, deployment and review of the emergent standard. The first methodology considered, involved the selection of relevant standards that were already available and achievable by ICT businesses (cf. the

¹⁷⁹ Defined by the then Department of Trade and Industry as a business with less than 250 employees.

project to define a catalogue of publicly available risk treatments – see Chapter 3) but which may not be seen to be a clear advantage by the suppliers or their customers. This would not create a new standard but rather a ‘meta-standard’ of existing risk mitigation techniques. A period of investigation would follow to see whether the businesses applied these standards, and then award an AWM mark of quality as relevant specifically to the supply of ICT. These standards included – but were not limited to – quality management models such as ISO 9001 for quality systems, the Capability Maturity Model (CMMi) of the Software Engineering Institute of Carnegie Mellon University, and the European Quality Model (EFQM). The second option was to develop a bespoke standard for the SME ICT businesses that would take the lessons learnt from the quality management models referred to in the paragraph above and use SME suppliers and their customers to formally review the standard and iteratively improve it based on their feedback. Both methodologies would include a trial period whereby SMEs would apply – or benchmark – the standard (or meta-standard) in their businesses and use it as the basis of contract negotiation with their customers.

The two options were reviewed by the West Midlands IT Association (WMITA) which represents mostly SME ICT suppliers in that region. WMITA concluded that a single standard (the second methodology) was preferred because the ‘metastandard’ would presuppose that businesses needed other certifications first – questioning the correctness of the AWM standard for the SMEs, the completeness and consistency of a set of certifications held by one SME when compared to another, and the need to create a complex metastandard to close the gaps. Creating a new, standalone standard would give a simpler point of focus for the supplier companies and avoid a confusing ‘certification of certifications’ with no added value to the existing market for certification.

The second project that involved parts of the standards development life cycle (see Chapter 2) involved the Local e-Government Standards Body (LeGSB) – originally the Local e-Government Standards Board – which was established to set standards for e-government services provided by Local Authorities. LeGSB was a national project of the (then) Office of the Deputy Prime Minister (ODPM) established to support the transition to the provision of local government services on-line by the end of 2005. It ran from 2003 to January 2006. It is currently managed by North West e-Government Group (NWeGG) and has set itself the wider remit of setting IT-related standards for Transformational Government¹⁸⁰.

LeGSB used a model of standards comprising three classes according to how the standards are set: *de jure*, open, and *de facto*. *De jure standards* have some force of law; or are approved by one of four recognized international standards organisations (ISO, IEC, ITU,

¹⁸⁰ Transformational Government is a strategy based on the ‘transformation of public services for the benefit of citizens, businesses, taxpayers and front-line staff, the efficiency of the corporate services and infrastructure of government organisations, thus freeing resources for the front-line, and the steps necessary to achieve the effective delivery of technology for government’ (Cabinet Office, 2005).

UN/ECE). It is usual for each standards body to have a process whereby they will (sometimes mutually) recognise the standards of others. The British Standards Institution (BSI) for example, has several categories of 'liaison' (BS 0:1997) defined for the adoption of standards from other bodies. Secondly, *an open standards model* where standards are approved under an open process where all interested parties have input, results are publicly viewable, etc.; the organisation that developed the standard may be de jure or not. This may be extended in some models where to contribute directly to the development of a standard (for example, ISF, 2007), individuals or the organisations for which they work, must pay a membership fee. The third class of standards considered by LeGSB are *de facto standards* which are not usually subjected to the rigours of refinement but are declared as a standard because of common usage, or by proclamation of a dominant vendor and subsequent acceptance by the marketplace.

Each of these standards may themselves be one or a combination of three types: *practitioner standards* which provide authoritative information sources to support practitioners in complying with legislative or regulatory requirements and in delivering secure, effective and efficient systems; *information standards* that clarify data standards, schemas, or metadata to support the delivery of information; and *technology standards* that ensure the quality and effectiveness of technology to support effective and efficient systems operation.

LeGSB commissioned the draft of a 'standard for standards' to support its operations. The requirement set was to define a standard process by synthesising existing 'best practice' advice and guidance for setting standards (W3C, 2003; BS 0:1997; Cabinet Office, 2005; NCC, 2000; ISO/IEC 9126-1:2001) by developing new standards or adopting existing standards into the LeGSB corpus.

Through desk research, sources were taken from the standards bodies that had complementary or congruent objectives. The processes were selected or constructed for their appropriateness in managing risk in standards development, notably to: avoid a process which is too complicated but with sufficient opportunity for all stakeholders to contribute suitably¹⁸¹; avoid standards which do not meet the requirements of those who have to implement them or those who need to benefit from their implementation; and balance the mix of people, processes, and technology. The standard for standards would be compiled from the material gathered during the desk research, peer reviewed by standards practitioners within LeGSB and local authority representatives affiliated with it.

LeGSB also wished to pilot its *standards certification process* – as defined by their 'Certification Process Guide' – and identified sources of candidate standards for immediate

¹⁸¹ Sometimes – perhaps surprisingly – this may be a trade-off between simplicity and layers of complexity introduced for confidence. The specification for LeGSB concentrates on simplicity and effectiveness, and shows where this can be achieved without an impact on confidence.

action. The purpose of this pilot was to see how a representative sample of proposed local government 'e-standards' would progress through the fledgling certification process to gain acceptance in the LeGSB community. The LeGSB nomenclature was to refer to the approval of a standard for adoption as 'certification'. It had no connection with the popular concept of certification to a standard as a term of compliance which is associated with the term in most standardisation processes (particularly those of BSI and ISO).

These prior project outputs – proposed local government 'e-standards' – were the basis of pilot *Requests for Proposals* (RFP) which in turn became pilot *Requests for Comments* (RFC) and pilot trials of standards adoption/implementation etc. Because this was an exploration of the mechanics and robustness of the adoption model, it was difficult to be very specific about quantitative inputs and outputs beforehand. To cope with this, a short series of three work periods with fixed checkpoints (see Table 40) was agreed through which a staged view on progress (and costs) to date was taken, and only at each checkpoint would the work plan be set in detail for the next period. This allowed LeGSB an opportunity to cap its future commitment at each checkpoint. It was expected that the pilot would finish with some standards awaiting the field trials before certification.

Table 40: LeGSB project checkpoints	
Checkpoint	Control
1	A review of progress on getting RFPs and RFCs defined and out for consultation or pilot implementations and a plan for the following month.
2	A review of the interim/first conclusions from the first RFPs/RFCs cycle, a review of progress on the second cycle of RFPs/RFCs etc., and an outline plan for the following month to bring the remaining RFCs and pilot implementations to a close or arrange for their continuing beyond the close of this standards process pilot.
3	Review lessons learnt and present a report to LeGSB documenting them with recommendations on how the process could be improved.

These three check points were the planned project stages of the review process for adopting standards to manage risk in the delivery of e-government services, thus forming the first tranche of my investigation of the standards life cycle.

5.4 Deploying standards to treat risk: defining a collective methodology for fieldwork

The next tranche of the standards life cycle – the implementation of standards – was investigated in three pieces of field work in organisations engaged in the supply and management of social housing (project η), the construction industry (project θ), and a firm offering pensions and actuarial services (project ι).

An independent, not-for-profit housing association in the South West of England had evolved out of the trend for local authorities to delegate their responsibilities for social housing to third-party specialists. As a result, an organisation with close public sector ties had emerged but whose main objective was to control its affairs independently. The result up to the engagement of analysts from The National Computing Centre had been the maintenance of two working sites: one focusing on administration and the other as a depot for staff and contractors who deliver the association's services. This had left the association without an IT strategy that it could own and created the opportunity to draw one up with the treatment of information security risk in mind. The purpose of this project was to design and document this strategy.

The association managed over 3500 homes and 130 staff of which 80 were office based and 50 involved in property maintenance. The project was established to research and develop an information security strategy because information is critical to the association's operations and the security of that information is paramount for the confidence of its customers and legal compliance. The DTI Information Security Breaches Survey (2006) suggested that the high probabilities of incidents mean security may no longer be perceived as an additional option but must be an embedded part of the housing association's culture. This was true for the housing association's obligations at the time of the analysis and was becoming even more so as the housing association's information landscape became more complex, for example with the integration of the service with other public service providers such as fulfilling the local council's obligations to house vulnerable people.

Security was defined as protecting the information handled by the housing association from risks in three key areas (*Table 41*).

Table 41: Risk attributes for housing association information	
Attribute	Definition
Confidentiality	Some information is suitable for dissemination to the public or to tenants; other information may be highly confidential to a few individuals. It is necessary apply a system for setting a level of confidentiality on all information, labelling it in a consistent and visible manner, and ensuring that those without the appropriate level of privilege cannot access the information.
Availability	Information owners are expected to put measures in place to ensure that their information will be available as staff and tenants legitimately expect it.
Integrity	Staff, tenants, and other stakeholders must be able to trust the information that they are basing their decisions on to be accurate, complete and up-to-date.

In the second case study project (θ), where I investigated the implementation of standards for information security, a construction firm specialising in property fitting, support, and furniture making was improving its information technology network architecture and infrastructure with a centralised data centre in its main Scottish office with thin client links to its two satellite offices. It had approximately 300 network nodes (150 office based and 150 site-based) running its main applications of Microsoft Office/Outlook e-mail and its financial system. Some specialised software was used by its architects and surveyors. The firm had no formal security policies in place and although a disaster recovery plan was outlined, a complete business continuity plan needed to be developed. The changing infrastructure provided an opportunity to develop and implement an Information Security Management System (ISMS) and the firm agreed that that the advice encapsulated in ISO/IEC 27001 – as the recognised industry standard for best practice information security – would provide a suitable template¹⁸².

I looked at how the methodology – governing the choice and selection of contact with the organisations through the medium of action research – could be carried out, taking into account the associated risks and costs of each (Table 42). This standardisation (sic!) of approach defined for the housing association (η) was then used to guide the subsequent projects with the construction (θ) and financial services organisations (ι).

Table 42: Possible action research approaches to ISMS implementation				
	Method	Reasoning	Associated risks	Associated costs
1.	Prepare a prescriptive course of action to develop an ISMS that complies with good practice.	The research that underpins the instruction to the target organisation has been developed with rigorous scrutiny from peer organisations and subject matter experts.	Requires a high degree of trust from the business owners. The ISMS is likely to be developed with a lack of ownership because the components will be extracted from a book rather than developed with the understanding of the business process owners.	Lowest outgoing cost for the time of the action researcher and the lowest cost for the effort from the organisation, assuming a quick understanding of the prescriptive material.

¹⁸² Such an approach also had the future option for formal certification to the standard if the three organisations of the implementation case studies demanded it.

Table 42: Possible action research approaches to ISMS implementation

	Method	Reasoning	Associated risks	Associated costs
2	Prepare a framework of baseline actions that can be developed into specific ISMS components with the business process owners.	This brings the prescriptive elements to the business owners whilst accounting for their learning curve in adopting them.	This still requires a high degree of trust from the business owners. As the ISMS becomes customised for that organisation, there is a management or facilitation overhead to keep the development on track rather than allow it to become bogged down in organisational detail.	The action researcher will spend more time training staff from the organisation. The organisation's staff will spend more time understanding ISMS principles rather than developing an ISMS deliverable.
3	Precede any detailed contact with business owners that may lead to development of ISMS deliverables with a period of analysis that looks at what de facto elements of ISMS are established already.	An experienced action researcher in the ISMS field can match the elements of the implied ISMS with the requirements of ISO/IEC 27001. Subsequent work can then build on this gap analysis.	The negative risk of the action researcher being unable to discern a suitably wide picture of the ISMS components in place is overshadowed by the positive risk of building an ISMS that is not only tailored for the organisation but also gives the stakeholder business process owners an early opportunity to take ownership.	This will not only require investment in time from the organisation's staff to be interviewed by the action researcher, it will also cost additional time for the action researcher in the collection and analysis of data from the interviews.

The case study (i) where I investigated risk management for the company dealing in pensions and actuarial services was an interesting hybrid of the issues regarding the selection and implementation of standards because it involved benchmarking documented and perceived practices with a known standard (ISO/IEC 27001) as well as keeping the company's implementation of information security practices aligned with the standard(s) set – as documented by security policies – by the holding company (essentially the fourth category of standards described in the LeGSB¹⁸³ discussion above).

The pensions and actuarial services company had been bought by a larger organisation with a complementary service portfolio. The holding company had components of a relatively mature ISMS and dictated the requirement of compliance with good practice in information security to its subsidiary. The subsidiary company commissioned a short action research programme to analyse its current practices, review the holding company's security policies, identify any gaps or weaknesses compared with good practice and tailor them to be applied by the subsidiary.

The requirement for using accepted good practice as a benchmark was the driver for taking the standard BS ISO/IEC 27001:2005 BS 7799-2:2005 as the benchmark against which the company activity in information security could be compared. Although there are many information security standards (as shown by the *catalogue of standards and best practice advice for effective information assurance* – Project γ) only the international standard was comprehensive in its coverage and had a widely spread assessment and certification scheme associated with it. It was therefore decided to use a series of structured interviews with key staff in the subsidiary company to find out what the level of information security awareness was, and then edit the holding companies security policies to fit that level of awareness to achieve the information security expected by the standard. This was a more effective way of getting a set of security policies suitable for the subsidiary that would satisfy the holding company, rather than develop a set of policies in isolation from the holding companies practices. However the analysis was cognisant of the risk that the holding companies policies need to be reviewed with caution and themselves benchmarked against the good practice documented in the standard lest they introduce ineffective measures. The source of this risk was the transfer of methods from one organisation to another without comparing and adjusting them to a normalising practice first. What was appropriate for a larger organisation with American-based management may not be readily accepted by a small company based in the UK. The size, structure and cultural differences may result in differing attitudes to risk. At the time the research was carried out, there was no known way of measuring risk attitude (see *Chapter 4*).

So across these five projects I had identified the opportunity to see the efficacy of processes to select or develop standards to mitigate information systems risk in general and the

¹⁸³ Project ζ

implementation of standards to mitigate information security risk in systems in particular (Table 43).

Table 43: Action research across the life cycle of a standard			
Life cycle stage	Project	Objectives	Contribution to research
Standards development	ε - Accredited UK	New standard to be developed	What is done to define a new standard?
	ζ - LeGSB	Development of new standards or the adoption of existing or developing standards	How are existing standards adopted for new uses?
Standards implementation	η - Housing association	Benchmark of security practice	How do you compare an organisation's actual or implied standards with a recognised standard?
	θ - Construction	Implementation of an ISMS	How do you steer varying levels of practice in an organisation into an ISMS?
	ι - Financial services	Definition of local information security policies	How do you adapt imposed policies (standards) from one organisation to another?

5.5 Applying the collective methodology to the development and adoption of standards to treat risk during the procurement of information systems

5.5.1 Project ε: Accredited UK

The method of desk research and stakeholder review was applied to the definition of standards for the Accredited UK marque and the LeGSB (project ζ). The Accredited UK standard was specified to comprise a generic segment that would be applicable to every type of (small) ICT business and a library of special segments that would be applied according to the type or types of ICT product or service the business offered its customers.

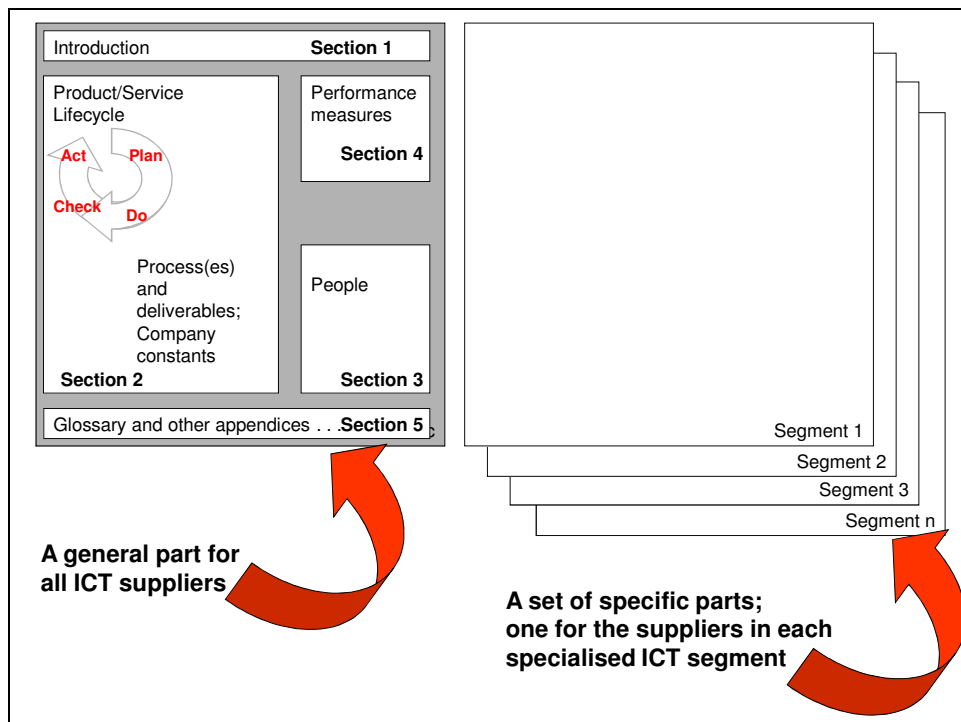


Figure 34: The overall structure of the Accredited UK standard

A specification of the initial generic standard requirements for Accredited UK was prepared by a consultancy – Brass Bullet – by developing a process model to allow an author from BSI to create a draft standard. The process model was the result of an analysis of a set of standards, codes of practice, and sector agreements (collectively known as the ‘domain standards’ – see Table 44). The constituent parts of these domain standards were assessed by the consultants for their appropriateness for inclusion in the generic section of Accredited UK. The BSI author would then draft the standard with its own unique structure that included or referred to the relevant elements of the domain standards.

Table 44 Source standards for Accredited UK	
Reference:	Domain
BS ISO/IEC 20000-1:2005	Information technology — Service management — Part 1: Specification
BS ISO/IEC 20000-2:2005	Information technology — Service management — Part 2: Code of practice
ISO/IEC TR 15504:1999	Information technology - Software process assessment
ISO/IEC 15288:2002	<i>Information Technology – Life Cycle Management - System Life Cycle Processes</i>
BCS	Code of Good Practice
Intellect	IT Supplier code of best practice
e-skills IT 2005-2008	Sector Skills for Business and Information Technology

Several early drafts of Accredited UK (then referred to as the 'ICT Supplier Standard') only contained text extracted from the domain standards but did not add value to existing standards by addressing the risks in the purchasing process when dealing with SME ICT suppliers. NCC and BSI agreed that BSI's editorial expertise was not established to draft new work but rather to manage the process of facilitating subject matter experts whilst they did so. The task was therefore handed over to NCC on the merit of technical writing experience of drafting standards for ICT quality management, particularly within the framework of the BSI committee structure. The result of this was support for BSI – who retained an editorial role – with a method comprising:

- Desk research and writing
- Stakeholder workshops
- Completion of the draft
- Stakeholder reviews
- Disposition of comments
- Second stakeholder review
- Evidence collection
- Scoring/normalisation
- Pilot certifications
- Results and feedback

20 drafts of the standard were written and distributed to stakeholders for scrutiny during this process. Desk research and writing involved designing a structure for the standard based on the background standards proposed by Brass Bulletin. These were supplemented by other standards (such as BS ISO/IEC 27002:2005 BS 7799-1:2005) when it became apparent that

certain good practice would be expected from the SME and that good practice was already documented elsewhere).

The first draft was mostly an outline created to settle the introductory elements and the contents so that stakeholders would know what was planned for the detail. The stakeholder feedback was used to create a draft with improvements to the foreword and introduction, general corrections and improved structure, and temporary authoring notes so that subsequent reviewers would know the intended content of a section before its development. This would provide an opportunity for early correction of any misunderstanding of stakeholder views. Some interim drafts were submitted to the project manager as a moderator for the interpretation of comments from the stakeholders by the author. The project manager provided corrections and direction and accepted comments were worked into the text. Disputed comments had counter-comments added that were removed in subsequent drafts but provide stakeholders with justification of the comments' disposition¹⁸⁴. A challenge at this stage was to create a generic standard for ICT suppliers without knowing what the 'specialist' – then referred to as domain – segments of the standard would be.

Throughout the drafting of the standard, mind maps were used extensively to set out the structure and ensure that the level of instruction being given to ICT suppliers in each section was objective and not too detailed in one section at the expense of another. The mapping technique was useful for sorting requirements into two complementary taxonomies of requirements: requirements that were categorised according to their instruction of people, the management of the ICT supply process, or the measurement of how well the business is performing; and requirements that were categorised according to Deming's plan-do-check-act life cycle (Deming, 1950) that is applied across management system standards published by BSI and ISO¹⁸⁵.

These categorisations gave additional structure to the standard and encouraged debate with the reviewers as to where a requirement best fitted or whether a requirement ought to be set at all. The need for each requirement was tempered by involving both the suppliers of ICT (the business view) and the purchasers of ICT (the customer view). The objective of maintaining the standard to be detailed enough for quality assurance, but simple enough for the SME supplier to take time to study the contents was challenging. Review comments would be implemented by taking out material from the core of the standard (categorised as people, process, or performance requirements) to build a new mind map and develop them

¹⁸⁴ Comments disposition is the process of deciding which comments on a document will be implemented as received, which will be implemented but modified, and which will be rejected.

¹⁸⁵ Including ISO 9001 (quality management), ISO/IEC 27001 (information security management), ISO 14000 (environmental management), ISO 18001 (occupational health and safety management), BS 25999 (business continuity management), and ISO/IEC 20000 (IT service management).

further. In the early stages of development, impersonal language was used in the process titles to ensure that the Accredited UK standard stayed true to its more complex ISO counterparts. The titles were simplified in a subsequent draft. The early draft also included initial performance measures based on the 'Balanced Scorecard' (Kaplan and Norton, 1992), and also introduced the 'people' measures. The draft was developed taking greater cognisance of personnel issues from BS ISO/IEC 27002:2005 BS 7799-1:2005, explaining the SME status; and making copious corrections to the text. Sections bearing 'signpost' information only were highlighted for more development. These were developed with rich feedback from stakeholder reviews. Feedback suggested the need to include more 'case' examples throughout, more emphasis on the need to keep written records where needed, and the need for SME suppliers to formalise ad hoc activity. This information was tabulated (see Table 45) to produce a draft of sufficient detail to be worthwhile passing to BSI for its first edit.

Table 45: The core format of the Accredited UK standard			
Stage	Activity	Result	Examples
Plan, Do, Check, or Act	What the business should do.	The desired outcome of the activity.	Examples of how the activity may be done and the evidence that the activity is likely to have the desired outcomes.

The first edit of the draft standard by BSI highlighted the conflict of formats demanded by BSI's standard for standards (BS 0) and the understanding by the author that the SME audience would prefer direct, personal instructions as more appropriate to them and hence the increase successful uptake of the standard. It was agreed that the stakeholder groups would decide on whether to use the language of BS 0 which prefers passive descriptions with the term 'shall' to show mandatory action, or the direct, imperative statements talking straight to the reader. The stakeholder groups preferred the imperative language so that the edits changing them to passive 'shalls' reverted to the original. The justification was that the standard takes the approach that if it's worth doing then it is a requirement of the standard and must be done. Documentation of the instruction is a requirement and so referring to it as 'shall' is superfluous. This was the result of creating a standard for small business entities by paring the body of knowledge down to some 'absolutes' and missing out the potentially negotiable. Whether omission constituted a complete failure to comply became part of the assessment model which became richly formulaic – supported by good, professional judgment of assessors who must pass a benchmarking training course and test – to deliver consistent results.

Several subsequent drafts were then written by completing the requirements for SMEs set out in the headings included as outline placeholders in the material passed to stakeholders

for the early reviews. Workshops were convened with SMEs suppliers and purchasers who agreed the need for more detail on people/ competencies and the assessment regime. This wisdom was also incorporated in the developing standard. Significant effort was then put into filling in gaps in tables defining the People/Process/Performance activities that should be evidenced in an SME, making several typographical corrections, and adding a description of the proposed assessment process. An appendix specifying the characteristics that are required for assessors was removed because it was not relevant to the requirements placed on the SMEs.

Another stakeholder workshop was held which concluded that much background explanation and advice should be removed to make the core requirements more prominent. The Process and People sections were reordered to match the order that actions are likely to be carried out in, so improving the usability of the document. The use of terms 'certificate' and 'accredit' were changed to conform to accepted practices. Some customer activity references were also removed in anticipation of the creation of a separate 'Customer Code of Practice'. (At that stage of development, the branding of AccredITUK was adopted over the holding label of the 'ICT Supplier Standard'.) The review of the more complete draft led to renewed debate on the passive versus imperative argument. The compromise reached was to change the language of the standard to remove the second person conversational tone and replace it with the third 'person' so that the text refers to what a business, rather than a person, should do.

Improving the standard continued such as the better use of heading levels to aid navigation through the contents and correcting diagrams for consistency with the amended text. The layout was harmonised so the graphic designer who would typeset the standard could see the relative weight of each section. Some footnote-related defects in the word processor document were corrected. The 'technical' contents were also improved with clear recruitment ideals in the People section and a new introductory section to the Balanced Scorecard added. Because the supporting process for how the accreditation body would operate had not been defined, holding paragraphs were inserted to explain about the recertification period to ensure it would be adequately defined in the standard. This supported the general aim that the standard should be comprehensive in its coverage of the requirements on the business and how the business should operate. This objective was derived from observations of confusions and misunderstanding about documents published by national standard bodies which appear the same but have different normative and informative value (being labelled, for example: specification, code of practice, and technical report).

Another area of consistent feedback was the concern of the SMEs as to how compliance with the standard would be measured, particularly the risk that a business would fail an assessment if it failed to comply with a requirement that may be viewed as far less important when viewed in the context of absolutely essential business activities. Discussions with the

SMEs reviewing the standard, agreed that the standard should be rigorous and that the requirements it specified were indeed those which a business must meet to treat the risks that an ad hoc business process may overlook. One of the SMEs proposed that the standard should be aspirational so that it was not to be an easy 'tick box' exercise to measure a business against. This presented the paradox that an SME should not 'build a reputation on what it is going to do' and so increase the number of SMEs who would fail an assessment. The solution to this problem was to continue to define all the requirements of the standard as mandatory but to get the SME reviewers to work with the author of the standard to identify the minimum set of requirements that *would* indicate clear non-compliance with the standard's objectives if not in place in the business. The result of this was to define the requirements in assessment terms as 'Lines of Enquiry' (LoE) that an assessor would follow when looking for evidence of the requirement being met. A set of 'Key Lines of Enquiry' (KLoE) were identified as the core or baseline for compliance. A business that could not provide documented evidence of a process being managed to meet a KLoE would fail an assessment. Although there was no numerical basis for comparison, the Accredited UK Project Office agreed with the SMEs that a business could fail to show evidence for up to 5 LoEs and still be deemed as compliant. Compliance with a LoE or KLoE was set according to a maturity model scale shown in Table 46 where the score of 3 was set as the minimum level of compliance expected.

Table 46: Accredited UK Maturity Model for Process Evidence	
Score	Interpretation
1	Unacceptable
2	Improvement Required
3	Acceptable
4	Good Standard
5	Ideal

The activity of the Accredited UK Project Office – which had worked through the process of engagement with the selected assessors – and the SMEs who had volunteered to take part in pilot assessments of their businesses against the standard were then monitored in the context of this research. The activity involved assessors visiting the SMEs and finding out what evidence they would present to an assessor to show compliance with respective clauses in the standard. The assessors then met to compare the range of evidence that an SME would be likely to present during an assessment so that it could be scored in relation to the model shown in Table 46. This maintained the aspirational objective of the standard because it allowed scope for improvement for SMEs who may just meet the 'Acceptable'

level. This maturity model also satisfied the SMEs reviewers who were concerned that there may be certain requirements which would not be applicable to a particular business, which it would then be expected to carry it out for the sole aim of being able to say it complies with the standard rather than meeting the objective the standard itself (the management of risk during the supply of ICT products and services). If an assessor agreed that an activity was not relevant to the respective SME, then they would be scored as 'Acceptable' – the minimum requirement (level 3).

The result was an assessor's handbook that documented sample evidence across the 1 to 5 scale for each LoE and KLoE. This provided a benchmark for assessors to manage the risk of different assessors awarding different scores to KLoEs or LoEs at the same level of maturity in different SMEs. Assessments of the pilot group of SMEs could then be carried out as a vanguard for the full scheme.

Table 47 summarises the results and interpretation of Project ε (Accredit UK).

Table 47: Results and interpretation of Project ε (Accredit UK)		
Results	Lessons learnt	Evidence and organisational idiosyncrasies observed
This project yielded a rich record of stakeholder views about the content of a standard and the process for reviewing that content for acceptability by the stakeholder groups. These included representation from small businesses that would be expected to comply with the standard, their trade bodies and regional development agency, and the customers whose demands were expected to be met more readily through their supplier compliance with the new standard.	This project shows what is done to define a new standard. Confidence in the standard moves from uncertainty to assurance as stakeholders are involved.	The interaction of stakeholders in the determining of what needs to be captured in a standard to mitigate risk in the procurement of ICT from small to medium-sized enterprises.

5.5.2 Project ζ: The Local e-Government Standards Board

The work on Accredited UK served to investigate and validate the processes involved in setting standards and creating a certification process to benchmark organisations against a set standard. The LeGSB case study was interesting from two aspects. The first was that the case study did not just involve defining a standard for the organisations delivering a service themselves to meet, as in the Accredited UK example, but that the artefact to be created was a standard about standards – a metastandard – that set out how other standards should be defined. The second aspect that made this case study of particular noteworthiness was the process of testing the efficacy of a standard for standards in its ability to define or select the actual standards to be adopted by a community. However it must be noted that during the interregnum between the definition of the standard for standards and the test of the process for adopting standards, the commissioning body lost sight of the metastandard and created a second document based on their assumptions of practices in standards development and without the rigour applied to create the original. For example, in isolation from references to accepted practice amongst standard setters, the owning committee of the developing standard defined the term ‘certification’ as the acceptance of a standard into its corpus rather than the accepted definition of it referring to the benchmarking of an organisation against a standard where certification refers to the granting of a certificate of compliance.

The early desk research involved looking to see what other standards bodies did to assure sufficient rigour in the assurance that the standards that they set are likely to solve the problems that they have been allocated to manage. These methods are discussed in Chapter 2. A process was defined using the basic ‘BS 0’ method but tempered for the size of LeGSB and the likelihood of it being able to convene enough subject matter experts to review standards in specialist areas as is carried out by BSI.

The first draft that was sent to LegSB for review included introductory material such as definitions of the life cycle and scope of the LeGSB standard for standards document and how it would be applied to the taxonomy of LeGSB work. This involved the opportunity to define work streams for each standards-related area and the proposed life cycle for each standard from a proposed need to a standard through to its obsolescence or withdrawal from the LeGSB corpus of standards (see Figure 35).

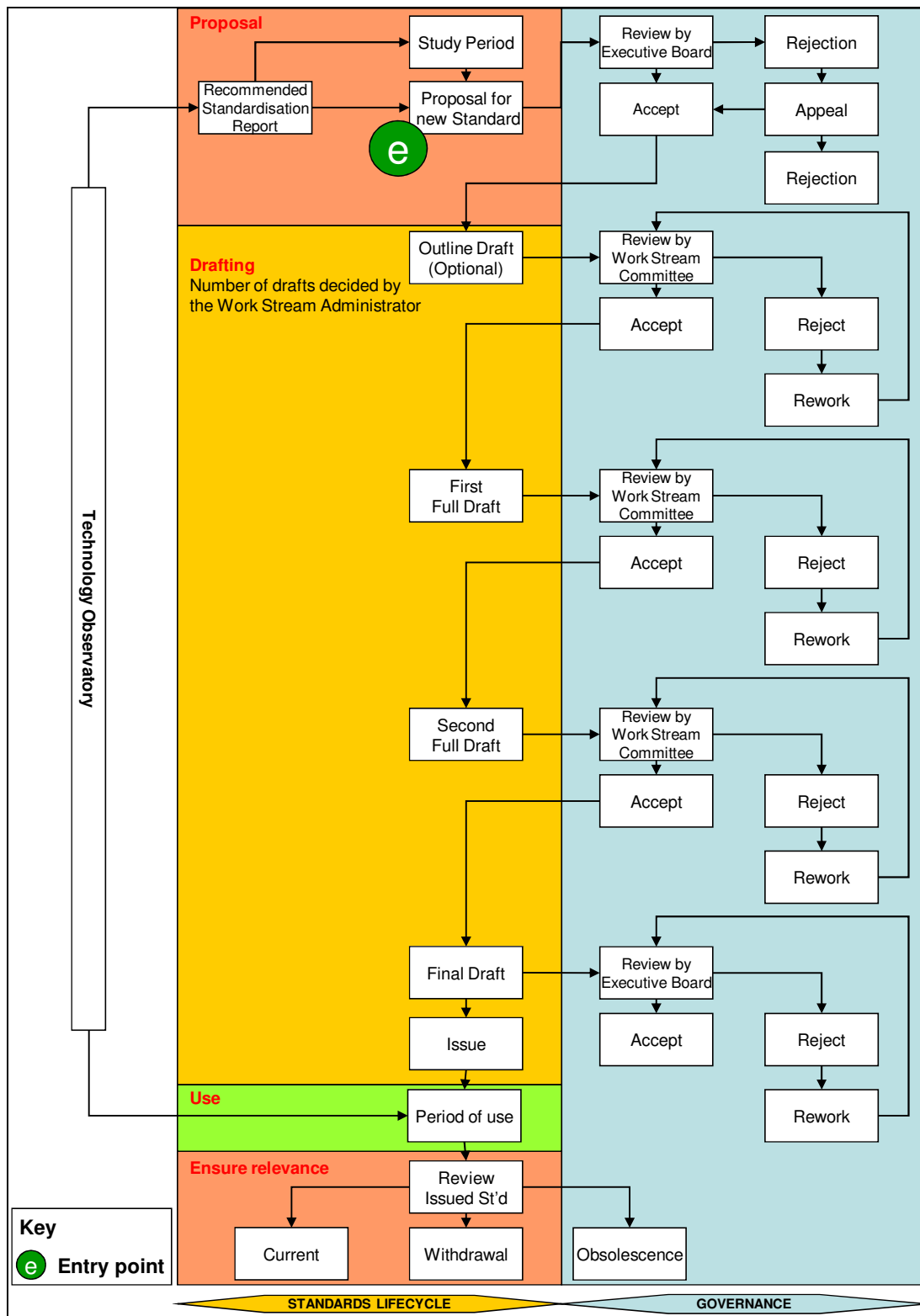


Figure 35: The LeGSB standards life cycle

Six iterations of the standardization definition document were produced in response to the initial commission and the comments received from the reviewers. Process diagrams were added and the imperative tone of the text expanded to more descriptive text. Some pagination improvements were made and some small changes to terminology for example,

the 'Initial Draft' of a standard was referred to in subsequent revision as the 'First Draft'. Some governance changes were made to the process. For example, acceptance of a proposal (for a new Work Stream or standard) became the remit of LeGSB's Executive Board. The term 'Observer' changed to someone in receipt of 'Information Only' to differentiate the role from a proposed Technology Observatory that would look for areas of developing technology where standardisation would be needed.

The LeGSB development process for creating standards was presented as a single recommendation that would make best use of the resources available to LeGSB, adopting a sustainable standardization model derived through the desk research of the process definitions from existing standards bodies. Two artifacts were created specifically to de-risk the standardisation process itself. These were a participation charter for contributors and reviewers to agree to, setting out their obligation for timely participation in reviews (to reduce the lag between identifying the need for a standard and defining that standard) and a conflict of interest declaration to allow controlled access from representatives of vendors or those who are, for example, on the standards-making committees of other organisations. The purpose of the latter was designed to control the development of standards that favoured a commercial offering yet allowed the expertise of the vendor community to be tapped and to avoid over-promotion of an existing standard that may not be in the best interest of LeGSB's thrall.

The completed specification of the 'Local e-Government Standard Board: Standards Development and Adoption Process' was handed over to the consultant overseeing the project in the expectation that this reviewed specification would define the modus operandi for LeGSB to build up its own sector-specific repository of standards that would be trusted by its stakeholders. However, this was not realised and I was commissioned to test the processes defined in a specification of 'e-SB Standards Certification Process' (where e-SB referred to the e-Standards Board, the successor by name to LeGSB).

A meeting with e-SB was arranged to confirm the work plan and the methodology with particular reference to levels of authority and the responsibilities for granting access to their on-line document repository (Custodian) during the pilot. e-SB created the first RFPs and handed them over to be driven through the subsequent process steps. Once the first candidates for RFPs/RFCs were actually in hand, the degree of rigour to apply to the community and stakeholder consultation and the appropriate time frame for any pilot adoptions/implementations was determined. For example, reviews of standards that were wholly documentation based could be expected to be much quicker than reviews of standards also requiring consideration of technical implications (that may have to be tested with hardware and software). Similarly, where technical considerations extended as far as requiring pilot implementations, it seemed most effective to seek to piggy back on existing implementation projects to expedite the review quickly – these had to be found and engaged with formally.

The initial discussions set the goal of teasing 5 RFPs through the ‘certification’ process to get a clear view of how the process would affect different sorts of would-be standards. However, the proposal registered as RFP004 was sponsored by a supplier and not by a local authority as required by e-SB rules. This was therefore withdrawn. The remaining four RFPs (Table 48) were deemed, in discussion with the e-SB Chief Executive, to be a representative sample.

Table 48: RFPs selected to test the standards adoption process	
RFP	Proposed standardisation
RFP001	A set of XML schema to support data integration for Choice-based Lettings.
RFP002	A set of Data Definitions from GovTalk, a document repository run by the Cabinet Office to distribute standards and templates to support the e-Government Metadata Standard (e-GMS).
RFP003	The Local Government Category List for the delivery of e-Government services.
RFP005	(of which more is said later) was eventually joined by RFPs 6, 12, and 15 as proposed standards for data sharing protocols.

To prompt meaningful discussion and useful commentary from would-be reviewers, a detailed review questionnaire for each RFP was prepared. As the work developed, some initial delays, (for example, compiling distribution lists of reviewers) were not allowed to extend the boundaries of the closed consultation so that it would be apparent how much could be done within that period. The Chief Executive of e-SB was kept informed of the plans, activities, and issues as the pilot progressed. Issues with individual RFPs were referred to the e-SB Standards Consultant (the lead contact for the RFP) championing the respective proposal.

In addition to the framework in the e-SB Certification Process Guide, ‘additional’ activity with e-SB to realise the process was agreed; as the process matured with a developed register of contributors and reviewers, some of the initial engagement correspondence, to entice participants, would not be necessary. The realised method for the trial is set out in Table 49.

Table 49: Trialling the standardisation method

Step	Activity
1	Material for each proposed standard was uploaded to the e-SB website within the Custodian library and encapsulated in a 'Request for Proposal' (RFP) form that noted the content and described the provenance of the material under consideration.
2	Each proposed standard had an appointed e-SB Standards Consultant who would assist in the development of a set of questions that would elicit useful responses from reviewers of the proposed standard(s). Each standard had its own set of questions – this was based on a proforma outline that was extracted from NCC's document review process, supplemented with ideas drawn from a North West e-Government Group (NWEgg) consultation which was forwarded by one of the e-SB consultants. These were provided to reviewers in Microsoft Word format so that they could use the 'Track Changes' function to highlight their comments.
3	The specialised questionnaires for the consultation became the basis of a library of editable review documents to be employed according to their type/category in future e-SB standards reviews. These were designed to elicit feedback in a familiar format for both reviewers (as they become used to the process) and the analysts who synthesise the comments into a coherent single strategy to issue, develop, or reject the proposal(s).
4	For each proposed standard, a discussion thread on the Custodian section of the e-SB website was set up. This comprised a note about each proposed standard, the deadline for comments, and a link to the source material.
5	Each e-SB consultant provided a list of participants for their respective consultation, with the support of the local authority sponsor of each proposal.
6	The Chief Executive sent out a vanguard e-mail 'warning' of third-party involvement in the review to all participants, and requested their cooperation and participation. This was a significant support because of local government practitioners who would not readily accept proposals that appeared to come from outside their ranks.

Table 49: Trialling the standardisation method

Step	Activity
7	<p>Following the Chief Executive's announcement, an e-mail directing each reviewer to the material relevant to the proposed standard under review was distributed, and included the respective, specially prepared question set. An attempt to create some 'momentum' was put in place by asking for the nominated reviewers to themselves nominate other contributors but before they get down to review the material so that these additional reviewers could be given as close to the six weeks elapsed consultation time as possible. The additional names were added to a register of reviewers. With the exception of the data sharing protocol proposal(s) – RFP005 et al. – there were few additional names added during the closed consultation period.</p>
8	<p>A separate e-mail followed the original to persuade closed consultation participants to use the on-line Custodian forums. This could have been included in the original invitation e-mail but this would have significantly added to the length of that communication.</p>
9	<p>When comments were returned, these were gathered together from the marked up review documents and a collated report was sent to the respective e-SB contact for each RFP.</p> <p><i>Note: The original intention of adding in comments from the Custodian forums was not necessary with the exception of one comment in overall support of RFP001 and general input for the 'recalled' data sharing protocol proposal(s) as little use was made of the on-line facility.</i></p>
10	<p>A summary of the collected comments (for RFPs 002 and 003) was collated and reported on a Board Approval form that was introduced into the process, during the pilot, for proposals which did not need to go to open consultation/RFC voting, or (in future) will have been through the RFC voting stage. (At which point the Board Approval becomes a quality control to assure the passage of the proposal/RFP through the appropriate open/closed consultation process and the correct disposition of the comments received during the consultations.)</p>

The on-line discussion forums (*Step 4 in Table 49*) were an isolated facility on the e-SB website that used an open source software threaded-discussion application (Snitz). Some initial discussion suggested that it may be replaced by a proprietary package from the service provider of e-SB's website but as this was untested, a decision to retain the 'Snitz' environment was taken by e-SB. This was timely because it meant no delay in activating the forums for this pilot, and had no implications on the knowledge of the e-SB technical coordinator or myself who were both well versed in the Snitz tool. It became apparent that this decision was worthwhile because the lack of response, in this pilot, to the use of forums

suggests that they may not be an effective consultation tool in this community. However, capitalising on the good experiences of other forums might still have been an option and this is discussed below.

The forums for the pilot were set up in consultation with the technical coordinator of e-SB. It was agreed that because the named groups for the closed consultation(s) were on the recommendation of board members, the Moderator function did not need to be used for the pilot. The moderator function would be used for 'open' discussions after the pilot to pick up on emotive comments that may arise, and understand local sensitivities. This formed a recommendation in the report of the trial and was based on based on experience of managing NCC's knowledge network forum.

The place of the forums in the closed consultation was questioned by one of the e-SB standards consultants, remarking that the questionnaires distributed with each proposal should promote enough commentary from reviewers. It was noted that the creation of the forum facility for each proposal was to allow contribution through as many channels as possible. On the whole, the key information came through responses to the questionnaires.

To ease the burden of administration, and more importantly allow instantaneous access to the forums, it was decided to allow participants to register themselves. They could then access the closed consultation forums straight away using the password contained in the e-mail (q.v.) drawing their attention to the facility. The level of confidentiality of the discussions was not seen to exclude the traditionally insecure method of distributing passwords in this way.

An occasional user did have problems down loading documents or registering for a forum. This had a minor time implication for the convenor of the forums who was expected by the users to offer the technical support also. This was a minor distraction for a limited consultation but could become more onerous as activity develops. This is not least because the configuration of a users own information technology can affect their connectivity and there is an expectation that the central facility (in this case Custodian) would either be (incorrectly thought of) as the source of the problem or as having the duty of care to provide the corrective of workaround for the user. At least one problem recorded during the trial was a user unable to read the '.zip' file of RFP material. It was clear that this was a result of trying to open the file direct from Custodian (theoretically possible, but not a stable process) rather than downloading the '.zip' file first. e-SB already had a clear source of technical support and the communications channel between the e-SB technician and the project to trial the standards adoption process worked well.

To get the closed consultations running, some peripheral documentation/instructions were created as the various RFPs were distributed for comment. This minimised the time taken to follow the critical path. To help to create a repository of products from the pilot, the various proforma items created were appended to the project report. After two weeks of no

contributions in the forums, it was suggested that each e-SB contact for the respective RFPs add an opening message to their forum/forums. This suggestion was not implemented.

It was useful to create an RFP progress log (as a spreadsheet) to keep track of the various proposals, the responses coming in, and the actions upcoming (such as sending out reminders to the would-be reviewers). The headings were added as they became apparent, and it suggested that a useful, formal tool should be programmed for project management of proposed standards through the review process, with traceability to a level of detail that can be followed by others staffing the process. This could ensure that leave, sickness, turnover etc. would have a minimal effect on the process. It would also be useful for internal audits for the quality assurance of the process.

RFP001 – XML Schema for Choice-based Letting

The proposal to standardise on XML Schema for Choice-based lettings, RFP001 tested the standards adoption process in two ways. Firstly, RFP001 was a specialist technical standard for a specialised area of local authority housing activity. It would therefore have to appeal to technology specialists (XML) and (indirectly) those who will be serviced by the systems that apply the standard. Secondly, it was the most difficult to elicit timely responses from those practitioners and local authority representatives that were invited to comment on the worthiness of the schema for standardisation. It may be noted that the RFP005 – which was coupled with several other RFPs for tiered data sharing protocols – also had few responses as compared to the list of names to whom the opportunity to comment was given, but the depth of response from the few who contributed delivered significant thought leadership on the approach for that collection of RFPs.

e-SB gave the direction to manage the proposal through a discussion following its receipt from a relatively closed source of a few users. It was noted that the material was distributed in several files and centred on a 'zip' file of 6 megabytes. The proposed standard was well recorded from the point of view of the amount of documentation; however where to start, and the relevant importance of the documentary items supplied, were not clear to reviewers. There was a clearly defined standard up for adoption but there had been no comprehensive set of comments about this standard. This might have been the result of (a) insufficient time to digest the material and to comment, (b) no interest in the subject, or (c) nothing to add to the discussion. If (c) then there should have been better effort to elicit such feedback.

RFP002 – UK Government Data Definitions

This proposal was to settle on the use of 8 definitions from the UK Government Data Definitions Catalogue from the Cabinet Office e-Government Unit information repository GovTalk. As this was from an established, 'open' source, it only required the closed consultation to validate the adoption. The information was supplied as an HTML page of links to the Data Definitions (from GovTalk) being proposed for certification. To send out a single document with all the items under review, an Adobe Acrobat PDF file was created and

the observation made that there are likely to be many RFPs of this sort. Because of this potential proliferation, e-SB should have been proactive in (a) reviewing the GovTalk content at the time, and (b) raising RFPs based on collections of relevant/related standards, and then maintaining a watching brief for new additions.

The reviewers for this were drawn from members of the Cabinet Office e-Government Unit (eGU) process and schema groups, local government people who had used the definitions in schemas, and suppliers to local government projects who had used the definitions in local authority schemas.

RFP003 - Local Government Services List

This proposal was for the adoption of the Local Government Services List (LGSL) from the local government e-services delivery (esd) toolkit as a standard. As with the data definitions of RFP002, the 'open' source suggested that the proposal only needed a closed consultation to validate the adoption, not least because of the trust that local e-government practitioners have in the research and maintenance of esd toolkit. However, although the adoption seemed straightforward enough in concept, there was a need to keep a close eye on 'additional services' which may need to be added so that they can be recorded separately and voted on for standardisation when the list became open for amendment (it had been frozen to promote its use as a stable entity). This tallied with a recommendation for a proactive standardisation observatory to be operated by e-SB (rather than waiting for external proposals from local authorities) which was similar to the proactive review of the GovTalk contents referred to above.

RFP005 et al. - Tiered data sharing protocols

In hindsight, the effective way of progressing standardisation for this – tiered data sharing protocols – would have been to initiate a process that proposed a standard for tiered data sharing (RFP) and then settled on the format to be proposed as a standard. This would be an example where several RFCs could bud from the proposal with a decision as to which one(s) would be adopted.

From the outset it was noted that this was not a topic area for a closed consultation with a restricted number of reviewers; it needed a very wide debate on this to get to an agreed position. This was reflected in the growing number of proposed contributors who themselves brought forward new, potential protocols as candidate standards (hence the 'budding off' analogy above). The actuality was that each protocol was registered as a separate RFP so that it became unclear as to whether it was an 'all or nothing' approach, or whether a complete set of proposals had been reached. This problem was exacerbated further by the rumour that central government guidelines for data sharing protocols were scheduled for release that autumn. The (then) Department for Constitutional Affairs (DCA) was contacted and its representative explained that DCA's current (2004) toolbox was still valid. However

they had intentions to update it but a proposal for this update was still being prepared for ministerial approval.

A more thorough, explanatory questionnaire was prepared for the collection of protocols, but this did not foresee (a) the growing number of suggestions that were being brought forward or (b) the bias from certain participants who naturally favoured the protocols that they had either used or had developed. This latter problem may not always be a problem in the assessment of standards but fundamental differences in the number of tiers a protocol should have were registered. It was also noted that one was oriented towards a particular suppliers 'solution'. In the light of these variables, the corresponding proposals were withdrawn to be used as input to a coherent proposal for standardisation in this area.

Table 50 summarises the results and interpretation of Project ζ (LeGSB).

Table 50: Results and interpretation of Project ζ (LeGSB)		
Results	Lessons learnt	Evidence and organisational idiosyncrasies observed
This project delivered detailed recommendations for establishing a sustainable process for setting standards that would increase the risk of the acceptability of the selected standards from the viewpoint of the stakeholder who would be expected to implement them.	LeGSB required a process to select standards to address areas of risk and it was through this process that they would engender a consensus view of acceptable standards.	A close-knit community of local government officers showed a tendency to either create their own standards and become leaders in the field of the standard or cautiously work around the area of standardisation in anticipation of change that would be effected by a new standard that they foresaw as emerging.

5.6 Fieldwork: the deployment of standards to treat risk

5.6.1 Project η: Housing association – information systems risk (security) strategy

The context of information security risk that the housing association required a strategy to treat was represented by three information attributes – confidentiality, integrity, and availability – that could be managed by the standard ISO/IEC 27001 for information security management. Confidentiality in practice would be where some information is suitable for dissemination to the public or to tenants yet other information is highly confidential to a few individuals. For the strategy – the localised implementation of the standard – a level of practical labelling information would be set to show its confidentiality in a consistent and

visible manner and ensuring that those without the appropriate level of privilege cannot access it.

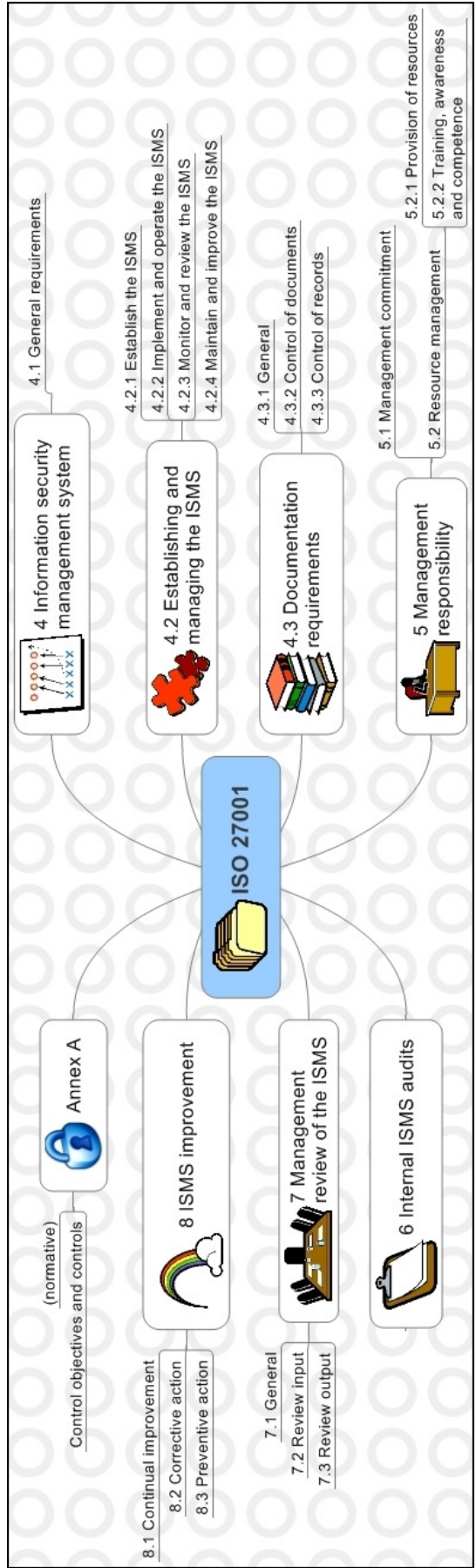


Figure 36: The structure of ISO/IEC 27001 for information security management

Availability was referred to the responsibility of information owners to put measures in place to ensure that their information will be available as staff and tenants expect it, and integrity was the propensity for staff, tenants, and other stakeholders to trust the information that they are basing their decisions on to be accurate, complete and up-to-date.

Table 51: Project η: Method for defining an information systems risk (security) strategy in a housing association	
Step	Activity
1	Project planning, organisation, assumptions and risk management
2	Interview planning and design
3	Structured interviews
4	Analysis of information gathered during interview
5	Preparation of draft information security strategy
6	Peer review of draft information security strategy
7	Revision and issue of the information security management strategy

To ensure an understanding of the research and reporting methods being employed, I created a Project Initiation Document (PID) for the association. This provided an agreement covering the objectives of the research, the scope of the investigations and the terms of reference for the work (BS ISO/IEC 27001:2005 BS 7799-2:2005); how the research was to be carried out – and what artifacts by way of reports or presentations the research would produce; the governance of the project defining relationship between the association's management (the project sponsor), other staff across the association, and the researcher; the likely risks to the research and how they would be mitigated; the assumptions the research would be based on and the pre-requisites to be in place at the association to make the research schedule effective. The PID also defined the quality assurance processes for the deliverables.

The sponsors of the project were selected to have sufficient status and authority to ensure that the project was recognised as a strategic priority. This led to the establishment of a high level and influential Project Board, with reports being received from an effective Project Manager. As many stakeholders were involved in the project, a Project Briefing was prepared for all of them to ensure that they were informed about the scope, objectives, and opportunities. At a practical level this saved the time of the analysts in explaining the objectives of the project and what was expected from meetings with each stakeholder individually.

Information gathering was designed to draw up a comprehensive understanding of the business/service context of the housing association. The business/service policies and priorities would then be prepared to drive the recommendations for secure exploitation of the association's information technology. This required arriving at a view as to how the housing association will operate in business terms in order to propose the optimum systems configuration for the future. Clearly the technologies proposed would have to not only provide for immediate requirements, but also for future developments. The first stage of the information gathering was reviewing available documentation such as corporate/business plans, before moving on to IT-related strategies and standards.

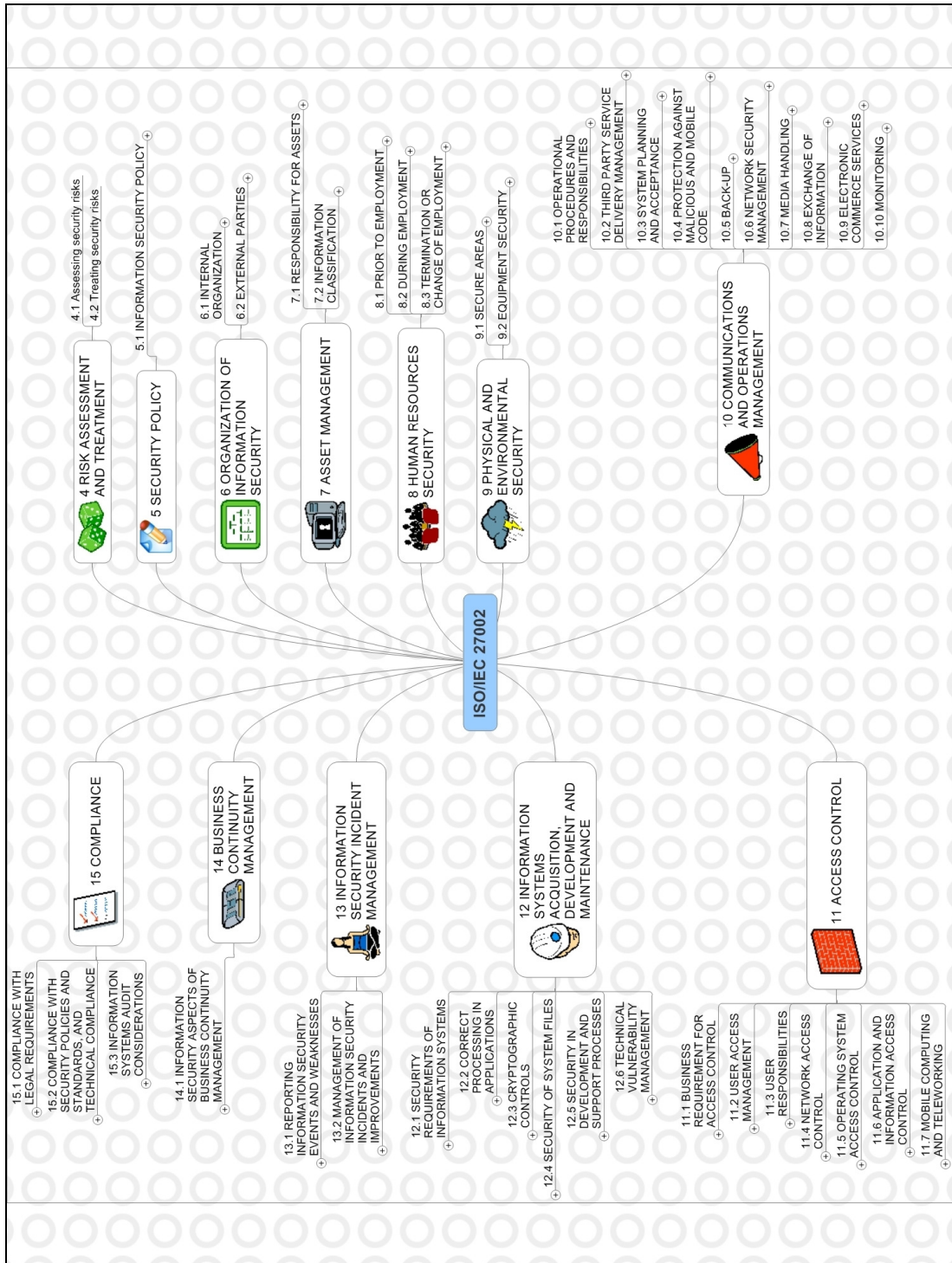


Figure 37: ISO/IEC 27002 controls for information security management

A structured programme of interviews for collecting information using the information security control objectives of ISO/IEC 17799 (ISO/IEC 27002) was prepared to ensure that there would be consistency across the project, in terms of the level of the information acquired. The objective of this was to build up a complete store of factual information, knowledge of strengths and weaknesses and aspirations. This approach enabled those with minimal knowledge of information security to express their requirements in non-technological terms. Line managers involved in the fact-finding were selected for their knowledge and

representation of strategic and service management requirements. The basic structure of each interview examined the closeness of the realized information security risk management processes of the association, with the practices defined in the ISO/IEC 27001/27002 standard(s). This started with asset discovery and asset management, to understand how well the association knew about, and kept, records of the information it held to effect its business processes.

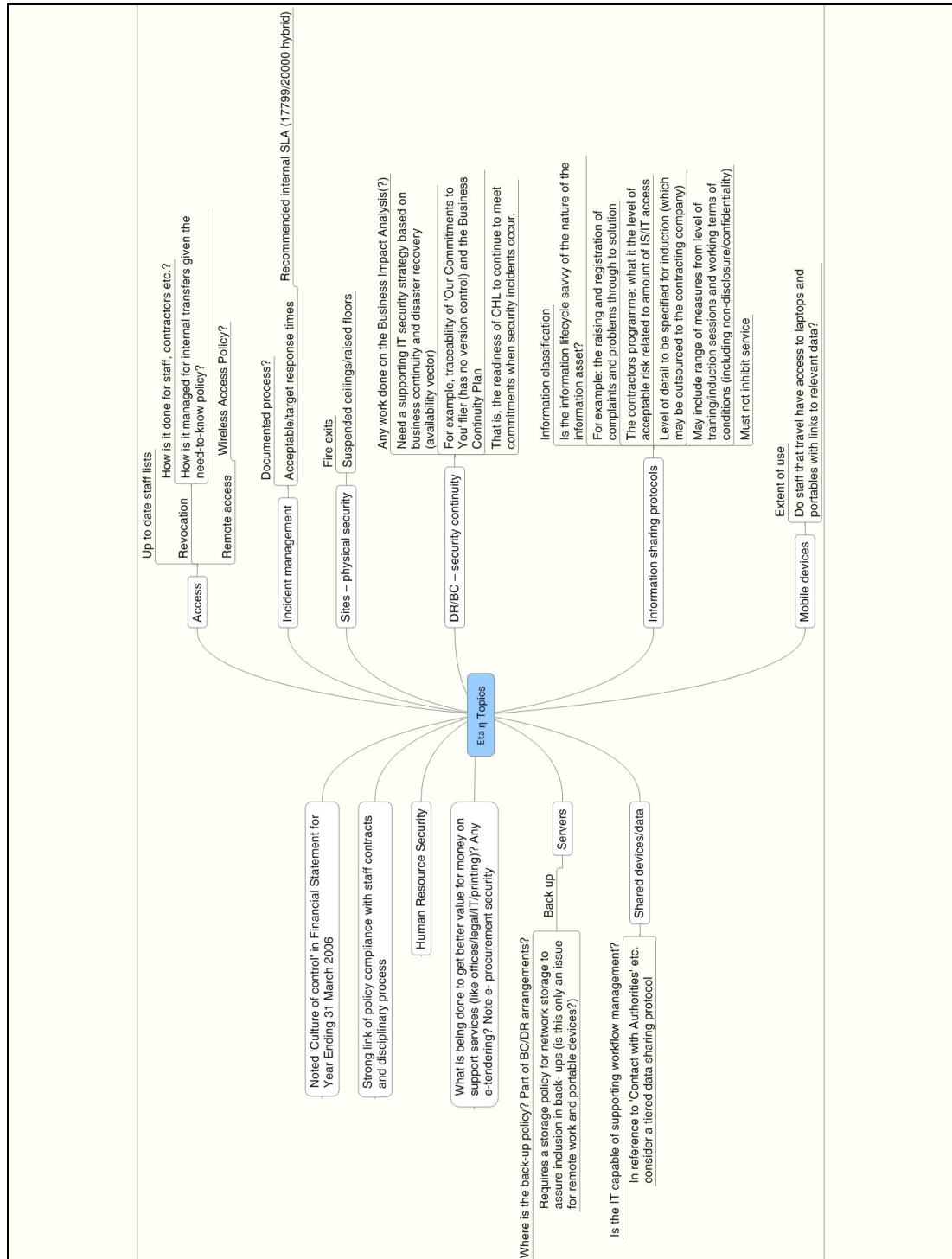


Figure 38: Structure for the questions repeated across the stakeholders interviewed

When information gathering was completed, I compared the current practice with that set out in ISO/IEC 27002 and documented the options for consideration for inclusion in a future security strategy. These were then presented in a report to provide opportunities to test options individually, and in combination to eliminate options that are not feasible and produce further options, resulting from the review. The report could then be refined and published as the definitive strategy to work to.

The project set out to mitigate the risks where its method could be affected by the quality of information and the availability of stakeholders for interview. These were based on the specific project risk which required that all relevant documentation would be available for review at the start of the project, and that all relevant staff would be available for consultation during site visits. The mitigation of these risks was based on the early identification of personnel to be interviewed, any additional documentation required and visits to other offices. A project start date was agreed with confirmation that all staff, documentation, and access to premises would be available. Relevant staff agreed and confirmed their availability during the analysts' visits. During the early review of the information security related documentation that the housing association could show on demand, a selection of information handling policies were already apparent that could be extended to explicitly direct categorised information to those who need – and have a right – to know (an example of the effect of legislation as a standard as described in Chapter 2). This could be implemented by an asset/risk/impact-based model to that would treat risks associated with business continuity and disaster recovery (as implemented in Project θ). The recommendations referred to the establishment of policies – localised standards – that would be commensurate with the corporate responsibility that the housing association has for the information it deals with. Applying Deming's management cycle (Deming, 1950) favoured by BS ISO/IEC 27001:2005 BS 7799-2:2005, the extension of the existing policies would be carried through to defined processes setting out the method to manage risk (plan), introducing a supporting framework of training and awareness (do) and followed up to ensure compliance with the policies (check), reviewed to a schedule for continued relevance to the association's mission (check) and enforced or amended as necessary (act).

5.6.2 Project 0: Fieldwork in construction – risk to treatment analysis

Table 52: Method for project 0: fieldwork in construction – risk to treatment analysis	
Step	Activity
1	Project planning, organisation, assumptions and risk management
2	Interview planning and design
3	Structured interviews to inform the content and detail of the workshop programme
4	Analysis and design of a workshop programme to support the company in learning about and implementing information security risk management
5	Workshop I: Information security management training and information security policy writing
6	Workshop II: Risk assessment (carried out on two sites)
7	Workshop III: Risk treatment

Option 3 from Table 42 was selected because it would provide the client with the best fit of the standard to its operations. The methodology was applied by convening a project initiation meeting between the action researcher and the organisation's Director of IT. This meeting was used to reconfirm the scope and timescale of the assignment, discuss any sensitive issues, identify staff to be involved with the project, and agree contents of a project briefing for all staff who will be involved with the project. Site visits to two of the organisation's 3 offices were arranged where interviews were convened with business process owners and support staff (IT manager, business systems manager, systems administrator, representative(s) from operations, quality manager, financial controller, and human resources director) who could articulate the detail of the information they handled and the need for protection of that information. Three workshops were planned using the information from the structured interviews to create ISMS artefacts: to teach the writing of information security policies; to design and begin populating a register of information assets and risks to the confidentiality, integrity, and availability of those assets; and to develop a risk treatment plan to show how the information assets will be protected from the risks identified during the preceding workshop.

After the information security policy writing workshop, staff undertook to spend time using a template to complete a first draft of the security policy documentation. This was carried out by prioritising about a dozen individual policies to be completed as a basis for working on in the context of the second, planned workshop (Risk Assessment). Ownership of the policies – to assure that they would be written by those whose area of responsibility they cover –

was confirmed. The policy owners were encouraged to get together with their contributors within two weeks of the workshop to begin the drafting work whilst their experience of the workshop was still fresh. On request of the client's project manager – who thought the policy areas were too generic to inform the owners as to the required content – I prepared templates with some sample content. These provided the policy owners with more explicit instruction as to what was needed to control information security.

Although this was done before focusing on risk assessments, it had the advantage that staff could immediately bring in known issues within the boundaries of organisations ISMS. I reviewed the draft policy documents and prepared and convened a second workshop to present feedback and provide risk assessment training based on the client's business activities (as derived from the structured interviews). This second workshop was followed by the client conducting a full risk assessment project to produce a report that identifies acceptable levels of risk. The draft policy documentation was updated to reflect the findings from the risk assessment. I then reviewed the risk assessment report and prepared a third workshop covering tools and methods – defined by ISO/IEC 27002 – that may be deployed to mitigate the risks. The result of this third workshop was the development of an information security policy manual and a statement of applicability (which specifies which controls should be deployed where) and a risk treatment plan which applied the following mitigation methods: prevent realisation of the risk (stop it happening), reduce the effect it has, transference (making treatment the responsibility of someone else – perhaps an outsourcing arrangement), contingency (having an alternative way of working if the risk is realised), and acceptance (recognising that the risk is just too onerous to mitigate, or its impact too negligible to worry about, and so that the organisation will carry the risk and its impact if realised).

5.6.3 Project 1: Pensions and actuarial services – risk management (security) policies

Table 53: Method for project 1: A review of risk management (information security) policies in a financial services firm delivering pensions and actuarial products.	
Step	Activity
1	Project planning and initiation
2	Short audit of current information security arrangements
3	Review existing information security policies for the holding and subsidiary organisation
4	Preparation of structured interviews to understand risks and organisation’s culture
5	Structured interviews with staff
6	Gap analysis of responses: the difference between actual and recommended information security practices
7	Collate existing information security policies and revise in context of interviews and benchmark with ISO/IEC 27001
8	Review the drafted policies with the company
9	Revise the policies and issue them for implementation

5.6.3.1 Review existing information security policies

A thorough review of the holding company’s documentation was carried out against the relevant parts of the BS 7799 (ISO/IEC 27000) standard series. This was repeated for the policies that had been drafted for the subsidiary company covering existing, relevant subsidiary company IT and HR Policy documents.

5.6.3.2 Preparation of structured interviews to understand risks and organisation’s culture

Structured, in-depth interviews with staff were carried out to audit a sample of activities from different business divisions and office locations to assess what practices were implemented. This included the IT support manager, a network support analyst, the human resources manager, a senior HR officer, an actuarial services partner, a general insurance consultant, a risk-benefit unit consultant, an investment consultant, the facilities administration manager, and the IT director.

5.6.3.3 Gap analysis of responses

The records of the structured interviews were analysed to identify any discrepancies / gaps between the subsidiary and holding company practices, the requirements of the holding company, and industry good practice.

The company's existing information security policies were collated and revised in the context of the interviews and benchmarked with BS ISO/IEC 27001:2005 BS 7799-2:2005/BS ISO/IEC 27002:2005 BS 7799-1:2005. The result of this work was a draft report showing gaps in compliance with accepted good practice and recommended changes to the management of security to comply with the good practice.

5.6.3.4 Review and revision

The report was reviewed with the IT manager of the subsidiary company and his feedback and the report were used to update the draft information security policy manual for issue.

5.7 Resulting intervention

In this last major subsection of the chapter, I consider the instructions given to the three organisations who commissioned the fieldwork. The implications of these interventions – the lessons learnt from the projects in relation to my research questions – are discussed and tabulated in Chapter 6. The details of these interventions show how the clauses of a standard may be extracted and applied as specific risk treatments in a rich mapping of a standard to the risks.

5.7.1 Project η: Housing association – information systems risk (security) strategy

This subsection sets out the implementation of the parts of ISO/IEC 27001 and 27002 standards that would treat the risks to the housing association's information systems. I acknowledge that these address known risks, but note that the handling of emergent risks is possible through a generic learning process triggered by incident management (hence recommendation about this to the association including counsel to implement the international standard – PD ISO/IEC TR 18044:2004 – for this discipline). The housing association's aims and objectives were summarised in two core documents. One was externally focused for its customers entitled '*Our Commitments to You*', and the other was for internal instruction: a business continuity plan that established the readiness of the organisation to continue to meet those commitments when information security incidents occur. The following observations and interventions were specified to support the goals set out in those two primary documents.

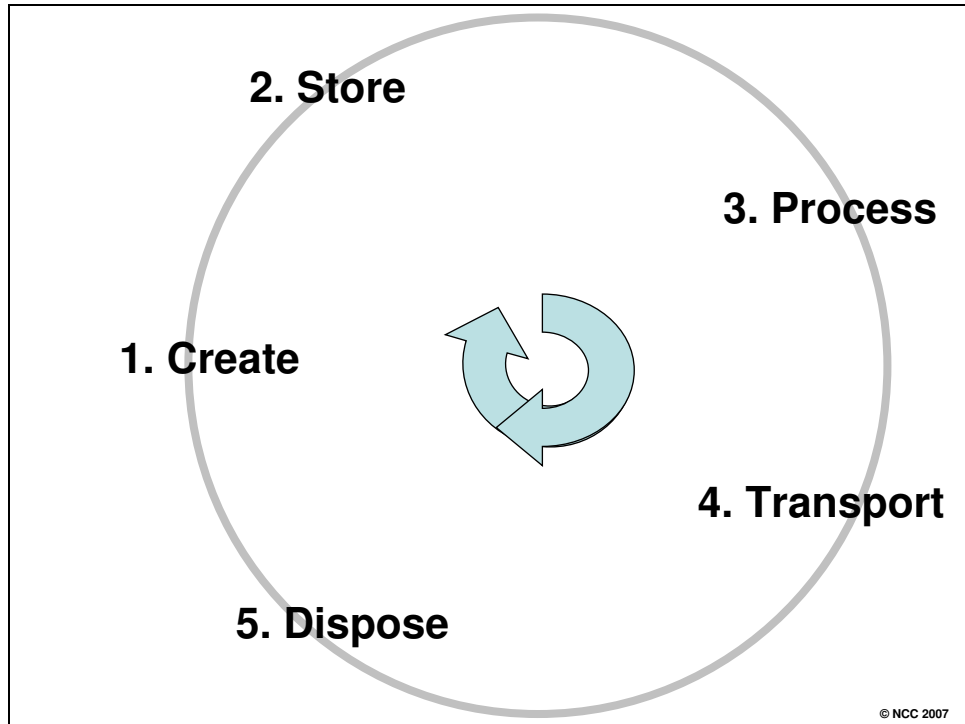


Figure 39: The organisation’s information life cycle

In regard to this, a report made the following key recommendations for the housing association (Project η), tabulated in Table 54 and detailed below, set out in the ISO/IEC 27001 taxonomy:

Table 54: Recommendations for the housing association target of Project η		
	Observation	Recommendation from the information BoK
1	The organisation’s information system is a technology-supported capture, processing and reporting mechanism that underpins the supply of housing and related services within a social context (Figure 39). Information is a core asset and must be treated to the same scrutiny as physical assets that may be more easily measured in financial terms.	Bridge the gap between the document retention schedule and the business continuity plans by addressing the risks to discrete and collected information assets This will support the realisation of business continuity which is currently aimed at bringing information technology back on-line. It should be extended to the appropriate availability of information assets. (Figure 40)

Table 54: Recommendations for the housing association target of Project η

Observation		Recommendation from the information BoK
2	Apply standards to the organisation's goals for the security and effectiveness of its information systems provision.	ISO/IEC 27001 (BS 7799 Part 2) <i>Information technology. Security techniques. Information security management systems. Requirements</i>
		BS ISO/IEC 17799 (BS 7799 Part 1) <i>Information technology. Security techniques. Code of practice for information security management.</i>
		BS ISO/IEC 20000:2005 <i>Information technology – Service Management</i> particularly the section that outlines the recommended contents for service level agreements (SLAs).
		ISO/IEC TR 18044 <i>Information security incident management.</i>
		ISO/IEC 18019 <i>Software and system engineering. Guidelines for the design and preparation of user documentation for application software</i> ¹⁸⁶ .
		Payment Card Industry Data Security Standard

¹⁸⁶ Although this is a work for technical writers, it was noted that the IT team are correcting work done following an in-house manual that gave incorrect instruction. This had implications on the time taken for the IT Team to correct the database and the time during which the integrity of information on a database was not commensurate with requirements.

Table 54: Recommendations for the housing association target of Project η

	Observation	Recommendation from the information BoK
3	<p>There is already board-level recognition of information systems risk¹⁸⁷. Extend this throughout the association's management and operational staff.</p>	<p>The 'Central Services – Information and Communications Technology' section of the <i>RISK MAP SIGNIFICANT RISKS 141206.xls</i> document, developed and maintained by the association, is the foundation for a focused ICT risk assessment that would feedback to future board-level direction. Base this risk assessment on the information assets and carry the respective requirements for confidentiality, integrity and availability through to the business continuity plans so that the investment in business continuity stays aligned to the return to the business operations.</p> <p>Many projects will share common risks and should feed into a project risk register that carries respective risks up to the Significant Risks List as appropriate.</p>
4	<p>Build on current IT security policies to establish a comprehensive set of policies that apply controls to mitigate risk continuously.</p>	<p>This comprehensive approach to policy making will:</p> <ul style="list-style-type: none"> • Increase efficiency of working practices. (No time lost to incorrect recording or processing information or retrieving information incorrectly exchanged.) • Set out requirements for information systems that treat risks as a matter of course. • Make business continuity an 'organic' component of the organisation's activities rather than an 'add-on'.

¹⁸⁷ The call for the study in project η is evidence for this.

Table 54: Recommendations for the housing association target of Project η

Observation		Recommendation from the information BoK
5	<p>The current duty of care for the information held by the organisation on its customers, and the growing information base with which it will work for vulnerable people should be based around a data sharing protocol. Such a protocol can benefit internal communications – especially between business areas, communications with public sector agencies, and the organisation’s supply chain.</p>	<p>Focus on the information requirements of the data sharing protocol that will set out business-driven requirements for IS/IT out to which the appropriate security controls may be applied.</p>
6	<p>The organisations Human Resources Department should design and effect an information security awareness programme.</p>	<p>This programme may seem to be in parallel with the core business of the housing association. However information security management is effected by day-to-day operations and these are guided by policies/lessons learnt which are used to improve policies within the context of risk to the organisation.</p>
8	<p>There are firm foundations that can be built on. These were manifest in work including:</p> <ul style="list-style-type: none">• Various methods of asset registration including the minimum period for the retention of financial documents, and the hardware asset register.• A significant risks map.	<p>Continue with this good practice.</p>

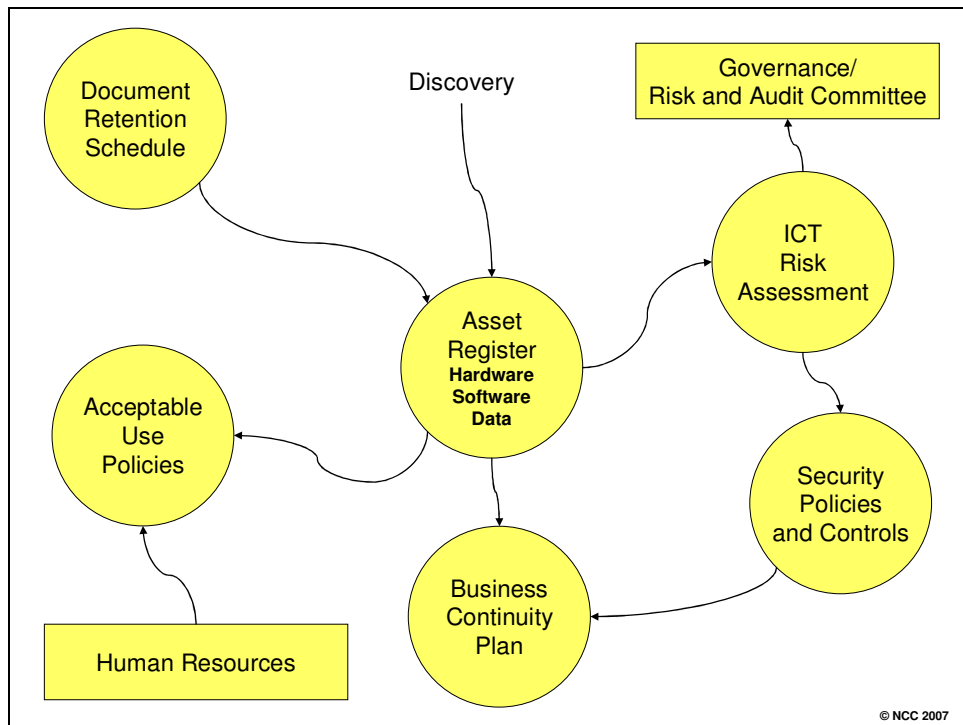


Figure 40: Core information assurance strategy for the housing association

5.7.1.1 Asset management

Information is an asset of the organisation (Stewart, 1997) and must be treated to the same scrutiny as physical assets that may be more easily measured in financial terms. The housing association should bridge the gap between its Document Retention Schedule and its Business Continuity Plans by addressing the risks to discrete and aggregated information assets. This will support the realisation of business continuity which is currently aimed at bringing information technology back on-line. It should be extended to the appropriate availability of information assets. Section 7.0 of the association’s Asset Management Strategy should make explicit reference to the security requirements of the housing association for its information assets. This includes the classification and control of information. The association should consider rankings of the value of assets to assist with decisions for investment in security controls (commodity items such as PCs should be regarded separately from the information stored on them).

The association needed to add a system of security classification to the Document Retention Schedule to connect each document explicitly to the rules for handling and sharing. The comprehensiveness of this schedule is a foundation to an information security programme. This is good for the main documents but will not cover ‘helpful’ uncontrolled spreadsheets that may have been created by knowledgeable users. It also needs to cover software in use and the development tools. Assets should also be assigned owners. (See Figure 40.)

5.7.1.2 Defining information security policies to treat risk

Information security policies will need to be championed on a daily basis. They will form part of the system requirements for current and new systems. The recommended format¹⁸⁸ for the elements of a central policies document is shown in Table 55.

Table 55: Recommended contents of an information security policy		
	Policy section	Description of the section
1	Purpose	Why does the association need the respective policy and what is the risk of not having it?
2	Scope	What does the policy apply to, and what – if anything – is excluded?
3	What the policy is	A clear, pithy, and imperative description of what must be done.
4	How it's monitored	Follow the Deming quality cycle of plan-do-check-act (Deming, 1950). How is the implementation and the effectiveness of the policy checked (monitored)?
5	What happens if the policy is breached	No assumption should be made of 100% compliance so what is done if the policy is not followed? What is the corrective action or sanctions against those who have not complied?
6	What to do to enforce the policy?	Technology, awareness, or a mix of both

Stakeholder reviews were recommended to identify known and currently unknown risks (Alexander, 2007 and Carr, Konda, et al., 2003). These should be held for legacy and new information systems (reviewing them for compliance to the housing association's information security policies), service level agreements (for example with the IT support company and the disaster recovery facilities provider for assurance of the suppliers' commitment to security¹⁸⁹).

A review of the current, documented network security policy document noted ambiguities or areas of opportunity to remove redundant paragraphs and tighten up the presentation to increase confidence of readers and make room for new policies (which are inevitable with the changing landscape of threats and technology). For example, clause 2.3 referred to 'line

¹⁸⁸ Based on the Policies Project at the SANS (SysAdmin, Audit, Network, Security) Institute (www.sans.org)

¹⁸⁹ It was recommended that where possible and available, governance may be easier by selecting organisations with certification to BS ISO/IEC 27001:2005 BS 7799-2:2005. A register is maintained on-line at <http://www.iso27001certificates.com/>

manager' authorisation whereas clause 7.1 referred to 'Senior Manager' and at least part of the association uses the term Supervisor for the reporting hierarchy. The document did not cover: environmental and physical security, risk treatment for mobile workers, or taking a proactive approach to building security into the acquisition and development process for information systems.

5.7.1.3 Organisation of information security

Appropriate agreements with third parties should be established (for example with the software house providing the housing management system) to assure the information security controls they apply¹⁹⁰. This is important given the apparently open, remote access they need to supply support services (ref. an association document: Service Level Agreement December 2006[1].doc). The security obligations (such as specifications and testing) with website developers and package developers supplying the housing association need to be defined. Because the housing association will require the use of niche packages that may not meet acceptable security standards, penetration testing should identify what amendments may be reasonably requested from suppliers or developed as 'wrappers' by the housing association's IT team. These wrappers will themselves need testing for vulnerabilities.

5.7.1.4 Independent review of information security

There were several overlapping internal audit initiatives which would benefit from coordination, including a business continuity audit, ongoing internal audits, the governance components of an external audit (much of which can be applied by attention to information security), the security element of the IT Strategy Review, and initial discussions about implementing the BS ISO/IEC 27001:2005 BS 7799-2:2005 standard. Audit coordination should be risk-based to make use of limited, independent audit resources. Recent audits have included scrutiny of IT which did not receive attention under the regular audit programme. Penetration testing had been carried out two years before these investigations. However, the de facto standard for an organisation of the housing association's size and information profile is for penetration test to be carried out annually. This should be comprehensive enough to cover current policies but there may be areas that can be tested quickly and effectively in-house. For example, it was *assumed* that the association's thin client terminals are not configured for use with USB memory sticks but this potential source of malicious software infection and data loss had not been checked.

¹⁹⁰ This is compliant with Ashby's requisite variety (Ashby, 1957). Management of risk is distributed to suppliers rather than the central recipient of the suppliers' services being expected to manage risks whose channel into the organisation is through each supplier. Standards – such as BS ISO/IEC 27001:2005 BS 7799-2:2005 provide not only a risk management lexicon between stakeholders but also a medium for addressing commonly acceptable levels of risk (Wood and Dresner, 2007).

A third-party provider of disaster recovery facilities had tested the business continuity and disaster recovery plan but not all problems warrant the expense of calling on the provider or are suitable for the provider to evaluate in terms of the impact of the risks faced. For example, what happens when key staff are unavailable or an unplanned power cut tests the uninterruptible power supply (UPS) units? The association must schedule its own sequence of tests.

5.7.1.5 Human resources security

There was a good attitude to starter/leaver induction and exit interviews respectively. However little was done in between, so ICT management process needs to be enhanced to include changing authorisation privileges when staff move within the association. This may become more critical as the amount of sensitive information increases (for example, information about vulnerable individuals through liaison with the local authority).

Several agencies were being retained for the provision of temporary staff and the responsibility for selection is transferred to them. Requirements for agency staff such as security screening and briefing by the providing agency should be clearly specified in the mutual agreements. The housing association should make their confidentiality requirements explicit, with appropriate confidentiality/non-disclosure agreements carried through from the housing association to the agencies and the temporary staff (who also need a security component to their induction).

General awareness of security responsibilities – not currently part of the starter programme – should extend beyond the induction of permanent and temporary staff to refresher sessions for those who have been with the association for some time. It was suggested that staff who had been in post for more than three years would not have benefited from the improved security awareness included in the induction for new staff.

Technical staff should have the necessary training to be aware of the security nuances of the technologies with which they are working. As noted, although there was an intention to move from bespoke, in-house development, to buying proprietary systems, support and tailoring of these systems can introduce vulnerabilities.

Staff who have responsibility for adding information to housing association databases should have their understanding of their tasks verified by an internal qualification or mentoring. This will reduce the risk of incorrect information on databases and the need (as experienced) for the IT team (as has happened) to make corrections directly to the database. This suggests that a tiered privilege access model for end-users may be appropriate so that supervisors can make corrections rather than the IT team being responsible for such corrections.

The association's policy which sets out the uses of its information system facilities which are deemed acceptable covered Internet and e-mail well but did not extend to other potential applications of housing association resources (such as printers and copiers) and should be updated to do so.

5.7.1.6 Physical and environmental security

The organisation's headquarters had a straight forward approach to physical security based on a reception desk challenging visitors. Standard common-sense security measures such as locking windows and a clear desk policy for sensitive documents should be encouraged through a security awareness programme. In contrast, it was noted that it may be possible to access and move around the housing association's building services premises unchallenged through external doors left open or through reception when unstaffed. Plans for a proposed new building should include design based on risk assessment of the areas where sensitive information is handled and application of the respective risk treatments from NISCC, 2005 on physical security.

It was noted that the provision of on-site disaster recovery facilities relied on the availability of a suitable power supply but the current site has no contingency for a loss of power other than a 15-minute UPS for a fail-safe shut down (which has been tested during power cuts). If this risk is acceptable it should be stated explicitly in the significant risks log rather than implied. Desktop computers were allowed to be left on standby and in one office a mobile phone charger was plugged in but unconnected. The latter was a fire risk but both add unnecessary cost through the electricity wastage which did not fit the housing association's ethos.

Printer output was not always collected which may expose sensitive information to those authorised to be in the offices, but not authorised know about the exposed subject matter. The ease of printing led to confidential documents being left uncollected from printers (which also has environmental considerations). A secure printing facility was available and should be rolled out to staff handling confidential information. This was an opportunity to reduce waste and improve security simultaneously. Sensitivity to environmental issues may be the driver for this risk treatment over the security implications and is an example of harnessing risk attitude to treat more than one risk (See Chapter 4).

5.7.1.7 Communications and Operations Management

There was a variety of specialist software in use but no central repository for taking care of the installation discs so that their whereabouts were subject to individual awareness such as a reliance on knowing what had been moved during tidying or office reorganisation. Although server data is backed up and an iteration kept off-site, a problem could be the lack of access to the original machine and the discs to reinstall the application software to access it. The security of back-up tapes was scheduled for improvement with the purchase of a fireproof safe.

Asset management (see above) would be improved with a central, safe repository of master discs.

Amongst the documents reviewed during the research were two versions of the Terms and Conditions for Employment (without an indication of whether they were special to certain

staff) and the agreement with the third party retained for disaster recovery services. This latter document was mainly dated 2002 (with some parts marked earlier) and so lacked records of the up-to-date technology configurations to be recovered in an emergency and the association's and the provider's points of contacts. This was an opportunity to combine good practice of current documentation being available, obsolete, and obsolescent information being withdrawn or marked accordingly to avoid misuse, and documents to carry a security classification according to a preset policy.

There were no controls to protect information that is kept on portable storage devices which tend to proliferate and are easily lost. A policy for authorised use – supported by technical implementation – was needed.

The contemporary responsibilities of the association for handling sensitive personal information and the increase of the exchange of this type of information with the inclusion of delegated responsibilities from its local authority and interaction with other agencies show the need for a tiered, data-sharing protocol. This would allow two-way sharing of information appropriately within parts of the housing association and between the housing association and the authorities. These arrangements would set out the policy requirements of confidentiality and data management for ICT to implement and enforce through technical risk treatments. Some guidance was provided by the Department for Constitutional Affairs (which became the Department of Justice) although it is often advisable to adopt the controls model that other local authorities are already using with similar associations (standards for which are governed by the e-Standards Body – see Project ζ). This would support the association's objective (as set out in its Corporate Strategy 2005 – 2010) to 'facilitate the greater supply of housing by working in partnership with the private and public sectors'.

Risk management for consideration to permit information sharing also included the association's contractors' programme: what is the level of acceptable risk related to amount of IS/IT access and what is the level of detail to be specified for the induction of staff and contractors (which may be outsourced to the contracting company)? Risk treatment may include a range of measures from the level of training/induction sessions to working terms of conditions (including non-disclosure/confidentiality agreements).

5.7.1.8 Access control

Processes for granting authorised access seemed to be well covered for full/part-time starters and leavers – the latter improving with the human resources department, the line managers, and the IT department working on the notification process. The process when staff change roles needs to be made explicit to ensure the appropriate removal of old privileges as well as the granting of the new access requirements.

The policy for wireless access to computer networks was defined as 128 bit WEP for wireless security. The association should consider WPA or WPA2 which closes weaknesses in the WEP standard that could allow unauthorised access.

5.7.1.9 Information systems acquisition, development, and maintenance

Although focusing on acquisition and embedding packaged software, there is a risk in tailoring (see below). Focus should be on developing well-specified and tested end-user routines that do not rely on the IT Team to regularly set up and manipulate. One example where development policy needs to be driven through, is a suggestion that an arrears report is extracted from one database into another before producing letters. This would require another technology to maintain and secure. This is also an example of where IT is expected to deliver a process that it does not own and therefore struggles to control with confidence.

Although comprehensive in-house development is being phased out, there are still vulnerabilities that can be created during the tailoring and adapting of packaged software that will continue to be done by the association's in-house IT team (for example, the threat of SQL injection that can expose confidential information in a database which was highlighted during penetration testing). Developers should embed specific security tests in their test plans to the standard set out in tests for different technologies at www.sans.org/score (Security Consensus Operational Readiness Evaluation).

The IT team showed good awareness of the Payment Card Industry Data Security Standard and explained the decision to outsource on-line payments. As a matter of due diligence, a statement of compliance to the PCI DSS should be obtained from the third party providing on-line credit card payment facilities. The current website developers were keen to provide an e-commerce option but this was turned down. The policy should be clearly documented to ensure that this policy to outsource credit card handling remains a strategic way forward.

Support for incident and events relied on the goodwill of staff to work extended hours or out-of-hours. A formal out-of-hours or leave-in-lieu policy should formalise this. The IT team has shared core skills that are likely to be sufficient to support the basic technologies in use. Incidents involving the need for their specialist skills seem to wait for their availability without a serious loss of service. This reliance on individuals should be a documented policy – supported by a risk assessment that shows the decisions regarding the availability of skills in relation to the reliability and business criticality of the respective service (a business impact analysis).

5.7.1.10 Information security incident management

Information incident management records noted a good account of the reaction to a major outbreak of 'spyware' and the subsequent decision to move from McAfee antivirus to Kaspersky Labs. The original source of the infection was not determined. A forensics policy may have helped. The association should adopt the practice of costing the incident with the goal of ensuring cost-effective responses to security incidents.

5.7.1.11 Business Continuity

A 'business critical' IT problem can be flagged for resolution within a day but if staff are mobile and are only on site for a short time, this may well be too long (and could have to conceivably wait a week until back on site) losing the opportunity for preventing the occurrence of the same incident with other users or the efficiency of the staff who are working away from the association's premises. The association should adopt a risk-based formula to align the IT response time to the business continuity plan (allowing a higher priority than 1 day). Reliance on a single telephone line needs to be kept under scrutiny.

There was no 'standard' build for PCs because of the diversity of specialist applications required. This strengthens the need for centrally held records of the configurations. Even a simple record of (say) the latest, patched version of the operating system and application X, Y, Z is desirable so that in the event of a crisis, recovery of the facilities needed is not down to personal experience/memory. This also supports any contract staff whose specialist skills may be needed in an emergency.

The business continuity plan had yet to react to the pandemic response planning which had had its profile raised by new strains of the influenza virus. The association was directed to consider the advice available from public sector websites. Although there is a limit as to what could be done in the event of a pandemic, ICT support is likely to be a key issue (with problems connected with regular tasks such as the back up routines). ICT may be needed to allow more home-working as schools will almost certainly close, with implications on the childcare arrangements for some staff. Enough remote working connections should be available in advance. The association should carry out an audit to see if staff who may be required to work from home will have the equipment and suitable connection to do so. Staff working in these conditions will need to be being more aware of teleworking risks (which comprise issues equally relevant at home as in the office)¹⁹¹.

Table 56 summarises the results and interpretation of Project η (the housing association).

¹⁹¹ for example: the Health and Safety at Work Act (1974), screen (VDU) regulations, room temperature and ventilation, applying the Working Time Directive or screen breaks, having an adequate supply of two-factor authentication devices, the use of unsafe equipment, having available sockets and power supply which are adequate for the IT installed, trailing cables that might constitute a danger, and how to deal with a security breach away from the association's premises.

Table 56: Results and interpretation of Project η (Housing association)

Results	Lessons learnt	Evidence and organisational idiosyncrasies observed
The project used the ISO/IEC 27001 standard to benchmark the current activity of the housing association to secure its information systems and then recommended an information security strategy to be implemented as part of an information technology strategy.	How a standard for information security can be embedded into an IT strategy to assure board-level attention to information risk mitigation.	Exposure of employees to sensitive information about people's housing circumstances was available to, but on the whole not of concern to, the call centre or maintenance staff who had access to it.

5.7.2 Project θ: Fieldwork in construction – risk to treatment analysis

This project differed significantly from the two other case studies discussed in this chapter. In the work with the housing association described above (Project η) a detailed report was created to show where the implementation of information security management standards was advisable as part of their information systems risk strategy. The client wanted detailed instructions of the improvements needed for information assurance. The research phase led to intervening advice about how to create an environment where risk is mitigated. In the intervention with the firm offering pensions and actuarial services (Project ι) that follows below, a set of risk management (security) policies were developed following on from the research (see Table 59). The client received elements of their risk mitigating standards as a result of the research. By contrast, this fieldwork in with a construction firm (Project θ) delivered neither specific standards and policy, nor advice on what was needed, but rather facilitated a programme of knowledge transfer for the company to effect its own standards adoption, policy setting, and risk mitigation.

Table 57 summarises the results and interpretation of Project θ (the construction sector company).

Table 57: Results and interpretation of Project 0 (Construction)

Results	Lessons learnt	Evidence and organisational idiosyncrasies observed
<p>The organisation became involved by a series of interviews that informed the research of the state of information security across its business functions. This became the starting point for a knowledge transfer activity because the discussion during these interviews informed the interviewees on pertinent risks to their business information that they were often failing to manage. As a result, the knowledge transfer process was completed with a series of workshops that made the IT management team able to assess and mitigate risk.</p>	<p>How a standard for information security can be embedded into the management system of an organisation to protect a business from risks to its corporate and customer information and the losses that would ensue in the event of an incident. Embedding the expectations of the information security management system standard into the business management system of the organisation made it accessible by default.</p>	<p>The organisation comprised polarised attitudes to information security varying from tight policies displayed by architects and surveyors to a lack of awareness of the sensitivity of customer information by staff charged with reviewing the architects' work for compliance with health and safety regulations. The implementation of information security policies by the supplier to protect customer information could exceed the protection allotted to that information by the customer.</p>

5.7.3 Project 1: Pensions and actuarial services – risk management (security) policies

My initial expectations that the detailed stakeholder interviews would guide an adjustment or focusing of the policy documentation imposed by the parent company did not manifest. Rather than suggest specific policy recommendations, the interviews showed a low level of process maturity (Crosby, 1979) with respect to information security management. Apart from some core, good practices from the IT department and the estates management representative – both in regards to access control but, contrastingly, logical and physical respectively – information security risks were endemic and security measures viewed as an inhibitor to work (for example being allowed to download and work on confidential company documentation on a home computer that is not subject to the rigorous scrutiny in terms of malicious software detection or intrusion detection and prevention). The interviews became an opportunity to increase awareness of risk and explain the reasoning for the access

controls already in place. For example, a solicitor agreed to reconsider working on company documents using a computer used for filesharing by other members of her family when learning of an instance where such behaviour had led to the extraction of confidential files not intended for access by the file-sharing software. The documents in the example were published on a hackers' website¹⁹².

The considered response to this was to write a set of instructional information security policies based around generic good practice (guided by the BS ISO/IEC 27001:2005 BS 7799-2:2005 standard). The policy documentation was written to show an understanding of the repeated concern that introducing a layer of security would be an inhibitor to getting work done. I stressed that security was not a separate layer but rather the enabling mechanism for assuring confidentiality, integrity, and availability for work to be done at home or outside the office without having the variety of locations compromising the controls of a working environment with a definable perimeter. Essentially, policies were being established to allow high-risk data processing such as remote and mobile working as long as the risks are managed. This is a regulatory approach to risk management beholden to financial sector business in particular (See Figure 12).

Some directional advice was also given with a suggestion to review the company's segregation of responsibilities in the business processes and how the IT may support that with sign-on sequences and forensic records of non-repudiation. This may have avoided the client's previous exposure to fraud. To enable this, the client would need to define the boundaries of its information assets and assign ownership. This would require, in the first instance, creating an information asset register that records the retention and degree of confidentiality of information assets such as medical records, policy documents, actuarial forecasts and so on.

Table 58 summarises the results and interpretation of Project 1 (the finance sector company).

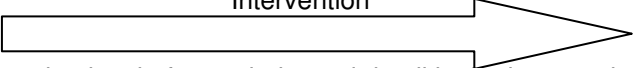
¹⁹² Examples that made the business team aware of opportunities for improved compliance included this external example of an Equifax credit report being stolen over the Internet (where it was published for mischief) from the 'private' part of a PC because the wife of the reportee used peer-to-peer software on her 'private' part of the same PC. Also a local example from the client's firm where a member of staff received a document by e-mail, edited it, saved the changes and e-mailed (apparently) the changed document to find that the changes had been 'lost'. The implications were two-fold. Firstly the confidential document was left in a temporary folder of an insecure PC, and secondly the user was left fretting and did not call the help desk who would no doubt have been able to talk the user through the problem, possibly retrieving the changed version and cleaning the cached copy which was leading to a loss of efficiency.

Table 58: Results and interpretation of Project ι (Finance)

Results	Lessons learnt	Evidence and organisational idiosyncrasies observed
<p>Policies from the parent company could be localised for the subsidiary and remain true to the original standard from which needed to comply with. However, the local implementation suggested an unfounded expectation that the subsidiary would be complying with something other than the view of the parent.</p>	<p>How a set of standards can be adapted locally without losing their identity and still retain compliance with the parent company standards and an international standard for information security in order to de-risk information systems. This is a case study where the localisation of standards creates their accessibility.</p>	<p>It was whilst working with this company that the need for localised interpretation became evident. Not only is there often a reluctance to espouse standards (as discussed in Chapter 2) when there is a lack of external influence demanding some level of compliance, even the pressure of taking edicts from a company's owners still leads to compliance with the imposed standards through the local lens of what the individuals there agreed were the risks that needed mitigating.</p>

5.8 Conclusion

This chapter has looked at the practical implementation of the standards life cycle in the identification of the need for standards, the creation of – or adoption of existing – standards, and then (Table 59) how standards are implemented in different ways in different organisations. I have considered these complementary projects where standards have been applied either as frameworks for developing the organisations' own risk-mitigating practices (Project θ: construction), direction about the risks that need to be mitigated, and the standards that have been designed to do so (Project η: housing association), or the local implementation of a centrally-issued standard that provided a tailored policy set to match the culture of the organisation facing the risks (Project ι: pensions and actuarial services).

Table 59: Contrasting three types of action research		
Project θ: construction	Project η: housing association	Project ι: pensions and actuarial services
Knowledge transfer. Arm's length advice and training about how to determine the information security policies needed.	Instructional report setting out the structure, content and management process of running an information security management system,	Detailed, direct intervention of writing security policies that set out technical controls and behavioural improvements.
<p style="text-align: center;"> Less Intervention More  Increasing level of granularity and detail in the intervention </p>		

Chapter 6 analyses the results of this action research and the implications of the projects for the research questions set out in Chapter 1.

CHAPTER 6. ANALYSIS, CONCLUSIONS, AND FUTURE WORK

6.1 About this chapter...

This concluding chapter of the thesis revisits my research questions and analyses the results of the research projects in their context. From the questions and projects' results, I consider the conclusions that may be drawn from the research, the questions still unanswered, and look to the future both in terms of work to understand the 'unknowns' and how the components of the research that have shown positive outcomes can be extended and exploited for the effective use of information systems – the mission of my main sponsor, The National Computing Centre.

Because the research was realised by a *programme* of projects, I have tabulated the connections of the research questions to the results (Table 60 to Table 62 inclusive).

6.2 Revisiting the aims and objectives of the research

The underlying hypothesis of value in the research described in this thesis is that *risks may be managed by the implementation of standards to avoid undesirable outcomes*. Lessons from good practice in information systems development and operations – specifications of tools and techniques – can be encapsulated in standards to mitigate at least the known risks. In summary: *standards mitigate risk*.

My original plan was to test the hypothesis by way of a developmental research project in which I would create a framework 'standard of standards' as an accessible, scalable route map through standards to be usefully applied to information systems to assist organisations avoid undesirable outcomes. The motivation for the research was to encourage a beneficial environment for innovation, and a stable, sustainable business 'ecosystem' for existing business practices encouraging trust and security. Reflecting on the core hypothesis – particularly in the light of the literature review (Chapter 2) – I began to understand that there were methodological considerations behind the hypothesis as I synthesised three research questions to investigate it (Table 60). This became an early lesson in learning how to learn: formulating the research in a way that it leads to telling investigations. The epistemology developed in four ways: the objectives to find and deliver interesting research, the interest in risk, the end effect of applying standards to mitigate risk, and the very personal objective of learning. This personal objective was given momentum by attention to frameworks (discussed in more detail below around Figure 48) as I applied a framework of projects to learn about the potential of a framework of standards to mitigate risk. This strongly supports my research methodology from the perspective of cybernetics because frameworks and the many combinations that their contents can be applied in result in the amplification of variety and protect the research from the attenuation of translating real-world situations into static models (Beer, 1993).

Table 60: Research questions	
Research question	Methodological extension
1 Do implemented 'Standards' mitigate risk?	Can 'Standards' be implemented to mitigate risk?
	How can risk reduction techniques be linked to the reduction in risk with surety?
2 Can 'Standards' be made more accessible?	How can 'Standards' be made more accessible by relating them to risk and the causes of risk?
	What are the barriers? Why don't people access standards?
3 How do you link risks to the 'Standards' that may mitigate them?	Do the selected standards affect the outcomes of the mitigating action?
	Does the difference in outcomes that results from different analysis methods become a threat/risk?

6.3 A personal epistemology

This seven-year journey has been an exercise in risk management. I set out with three research questions, but the methodological approach to answering them became a hostage to fortune of the case studies available to investigate - would a variety of projects provide the depth of knowledge, or should profundity be risked in a single, 'soup to nuts' undertaking? Over time, this apparent weakness became a significant strength. The uncertainty of applying all the research method to one project was dependent on the cooperation of the stakeholders in the scrutinised work (see also 6.7.4). So, rather than hedge all on sufficient detail being found in a single case study, I looked for significance across the life cycle of standards. A mixed method developed comprising action research informed by desk research and surveys in an interpretive approach to learning.

Re-evaluating my original proposal – the formulation and search for proof of an hypothesis that *standards mitigate risk* – I had intended or expected a positivist study of the cause and effect of standards on risk, describing measurable properties independent of the researcher (Orlikowski and Baroudi 1991). If I regarded risk as 'loss' then I could define that loss in terms of objective, measurable properties of an information system such as cost, efficiency,

quality, and content (Figure 9¹⁹³) and test the implementation of standards to reduce (at least) the loss. However, even the desk research of projects α , β , and γ (see *Appendix B*) were subject to interpretation through the lens of my experience at The National Computing Centre and rest on the assumption of value in empirical experience over clinically validated wisdom (Schein, 1976). As soon as the action researcher enters the frame – as I did so significantly steering the stakeholders in each case study project (Chapter 5) with a proposal of how each project should be shaped and managed – the researcher becomes attached to, and so part of, the organisation. Hence the organisation is changed by the observer, of Heisenberg's Uncertainty Principle, (Heisenberg, 1927). The result – in terms of classification and labelling – is that action research cannot remain in the positivist camp and must be fleet of foot to make an honest accounting for what the organisation (without the researcher) will have to do to sustain the intervention in his or her absence. The expected clinical testing of the hypothesis that 'standards mitigate risk' became a fuller study of how standards coalesce with the expectation that they will treat risk, and how attitudes – strong regulators in the arena of research – to risk and standards affect risk management. I had lost the positivist grounding in the emergent project opportunities, and found an interpretive approach to access reality (Humphrey and Scapens, 1996) through consideration of the language of standards, focusing on the full complexity of human sense making (of risk attitude and the readiness to espouse the knowledge of mitigation and implement it) as the situation emerges (Myers, 1997). This was built into the core project – the research and development of a tool to detect where there are risks as a result of human vulnerabilities in information systems (δ). The consciousness of the subjects (Kaplan and Maxwell, 1994) was modelled by investigating and analysing their attitudes to risk and using the shared meanings of standards as risk treatments (followed though in the analysis of the case study projects η , θ , and ι). But I still question the dependent and independent variables of risks and mitigating standards (Myers, 1997). Does a standard-risk treatment pair represent dependency? This uncertainty generates the impetus for future research (6.8) into the cause and effect of standards and the amelioration of risk. This standard-risk treatment model is complex (Chapter 3, project γ). The project (γ) showed the 1:1, 1:M, and M:1 relationships between risk and standards whilst project δ brought out the complexity in relating attitudes to risk and attitudes to standards.

I have finished with a critical element to my thinking because standards record knowledge and are dependent on an historical epistemology and an historical constitution. The evidence for their efficacy is lacking; the effects of their implementation may be initially predictive until proven...or not disproved (Popper, 1963) and yet organisations still fail when following standards (Seddon, 1998 and Thomas, 1997). Standards are produced, reproduced and interpreted (Figure 43) by people who may not openly or even covertly

¹⁹³ The area within the cloud outline within which the project resources and attributes should be contained to achieve the desirable outcomes, that is, where risk is managed.

embrace their advice; elsewhere the standards are the ways of working (as noted by the experiences from The National Computing Centre's help desk in Chapter 1). These oppositions and contradictions remain. The future work brings the research full circle to the positivist camp and my original proposal.

6.4 Answering the research questions

Figure 41 is repeated from the introduction (Chapter 1) to show the connection between the research questions (labelled 1, 2, and 3) and the respective research projects. Table 61 then goes on to compare the research questions with what has been learnt from the research so that one column shows the research questions – and their related methodological questions (from Table 12) and matches them with the answers that emerged from the research.

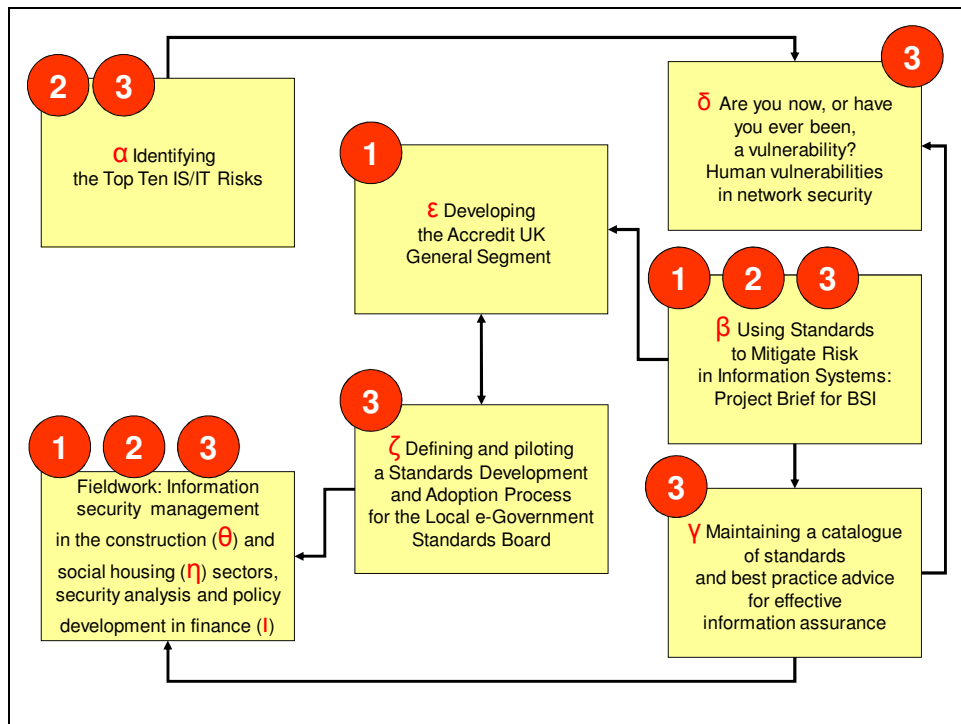


Figure 41: Relevance of the case studies to the three research questions

Table 61: Research questions answered

Research question	Learnt from the research
<p>1 Do implemented 'Standards' mitigate risk?</p> <ul style="list-style-type: none"> • Can 'Standards' be implemented to mitigate risk? • How can risk reduction techniques be linked to the reduction in risk with surety? 	<p>The literature review (Chapter 2) and continuing involvement in projects to mitigate risk in information systems¹⁹⁴ suggest – but in no way prove – that standards mitigate risk. This conclusion is based on the consistent opinions expressed in the literature that information security and assurance come from the implementation of standards. These standards continue to be defined and refined on the basis that the advice therein is effective.</p>
<p>2 Can 'Standards' be made more accessible?</p> <ul style="list-style-type: none"> • How can 'Standards' be made more accessible by relating them to risk and the causes of risk? • What are the barriers? Why don't people access standards? 	<p>Cataloguing work (Chapter 3), work to measure risk (Chapter 4), and field work (Chapter 5) show that the many standards become more attractive to stakeholders when they are related to risks – a direct benefit of following the advice in a standard can be shown to the actors in the information system. The linkage of standards to risk becomes the method of selection that helps to break down real and implied barriers to the accessibility of standards.</p>
<p>3 How do you link risks to the 'Standards' that may mitigate them?</p> <ul style="list-style-type: none"> • Do the selected standards affect the outcomes of the mitigating action? • Does the difference in outcomes that results from different analysis methods become a threat/risk? 	<p>Recognition of the risks, the degree to which the knowledge is encapsulated in a standard, and the expertise required from people to convert that knowledge from explicit to tacit allows a cataloguer to place standards against a taxonomy of risk with some confidence of their likely efficacy.</p>

Throughout the five-year programme of research projects, I found it challenging to steer the interesting research opportunities away from the single goal of each body commissioning a

¹⁹⁴ Including a workshop at the Cabinet Office to review the National Information Assurance Strategy, 6 July 2010.

project, to retain the wider view of the research questions and add value to research for the sponsor. In the following subsection, I have again used a table to show the connection between a research question, the project applied to find an answer to the respective question, and what the results of the related projects show.

6.5 How do the outcomes of the projects explain the answers to the research questions?

Working for a professional body provided a rich catalogue of opportunities to formulate, adapt, or adopt projects which would inform or help to answer the research questions. These are described in detail in Chapters 3 to 5 (inclusive). Table 62 shows how the framework of projects enlightened the answers to the research questions about a framework of ideas (Checkland and Holwell, 1998).

Table 62: Research questions: what can we learn from the research projects?

Research question	Project	Shows
<p>1 Do implemented 'Standards' mitigate risk?</p>	Accredit UK (ε)	The interaction of stakeholders in the determining of what needs to be captured in a standard to mitigate risk in the procurement of ICT from small to medium-sized enterprises.
	BSI Project Brief (β)	The peer review of the concept and utility of organising standards into a framework of good proactive instructions about how to mitigate risk.
	Fieldwork: housing association (η)	How a standard for information security can be embedded into an IT strategy to assure board-level attention to information risk mitigation.
	Fieldwork: construction (θ)	How a standard for information security can be embedded into the management system of an organisation to protect a business from risks to its corporate and customer information and the losses that would ensue in the event of an incident. Embedding the expectations of the information security management system standard into the business management system of the organisation made it accessible by default.
	Fieldwork: finance (ι)	How a set of standards can be adapted locally without losing their identity and still retain compliance with the parent company standards and an international standard for information security in order to de-risk information systems. This is a case study where the localisation of standards creates their accessibility.

Table 62: Research questions: what can we learn from the research projects?

Research question	Project	Shows
<p>2 Can 'Standards' be made more accessible?</p>	<p>Top 10 IS/IT Risks (α)</p>	<p>That there is a common perception of the most prevalent risks threatening information systems and that perception can be used to steer stakeholders towards standard practice to ameliorate the risks. Familiarity with a risk and a link to its mitigation makes the mitigating action – included in the relevant standards – desirable when explained to a practitioner within the business.</p>
	<p>BSI Project Brief (β)</p>	<p>Peer review of the framework to improve the accessibility of standards as a method of managing risk treatment information.</p>
	<p>Fieldwork: housing association (η)</p>	<p>By identifying risks to its information systems in the context of its business processes and connecting the risk treatments to the use of standards, this project made standards more accessible by putting them into a business context that was familiar with the stakeholders.</p>
	<p>Fieldwork: construction (θ)</p>	<p>How a standard for information security can be embedded into the management system of an organisation to protect a business from risks to its corporate and customer information and the losses that would ensue in the event of an incident.</p>
	<p>Fieldwork: finance (ι)</p>	<p>By identifying risks to its information systems in the context of its business processes and connecting the risk treatments to the use of standards, this project made standards more accessible by putting them into a business context that was familiar with the stakeholders and then translated those standards into a local governance and management framework.</p>

Table 62: Research questions: what can we learn from the research projects?

Research question	Project	Shows
<p>3 How do you link risks to the 'Standards' that may mitigate them?</p>	<p>Top 10 IS/IT Risks (α)</p>	<p>This was an important scoping study which identified a set of risks to focus on during the course of the research.</p>
	<p>BSI Project Brief (β)</p>	<p>The mission of BSI Standards is the promulgation of standards. The project brief specified a programme of work that would show how to promote standards as risk treatments by associating standards with the respective risks that their implementation implies.</p>
	<p>Catalogue of standards and best practice (γ)</p>	<p>This was the fundamental realisation of an answer to the research question showing that a taxonomy of information security risk can be populated with associated standards to treat the risks in that taxonomy. The project delivered a method for populating the catalogue, keeping it up to date and adding value to lists of standards by introducing a classification scheme for the level of treatment a standard provides for a risk and the expertise required of those who implement the advice encapsulated in the standard.</p>
	<p>LeGSB (ζ)</p>	<p>LeGSB required a process to select standards to address areas of risk and it was through this process that they would engender a consensus view of acceptable standards.</p>

Table 62: Research questions: what can we learn from the research projects?

Research question	Project	Shows
	Finding human vulnerabilities in information systems (δ)	On the understanding that human vulnerabilities are a prevalent risk in information systems, this project set out to find a way to identify them (which it did). Applying the premise that standards – as the definition of <i>controls</i> or <i>regulators</i> (Ashby, 1957; Beer, 1993) for risk – can be introduced to counter weaknesses from human vulnerabilities in information systems. By seeing the level of risk an organisation faces with respect to those human vulnerabilities in its information systems, a connection is made to the risk-controlling (regulating) standards which have the potential to make the organisation more or less reliant on the risk attitude of the people working for it.
	Fieldwork: housing association (η), construction (θ), and finance (ι)	Each of these three organisations should confer an understanding of the value of information to their stakeholders. This includes, respectively, examples such as information on vulnerable people who were eligible for social housing, having access to blueprints for banks, or detailed information on people’s pensions. A loss of confidentiality would result in at least reputational damage and in some cases prosecution. The organisations found that standards for information security management set out controls to ameliorate situations that could lead to these risks being realised and so provided case studies of organisations actively linking risks with mitigating standards.

6.6 Reviewing the methodologies

The core methodologies in this research were (one) peer-reviewed desk research which provided a firm foundation to apply and extend that learning in (two) action research. The challenge of the action research – ‘intervening with purpose’ – was that the projects may or may not retain their quality of fit to the research agenda (that is, answering the three research questions) as work progressed with the commissioning bodies. Happily, each has

contributed to the narrative and so they are presented in the thesis in order of learning – helping me to understand the problem better or answer (in part or wholly) some, or all of, one or more research questions.

In considering how the results were found to answer the questions, it is necessary to look at the planned intentions and expectations and compare them with the reality of the selected projects. My original intention was to investigate the research questions respectively by:

- (1) Designing a usable framework from which mitigating standards may be identified from the risks that give rise to their need.
- (2) Creating a methodology to populate this framework.
- (3) The analysis of standards implementation to understand if risk was managed as a result of the application of standards.

I expected the research to be more developmental with the cataloguing of risks and mitigating standards to be the greatest part of the work in terms of time and effort. What actually happened was when the opportunity arose to apply the research methods to the catalogue of publicly available information assurance advice (constructed from a taxonomy of information security risk and published standards – see Chapter 3) the catalogue development became a small subsection of the work to be done to investigate the research questions. It helped significantly in the research to find linkage between risks and standards but was superseded by the more interesting work to investigate how the strength of the mitigating standards may be used to counter human vulnerabilities in information systems (Chapter 4) and the efficacy of standards in fieldwork (Chapter 5). The result is a thesis which presents a developing framework of projects for learning about the application of standards in mitigating risk. It documents a journey from the initial reasoning and motivation in Chapter 1 and literature review of work in this area in Chapter 2¹⁹⁵. Chapter 3 describes how the research framework was steered by the three desk-research projects – the survey of surveys that identified a list of the ‘Top 10’ IS/IT risks (α) and the Project Brief for BSI (β) which both served to refine and define the scope of the research, and the gap analysis and cataloguing for CSIA (γ) which answers the question about linkage but shows that in terms of its actual uptake and implementation the cataloguing work is superficial. The more important need to look at the real-time attitude to risk and implementation of standards is embodied in the selection of the projects in Chapter 4 and 5. This journey through the projects over a five-year period demonstrated the challenge of steering the research to stay focused on the original questions, a challenge of action research struggling to maintain rigour in the heart of changing the relevance of – at least – the participants’ priorities (Baskerville and Wood-Harper 1996).

¹⁹⁵ Chapter 4 also has a significant element of literature review – carried out as part of the investigation into the human vulnerabilities in information systems. Appendix A lists those references used specifically to derive the risk attributes of the subjects under scrutiny.

6.7 Contribution to the body of knowledge

This research has contributed to the body of knowledge in four areas: knowledge management, risk management, measuring security culture or risk attitude, and methodologies for information systems research. More specifically the contributions are methodological as described in Table 63.

Table 63: How the research contributes to the body of knowledge	
Methodological aspect	Contribution
How standards are a channel for knowledge management.	The command and control of organisations may be regulated by applying the practices contained in standards. The knowledge is adapted locally but the standardising theme remains under central ownership of the standards-creating body. This results in an ecosystem that allows requisite variety but feeds back the lessons learnt. The idiosyncrasies of the organisation protect the day to day activity from stagnation.
How risks can be linked to the standards that mitigate them.	Here I have shown how an existing taxonomy of risks can be selected and a validated catalogue of standards which describe the mitigation of those risks can be assembled taking the goodness of fit and expertise required to apply the advice into account.
How the security culture of an organisation can be used as an indicator of which standards are needed for information assurance.	This work has bridged a gap. It matches other work in the field (Coles and Hodgkinson 2008) ¹⁹⁶ which focuses on measurement and then takes this forward with a course of action – through the application of standards – to regulate the resultant measurement within a defined tolerance.
How a body of knowledge ¹⁹⁷ creates a framework for learning about information assurance.	The concept of applying a methodology to learn about a framework of ideas has become an intense part of the methodology itself with the standards forming the framework and providing the instruction on how to apply it.

The discussion below shows the derivation of these contributions from the research.

¹⁹⁶ Also the SeCURE ‘risk culture’ measuring tool from the Centre for the Protection of the National Infrastructure.

¹⁹⁷ For example HMG’s Communications and Electronic Security Group’s (CESG) library of standards, policies and guidance, or BSI catalogue of standards.

6.7.1 Idiosyncrasy as the saviour of standardisation

The projects have provided evidence or the epistemological framework for understanding. Interventions in the action research may not necessarily have helped change – clients have embraced the reports delivered from the research but the work was done in an environment of knowledge transfer enabling their own audit. This has reduced the opportunity to return to answer my first research question, ‘Do implemented standards mitigate risk?’. However, each project has made a contribution to understanding. So I can attest to their usefulness if not to create change in the organisations but at least to create a better understanding of what the organisations should do for improvement on the assumption that the validated advice and experience encapsulated in standards (*Figure 11*) mitigates the predicted risk.

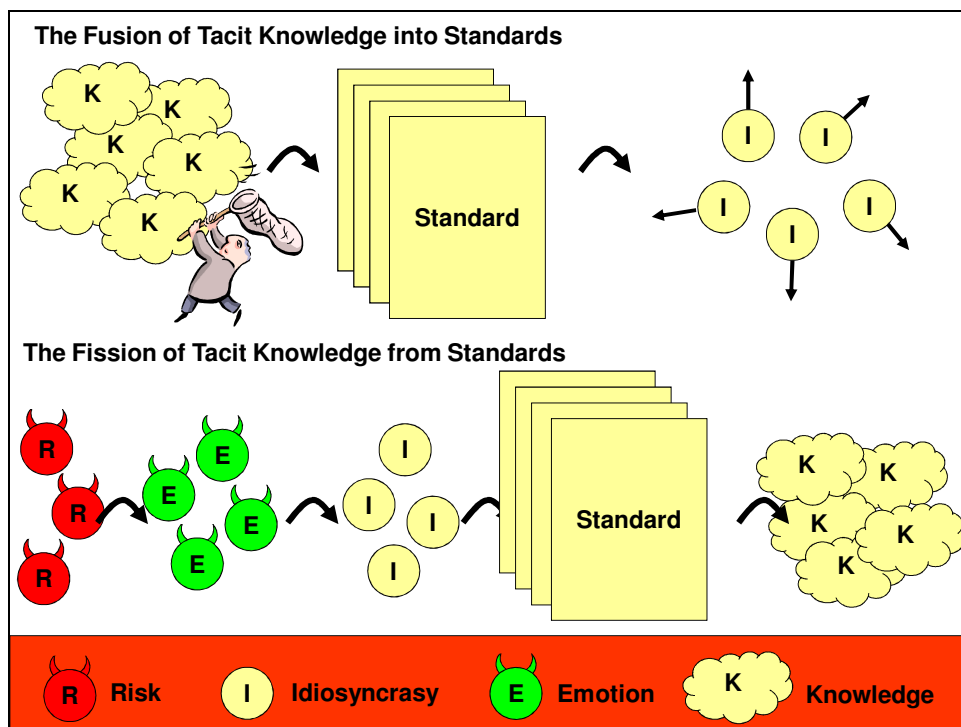


Figure 42: **Risk** stirs **Emotion** which promotes **Idiosyncrasy** that releases the **Knowledge** from standards

If I was to return to the organisations involved in the field work to assess the efficacy of the standards which have been applied, I would be challenged to find the appropriate metrics to measure improvements (or otherwise). This in itself would be a worthy research project because although a measurement methodology for risk treatment has recently been encapsulated in a standard (BS ISO/IEC 27004:2009) that has been through review and validation processes such as those described in my literature review (Chapter 2), the new standard is not strong in defining which measures prove the efficacy of a treatment. For example, an organisation may set a policy of training its staff to reduce the human vulnerabilities in its information systems in accordance with the recommendation of security objective A.8.2.2. Information security awareness, education and training (from BS ISO/IEC

27001:2005 BS 7799-2:2005). However the objective is then measured quantitatively comparing the number of employees who received annual information security awareness training and the number of employees who need to receive annual information security awareness training. Whereas this may be an important measure for planning to ensure that the employees attend the programme, it lacks the qualitative assessment of the employees' attitude to risk that should have been improved as a result of attending. This second, qualitative metric may be measured using the assessment method described in Chapter 4.

Opposition to the usefulness of standards suggested that as the implementation of a standard is characterised by the people, processes, and technology to be found within an organisation, there is no standardisation without uniformity and accusations (Knight, 2005; Schultze and Stabell, 2004) and this leads to constraint and stagnation. I discussed this as the 'Toynbee conflict' in my literature review (Chapter 2). My investigation throughout the literature review pointed to a cycle of standardisation where a degree of localisation was either tolerated, or in the case of management system (process and control) standards encouraged within a framework so that as long as an organisation stayed within the framework (for example of acceptable risk management in BS ISO/IEC 27001:2005 BS 7799-2:2005) the activity of the organisation could be deemed to remain compliant with that standard. And this was witnessed repeatedly in the three fieldwork projects (η , θ , and ι) and their localisation of the good practice and standards that the organisations were embracing to satisfy stakeholders, regulatory requirements, a desire to follow good practice, or all three. Over time, lessons learnt may be collected to normalise the standard with the current, common, good practice and update the documentation for the standard (Figure 43). In this model (sic!) variety is protected by the proliferation of different implementations of the standard – intuitively sounding like an oxymoron and a rallying point for critics of standards. But the good use of standards allows their application within certain tolerances (variety¹⁹⁸ is amplified) whereas in contrast there is bad use of standards where there is no benefit from complying uniformly with every clause (variety is attenuated) and risks cannot be treated because the cybernetic system of managing risk is prevented from healing itself.

The three organisations scrutinised in the fieldwork had a common goal of wanting to achieve a state of information security. Each organisation required benchmarking against recognised good security practice with a view to changing as necessary, in relation to that benchmark. The changes expected would control information handling activities (to use the current terminology of standards rather than the more useful description of 'regulators' – see 2.7 *The Toynbee conflict*). The organisations under scrutiny during the action research had a common goal and a common frame of reference to the body of standards which record the accepted good practice in information security. Hence, that body of knowledge was the equivalent of the model where a framework of ideas is applied to an area of concern – information risk – for learning (Checkland and Holwell, 1998). Here, the organisations have a

¹⁹⁸ (Ashby, 1957; Beer, 1993)

framework of ideas comprising the information security standards which are applied and subsequently used to learn from (through monitoring) to discover whether the adopted framework is effective. This is true to Deming's revised cycle – plan, do, learn (or study), act (Deming, 1986). An information security management system – formally in place with a set of audited policies and procedures or implied by the overlaying, by an observer, of the information security framework promoted by the documented standards – is a protective framework to regulate information security risk. This framework, as applied within the organisation or used as a lens by the observer, is shaped by:

- The operational objectives of the organisation. Why is it there?
- What is the structure of the organisation in terms of its location(s) or premises and the arrangement of its personnel?
- Are they human resources or human vulnerabilities?
- Collective and individual risk attitudes which are unique to each organisation which is shaped by individuals, decisions made, and how it adapts to its environment (Checkland, 1981).

Each organisation draws on their knowledge in standards and implements them according to their own idiosyncrasies, their mode of behaviour or way of thought peculiar to an individual or a distinctive or peculiar feature or characteristic of a place or thing (Oxford English Dictionary 2011, accessed online). It is the same standard deployed in each organisation but to the casual observer, the practice may not seem to be standard at all. With such a dynamic status, there is a need to have some benchmark of whether the organisation is within a tolerable level of risk. This is a contextual judgement that may be supported by the analysis provided by the appetite/attitude measurement described in Chapter 4. This takes into account the sociotechnical spectrum of information security activities to enable the observer to conclude whether the organisation has the regulators in place to be said to be in a state of information assurance. Information governance is needed to alter that state – to improve it or keep it steady in the changing risk landscape. Idiosyncrasies may be the regulators to manage risk. Where they are, encourage them for sustainability; where they are not, the organisation should look to the *standard* practices to inject into its operations and hook them on to the idiosyncrasies until idiosyncrasies and the practice of standards merge.

Awareness of this apparent difference in the implementation of a standard in different organisations should provide the standards makers with the confidence to include the guidance material in standards as a way of educating the implementers of standards as to the 'why' a standard defines a policy so. The classic reductionist stance of the standards makers to focus on the normative clauses which puts the use of standards at risk as implementers reject overall compliance and begin to create their own standards from first principle where they are just learning the lessons that the standards makers have already learnt. Standards makers, standards implementers, and the auditors of compliance would do

better to encourage the energies, expertise and innovation that grows from tacit knowledge and look to see that compliance is within a tolerance which itself is likely to fluctuate. They should ask when is a standard no longer being followed? From this we can learn how to write better standards, use standards, and improve those standards already set.

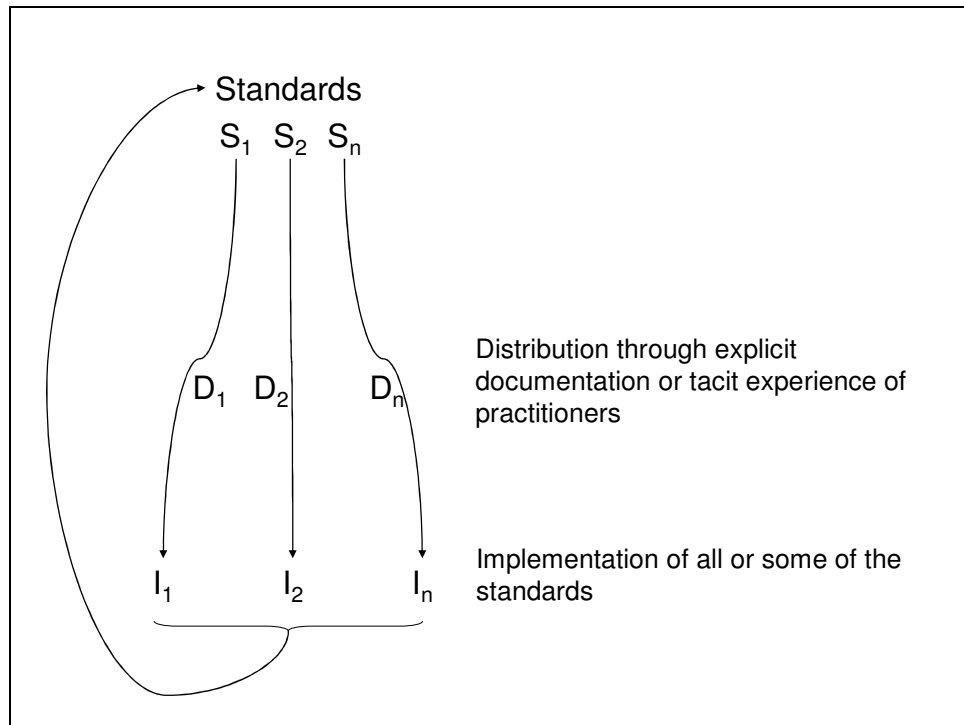


Figure 43: Standards are localised and lessons learnt are centralised

In defining this process, I considered when a standard may diverge from the norm and become unique in its application. Are uniqueness and standardisation mutually exclusive? The state of obsolescence identified during the literature review – where a standard is still in use despite the emergence of others – suggests that whilst standards raise an expectation of majority use, they don't require a democratic majority to remain on the catalogue although spare parts for a product made to an old standard may be difficult to procure. For example, the popular anecdote (Cusumano, Mylonadis and Rosenbloom 1992) of Betamax video which was overtaken by the VHS format, or the audio cassette that has been mostly – at the time of writing – superseded by the Compact Disc. These are standards developed to reduce the risk of recordings being lost, incomplete, or inaccessible. Figure 44 shows where a zone of proliferation – where there are no obvious followers – exists for standards that fail to reach some level of popularity. Standards may emerge out of popularity (which may be the result of successful marketing) taking the 'experimental route' or through development and consensus such as a common gauge for rail travel.

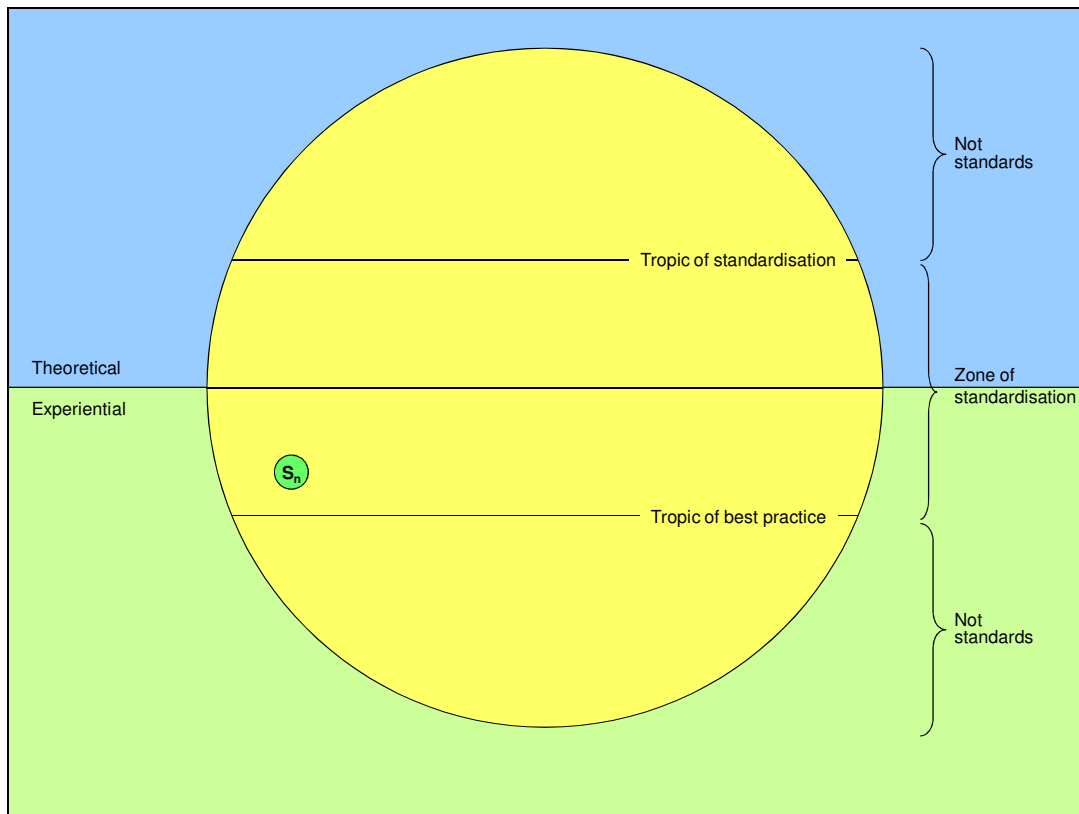


Figure 44: When is a standard not a standard?

In compiling a catalogue of standards to mitigate risk and keep it up to date (for example project γ , Chapter 3), there is a need for change and learning – appreciating when a standard is still a standard. In Figure 44, I consider a specification S_n which may or may not be a standard. S_n+R (where R is the influencing risk) is a standard associated with a risk and will remain the zone of standardisation. S_n-R will be outside the zone of standardisation – a specification without an associated risk. S_n will not be a standard if it does not address a risk. So a standard that is not used can still be a standard. So a more popular standard does not negate the status of ‘rival’ standard(s). R = may or may not be known.

Accessibility of the standard and the information it contains depends on its usefulness, its supportiveness in treating all or part of one or more risks, its helpfulness in effecting a satisfactory outcome to the risk management (Swann, 2000), and its adaptiveness to changing or emerging risks (Carr, Konda, et al., 2003).

6.7.2 Linking risk and standards

The research for CSIA (Project γ , Chapter 3) found that a lack of confidence in standards mitigating risk could be attributed to a lack of clarity in how suitable a treatment was for a risk – would it solve all or part of the problem? In working with users of information systems and the publishers of standards and good practice (Chapters 3 and 5), it became apparent that only part of the application of standards was inhibited by the completeness and rest was a function of the expertise of those applying the standard. To manage the level of expertise

and expectations of the outcome of implementing one or more standards to mitigate risk, the following labelling scheme (Table 64) was devised and applied through CSIA’s catalogue.

Table 64: Ranking of the risk treatments in the catalogue				
		How directly applicable is the guidance to the risk that it could mitigate?		
		A thorough approach A	Significant guidance B	Some help C
No expertise	1	A1	B1	C1
Some expertise	2	A2	B2	C2
Expert knowledge needed	3	A3	B3	C3

6.7.3 Security culture as an indicator of which standards are needed

In my investigation to determine a method to highlight human vulnerabilities in an information system (Project 5, Chapter 4), the results showed that the organisations (or communities) examined were stronger on policy than awareness of the individuals suggesting that closing this gap could reduce the human vulnerabilities, with a resulting improvement in risk culture. This has brought utility into my research to link risk and standards because the knowledge from considering the research questions was producing interesting definitions of risk and its treatment with standards. Without the research into the human vulnerabilities in information systems, the application of the research was lacking. Figure 45 and Table 65 show how an evaluation of the appetite of organisations and the attitude of individuals was compared to four points. By defining the appetite to risk of the organisation as adjustable by whichever controls – defined by standards - may be chosen I had created a chart of the cause and effect of introducing standards and expecting their update.

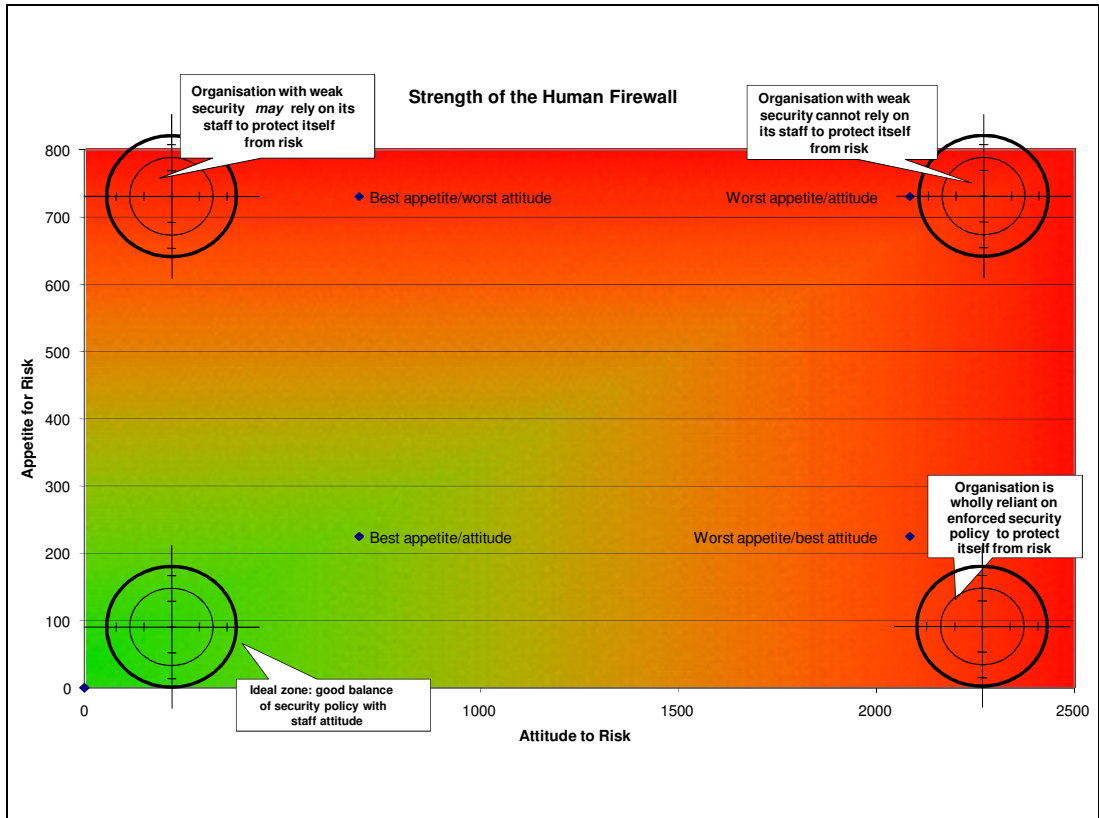


Figure 45: A risk chart: where are mitigating activities needed?

Table 65 Benchmarks of risk appetite and risk attitude	
1	An organisation or community with a 'balanced' appetite for risk with individuals who have a good attitude to risk
2	An organisation or community with a 'balanced' appetite for risk with individuals who have a poor attitude for risk
3	An organisation or community with a poor appetite for risk with individuals who have a poor attitude for risk
4	An organisation or community with a poor appetite for risk with individuals who have a good attitude for risk

The term *balanced* is used here to describe an organisation that is ready to use computer networks with their inherent risks but with controls – or regulators – in place that meet the current best practice (defined herein by International standards). The term *good* is used here to describe individuals who appreciate their responsibilities to manage a degree of risk and whose awareness encompasses the organisational measures in place to allow risk-managed access to the computer network.

Figure 46 shows the chart with the method's results applied to organisations who took part in the in-depth interviews described in Chapter 4.

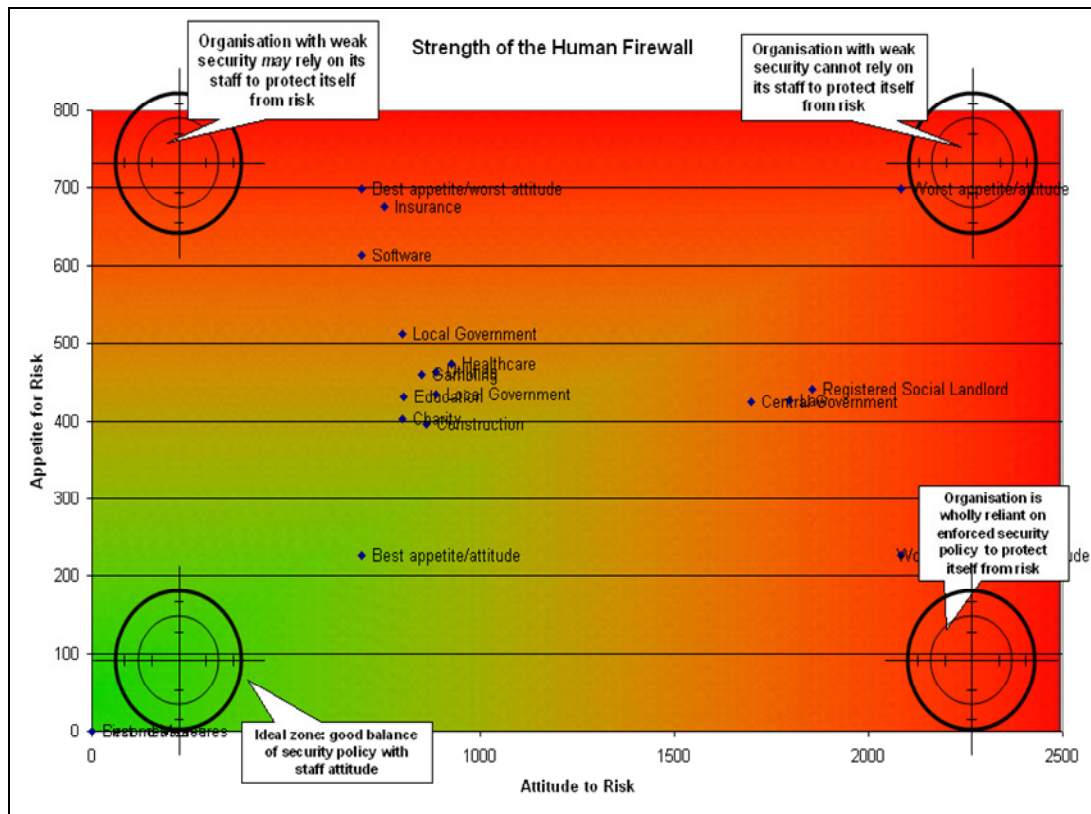


Figure 46: Placing respondents on the at-risk from human vulnerabilities monitor

What may be concluded? I consider that if the attitude of individuals to risk is appropriate, and a organisation (or community) has sound security policies that see benchmarked controls through to implementation, then a risk culture may be said to be fit for the situation when risk attitude and security policies converge. This is shown by the proximity of an organisation (or community) to the bottom left quadrant of Figure 46. This same observation can be used to identify divergence from the accepted appetite and so identify the risk of human vulnerabilities in the computer network. The degree of convergence can be used to measure the amount of remedial action – such as an improvement in risk awareness or a strengthening of security policy.

The project demonstrated four elements of innovation:

- (1) An innovative approach to the numerical measurement of an individual's *attitude* to risk.
- (2) An innovative approach to the numerical measurement of an organisation's *appetite* for risk.

By combining the first and the second innovations, the method derives a new measure of system vulnerability that allows us to identify zones of like-risk culture so that a gap analysis of the 'as is' and 'to be' risk cultures can now provide a basis for:

- (3) Systematic assessment and management of the human component of overall system vulnerability; and

(4) Systematic assessment and management of the organisational component of overall system vulnerability

The data collected in this project demonstrate that there is indeed adequate sensitivity in both the individual and organisational measurement methodologies to provide useful differentiation on both axes and in the derived measure of human vulnerability (Figure 30).

The sociotechnical innovation is shown whereby a more aware and risk-responsible ICT user community should engender a better environment of trust so that, for example, customers would engage with on-line facilities, use the tools given to them by the service providers (such as authentication technology offered by banks) and be themselves more responsible in their behaviour with confidential information. This could impact the potential for teleworking if organisations have used the methodology to make remote users more risk aware and if the organisations take advantage of the vulnerability analysis it provides to show where their teleworking 'human network' may be the greatest risk and so treat it with the lessons-learnt such as the controls or regulators (Ashby 1957; Beer, 1993) in a standard (BS ISO/IEC 27002:2005 BS 7799-1:2005). Benefits of less commuting on staff may accrue for their health, traffic congestion, and opportunities for a work-life balance.

Economic, environmental, and societal benefits may accrue from this methodology. Engagement with this methodology can deliver the opportunity to manage human vulnerabilities and the security breaches associated with them. A tool applying the methodology could be opened up to the whole ICT user market given the ubiquitous nature of network usage either within organisations or between users over the Internet. An ontological approach of preparing user views could adapt the project's deliverables for the home user, the small to medium-sized business, the voluntary sector, corporates, and the public sector too. Statistics from the business sector (DTI/Price Waterhouse Coopers, 2006) were that the average saving of avoiding a security breach would range between £8,000 to £17,000 overall (£65,000 to £130,000 for large businesses) per incident and that this cost increases year on year (DTI/Price Waterhouse Coopers, 2010). As the 2006 survey points out that 62% of businesses realise a security breach and that 49% of security breaches are the result of human factors, the potential savings from using the method to identify the weaker security links would be self sustaining.

The opportunity for improvement increases further by using the method to improve the security culture and therefore reduce the number of most kinds of security incidents. As the dynamic profile changes with technology previously in the domain of the corporates extending to home users (wireless networks for example), the method's database of risks and treatments would be kept up to date to educate the changing profile of the user community. By reducing security incidents ICT can be used more effectively for administration, innovation, research, and leisure.

The costs that would otherwise have been wasted on dealing with security breaches in supply chains can be focused on the core business of users of this method. As the method

will realise an improvement in risk culture within the viewpoints of the ICT user community (suppliers, intermediaries, and end-users) there will be a self-sustaining 'spill over' chain of improvement fuelling the ongoing maintenance of the method to detect human vulnerabilities in information systems for that community.

The method may have the potential to be used as part of a standard for supply chain formation (Dresner and Wood, 2007). The method would support this by supplying human vulnerability measures that can be compared to see what needs to be done for organisations to create zones of common acceptance (of risk).

6.7.4 Enhancing learning through research frameworks

Throughout the period of research I have worked within a three-tiered model (Figure 47) that has organised the research framework into the refined – usually peer reviewed – published knowledge of academic papers and business reports¹⁹⁹, the framework of the standards themselves, and the framework of research projects that have been applied to investigate the research questions (Figure 41).

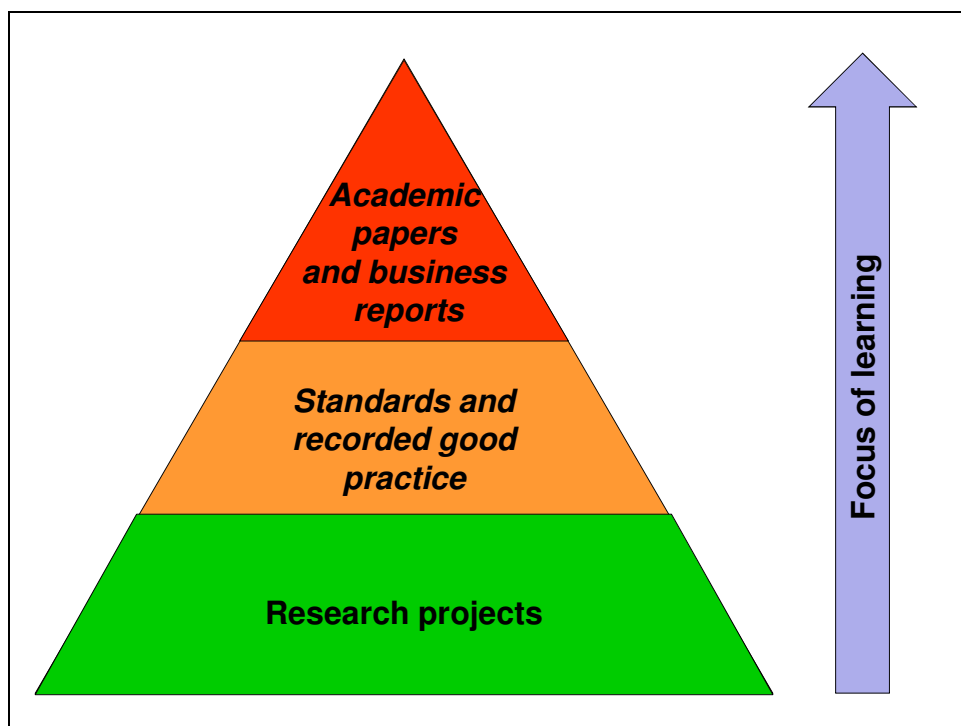


Figure 47: The three-tiered framework of knowledge and research

¹⁹⁹ The peer review of the business reports may not be as clear as the process for academic journals but it is prevalent and is shown by the credits in the DTI/BERR/BIS information security breaches surveys, and the review of information assurance policies published by Cabinet Office and CESG within the information security community. These two examples are referred to here because the significant references to these publications throughout my research.

Figure 48 extends the Checkland-Holwell construct to show how the framework (F) of the standards and the methodologies of the investigating projects (M) merge as the research papers yielding the learning are themselves a framework. The framework of projects overcame at least part of the problem of finding a single methodology that can present meaningful results with surety. The framework (Checkland and Holwell, 1998) introduces variety (Ashby, 1957) to regulate the risk that a monolithic case study may not deliver the breadth of information required for meaningful analysis. So, the framework of projects presents itself as the answer to the meta-research questions about the efficacy of the methodology itself – is this framework a good way of investigating whether standards mitigate risk? The variety in the projects is a risk reduction technique in itself; by looking at the problem through a selection of lenses it is more likely to remove the bias that a single view would constrain. Just as the relationship between many risks and many standards provide the requisite variety for cybernetic assurance, the framework of projects also protect the variety of research from attenuation (Beer, 1993).

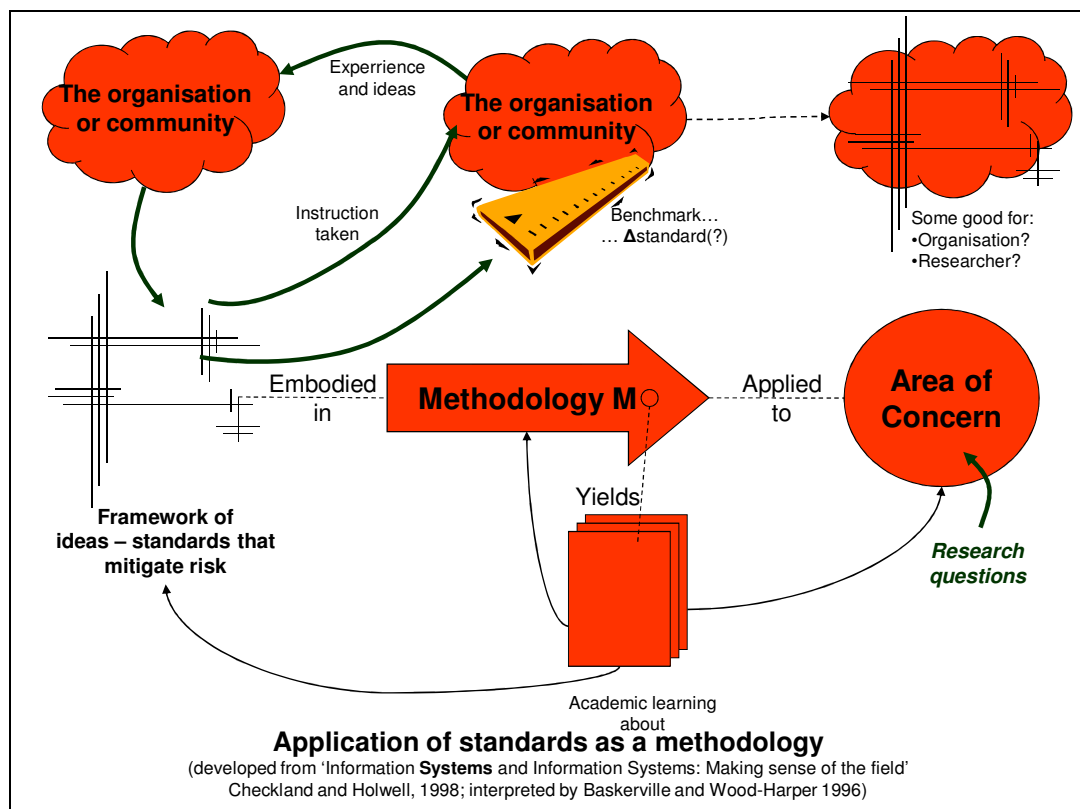


Figure 48: A framework for learning about information assurance

6.8 Recommendations for future work

In this section, I look forward to further investigation to support the findings of my research – to answer with surety the question: do standards mitigate risk? Also proposed is work to develop the tool to find human vulnerabilities in information systems (which is the clearest application of the research done) and to extend the research into a new piece of work that considers the language of risk and builds on the ideas of accessibility of the knowledge in

standards to create an expertise-agnostic method for defining the risk management (security) requirements of an information system.

6.8.1 Do standards mitigate risk?

Despite the popular feedback and positive responses from the participants in the research projects that demonstrated a *consensus view* that standard mitigate risk, there appears to be no evidence of a hard, causal link between the two. The connection remains intuitive. The feedback may be prompted by the apparent comfort that standards may provide. The uptake of standards may be the result of the desire to put trust in the methods of others, and abrogate one's own responsibility for taking risk. Although when standards are proposed as risk mitigating methodologies²⁰⁰ they are warmly accepted as 'lessons learnt' which fits Deming's management cycle of Plan-Do-Check-Act (Deming 1950). 'Check' was later refined to 'Study' (Deming 1986) where study introduces cybernetic feedback to shape the act of adjustment. Although, as the British Standards Institution states in each of its publications the 'compliance with a British Standard cannot confer immunity from legal obligations', it is likely to be a mitigating defence around the seriousness of an infraction if evidence of compliance can be shown. This is suggested by the threat of a £500,000 fine from the Information Commissioner being lessened when an information security management system (BS ISO/IEC 27001:2005 BS 7799-2:2005) is operating.

6.8.2 Developing the tool to find human vulnerabilities in information systems

Chapter 4 describes a feasibility study of the methodology to find human vulnerabilities in information systems using a limited selection of tell-tale vectors derived from a corpus of related research (mainly into insider threats). The methodology would benefit from extracting other elements from the body of research to refine the calculations that produce the plot of corporate risk appetite against individual risk attitude. These may include length of service, or greater psychological or temporal components for example: latent risk (related to the activity supported by the information system), any propensity to risk, and the variation of how people will behave (see Table 68).

A significant contribution to the 'factors' to test for came from Hillson and Murray-Webster, (2007). This was useful in encouraging a partially psychological approach to some of the questioning. A 'wholly psychological' side of vulnerability identification was felt to be beyond the timescales of the feasibility study and would have lost out by excluding some of the components that the research literature includes. This is also something to be developed in future work.

The method to determine the intensity of human vulnerabilities is designed to complement the technical and non-technical – or blended – countermeasures that are well known for use

²⁰⁰ For example by the members' help desk of The National Computing Centre – see Chapter 1.

against outsider threats such as hackers or the malicious software of criminal programmers. Technical measures would include intrusion detection and prevention systems, antivirus/spyware programs and firewalls. Blended measures comprise a combination of more than one reaction to threat, such as an implementation which may use technology to distract a criminal from gaining inappropriate access to a computer network by enticing attempts to access a decoy network or 'honeypot'. The method focuses particularly on the insider threat to information systems but in the wider context of including any stakeholder with legitimate access as an insider. These may include threat-pair vulnerabilities or potential discontentment at not being allowed (say) to use company equipment for personal MP3 downloads. The questions may be refined in future work to investigate more completely how the risk of uncontrolled equipment is made acceptable²⁰¹. It also strengthens the general philosophy for the method: putting the risks into context so that an apparently high risk may be well mitigated by a control. For example, technology designed to manage network deperimeterisation that inspects hardware/software configurations before granting access.

It is considered that non-tangible assets such as reputation, goodwill, staff morale etc. cannot be assigned meaningful, quantitative financial cost (Flechais, Sasse, Hailes, 2003). However, applying relative numbers to the attitude of those who may interact with an information system can translate them into a weighted ranking to put more obvious concerns – as shown by, for example, the Annualised Loss Estimate (Hayden, 2010) – into context to give a final judgement of where attention should be focused and countermeasures deployed to mitigate the risk. These may be new standards which require investment in equipment and training.

The method could be implemented in a tool – which has been labelled 'CatalysIS' – as the hub of a programme to improve risk culture. The tool derived from the method – shown in Figure 49 and explained in Table 66 – would work by asking network users about their attitude to risk, causes of risk, and the activities that may mitigate the risks and their outcomes. The user responses will be analysed for the 'quality of fit' of the attitude of users to the appetite for risk that the network's security policy is intended to realise.

²⁰¹ A problem being tackled with technical controls by the consortium-led Trusted Computing Module, a ubiquitous microchip implanted in 350 million devices (Trusted Computing Group, August 2010).

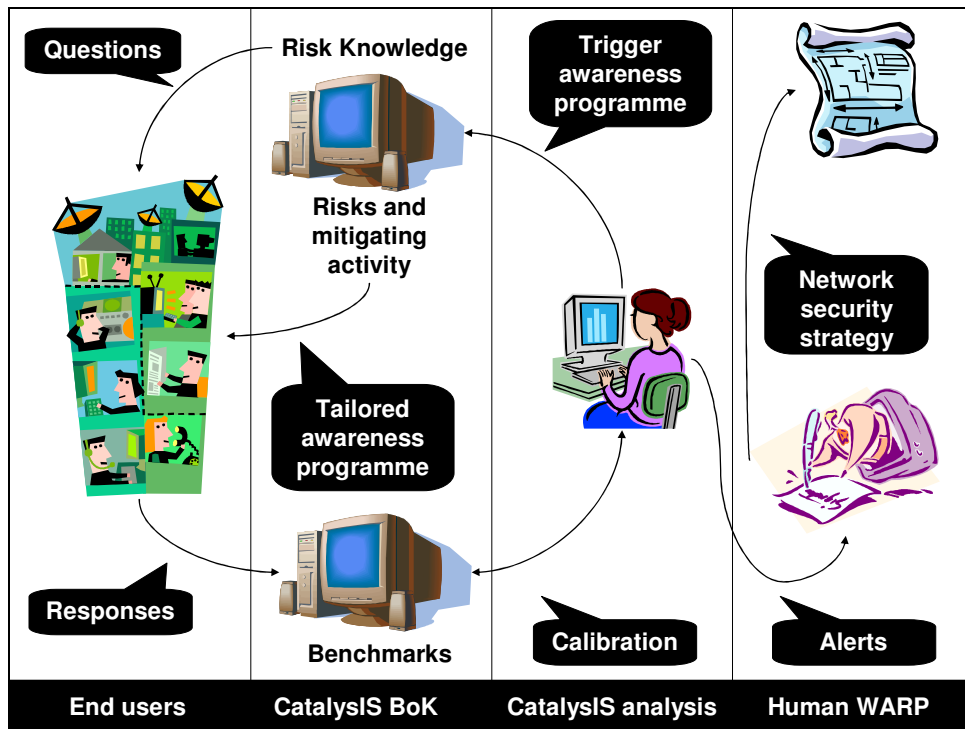


Figure 49: Activity in the method for finding the human vulnerabilities in information systems

Table 66: Components of the method for finding the human vulnerabilities information systems

	<p>(a) Mapping the landscape of risk culture</p> <p>The tool will question an information system’s users about:</p> <ul style="list-style-type: none"> • The organisation or community that has the prevalent stake in the security of the network on which the system relies. • The profile(s) of the users. • How they (the users) feel about risks to the information system and what can be done to treat those risks.
	<p>(b) Getting the measure of attitudes to risk</p> <p>The responses will be scored using a weighted ranking system to give a judgment of:</p> <ul style="list-style-type: none"> • The quality of fit of the individual’s attitude to the organisation’s/ community’s appetite for risk. • The maturity of the individual’s risk attitude in relation to the context in which the information system is used.
	<p>(c) Finding the human vulnerabilities and establishing the programme to improve risk culture</p> <p>The judgement on the risk appetite/attitude will be used to recommend an appropriate security risk awareness programme to improve the risk culture of the organisation or community under scrutiny.</p>
	<p>(d) Programme of improvements to the risk culture</p> <p>Aggregated results from the tool will be used to analyse the overall risk culture and report to stakeholder organisations as well as feeding back into the tool to ensure that its questions and supporting advice are kept up to date.</p>

An established implementation of the tool would alert network authorities to the types of users who may pose a threat to the network. The difference between the users’ attitudes and the intentions of the network security policy will be used to call on appropriately

identified awareness material from a collated body of knowledge and the standards which will match the appetite for risk of the organisation with the impact level of the information that it handles. This would lead to setting benchmarks of risk appetite and attitude which may assist judgements of risk in developing partnerships and supply chains and provide an ongoing body of research data that may be analysed to show areas of risk amongst different sectors or roles (zones of common risk acceptance – Dresner and Wood, 2007).

6.8.3 The language of risk

Some supporting research around the language of risk is needed to support the promulgation of a tool for detecting human vulnerabilities in information systems. Are the terms *risk attitude* and *risk appetite* sufficiently defined and understood? How does one describe appetite which may vary from one organisation to another, yet be good enough for each depending on the risk treatments deployed and the respective residual risk that remains? Some of this is addressed in the model for connecting organisations with a standards-based approach (Dresner and Wood, 2007). The term *good* is used here to describe individuals who appreciate their responsibilities to manage a degree of risk and whose awareness encompasses the organisational measures in place to allow risk-managed access to the information system.

My interest in standards implementation being invoked by the emotional response to risk may be extended to a communications methodology that recognises that certain symbolism evokes emotional responses. For example, the use of red signage in many cultures to warn the viewer of danger or perhaps to use that same emotion to promote a feeling of excitement by the use of red.

Semiotics is the art, science, or understanding of symbols. Words can also be associated with strong emotion and may also be combined with colour to heighten the response – such as the encapsulation of an instruction to ‘stop’ within a red border. Specifiers of requirements for products or services that store and process information may find that the association of certain words can either inhibit or enable specifications that require interpretation to move from intention to realisation. Stating that an information system must be, for example, ‘secure’ may result in the implementation of hardware, software, and processes which restrict access to such an extent that users – with no malicious intention – work around the security constraints and inject information into unintentional information systems or, conversely fail to realise the possible protection with safe outcomes. A requirements specification is challenged with being detailed enough to represent complexity whilst being simple enough to be unambiguous and understandable and not attenuating the description of the information system it models. Security is a *non-functional* requirement of an information system that must be as clearly defined as the colours, (data-formats for example) that are usually associated with other *quality attributes*, such as *usability* or *interoperability*. However, words associated with the specification of security are so riddled

with their own semiotic baggage that they are either used inappropriately, too often, too little, or not at all. Words such as ‘control’, ‘restrict’, ‘legal’, or even ‘risk’ suggest the red terminology of protection or danger.

In the specification of information systems that handle data in a way that is commensurate with all reasonable expectations of the impact resulting in compromise to its confidentiality, integrity, or availability, we need a language that recognises that it can be adapted to the risk literacy of both those who specify the information system and those who must apply that specification in development or delivery. This would manifest in a method to support the development of secure information systems by reducing the risk of inappropriate data processing and increasing the risk of containing the information in an accurate state and available where it is genuinely needed. The method would benefit human vulnerabilities detection (Chapter 4) by providing clear, unambiguous language for questioning the information system actors involved. The lack of a simple language-based tool: a methodology to articulate the requirements for security (MARS) would fill the standards gap shown in the Figure 50 below. In a recent application of the feasibility study tool²⁰², the language of security risks and their treatments that were used in common parlance was frequently misinterpreted by the different actors taking part.

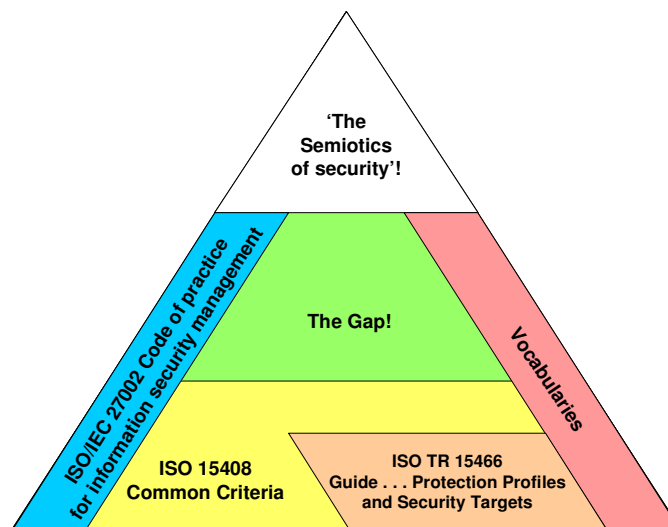


Figure 50: The gap between a non-expert language for formal specification of security requirements and available standards

The need for MARS is shown by the cataloguing work and gap analysis carried out for CSIA that developed the labelling system that was based on the quality of fit of a standard to the risk it was intended to treat and the expertise required to apply the risk treatment captured in the standard. MARS should also be a context-neutral language (Coles-Kemp 2008).

²⁰² In the IT department of part of a county’s emergency services.

6.8.4 Looking back

Looking back over this seven-year period of research – and particularly in experience from the investigation of the risks from human vulnerabilities, development – I would recommend a simpler path and research method which may be viewed as integrated rather than the mixed method that was realised. The steps in the method would comprise (in order) the cataloguing of standards that may treat risk in information systems (projects α and γ), the research and development of the tool to detect human vulnerabilities in information systems (project δ), then field work to apply the tool, find risk from human vulnerabilities, apply standards selected from the catalogue and then reapply the tools after a period of time to determine if those risks had been treated. This course of action would satisfy the first research question: ‘Do implemented ‘Standards’ mitigate risk?’.

6.9 Conclusions





When I established the three questions (Table 67) to shape and direct this research, I did not expect the rich picture of risk, standards, and research that would be sketched, linking so many people across so many organisations for the quality improvement of information systems through the treatment of risk, and a propensity for treating that risk efficiently through the uptake of lessons learnt as documented in standards. It is encouraging that although the research has not provided compelling evidence to answer all three questions, the overall approach of the methodology has become – in parallel to my work – a de facto way of working in many organisations including the policy (or standard) setters in influential areas. I have seen the rigour in the methodology supported academically (Hodgkinson and Coles 2008) and a significant element of its application shown relevance by the development, by the Centre for the Protection of the National Infrastructure (CPNI), of the SeCURE software tool. CPNI’s tool measures the Security Culture Type Indicator (SCTI) as the current nature of the organisation’s security culture – the ‘desired aspirations’ – and the Security Climate Evaluation Survey (SCES) which presents a snapshot of the organisation’s security climate according to its employees. This is complementary to the development of the human vulnerabilities tool which plots the information system risk an organisation faces as a function of its appetite and the attitude of its staff.

Table 67: Final evaluation of the research questions			
	Question	What has the research shown?	Question answered?
1	Do implemented 'Standards' mitigate risk?	There is significant backing for this, showing faith in this premise but the research has not delivered compelling evidence that this is so.	No
2	Can 'Standards' be made more accessible?	Doubts in the relevance of standards and the proliferation of standards which reduce the accessibility of standards and suggest that standards remain an under-utilised body of knowledge are shown to be settled by making the uptake of standards a source of knowledge for mitigating risk which <i>is</i> – at least at an emotional level – an accessible topic.	Yes
3	How do you link risks to the 'Standards' that may mitigate them?	The methodology of creating or selecting a taxonomy of risk against which standards can be mapped according to their efficacy and the expertise required to unlock the knowledge therein has delivered a linking mechanism from the research.	Yes

The work continues. Although there is work to be done to answer the initial research question – 'Do implemented 'Standards' mitigate risk?' – ongoing involvement in the field shows the connection between risk and emotion as the catalyst to release the knowledge from standards (Figure 11). An audit of physical security showed scant attention to the protection of company information but measures of protection were espoused when explained in terms of personal effect such as handbags and mobile telephones. Meanwhile, the interest in the field (Chapter 2) continues and there is articulated faith that standards mitigate risk to information systems: at a Cabinet Office workshop in July 2010 – all four working groups presented 'standards' as part of the solution to information assurance (IA) risk.

This is useful experience and knowledge that supports an understanding of how to apply the paradigm of standards as treatment for risk, given the variables (*Table 68*) of standards of varying suitability, risks of varying complexity, and people of varying attitude.

Table 68: Variables for the methods' success

	Risk	Mitigating standard
Acceptance of risk	 <p>There is a risk but will the actors do anything about it?</p>	 <p>There is a standard that could mitigate the risk</p>
Utilisation of standard	 <p>Actors do <i>not</i> extract the explicit risk treatment from the standard</p>	 <p>Actors <i>do</i> extract the explicit risk treatment from the standard</p>

REFERENCES

- ALARM (February 2001). *A key to success - a guide to understanding and managing risk*.
- Alexander, I.F. (2007). *A Taxonomy of Stakeholders: Human Roles in System Development*, Issues and Trends in Technology and Human Interaction, Editor(s): Bernd, Carsten, Stahl (De Montfort University, UK) IRM Press. 25-71 pp.
- Anderson, R. J. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd Edition, Wiley Publishing Inc.
- Argyris, C.; and Schön, D. (1974) *Theory in practice: Increasing professional effectiveness*, San Francisco: Jossey-Bass.
- Armstrong, J., Rhys-Jones, M., and Dresner, D. (2004). *Managing Risk: Technology and Communications*, Lexis Nexis.
- Ashby, W. R., (1957). *An introduction to Cybernetics*, Second impression, London. Chapman and Hall Limited.
- Australian Agency for International Development (2000). *AusGUIDELines, 5. Managing risk*, The Australian Government's Overseas Aid Program.
- Backhouse, J., Hsu, C.W., and Silva, L. (2006). *Circuits of power in creating de jure standards: shaping an international information systems security standard*, MIS Quarterly Vol. 30 Special Issue on Standard Making, pp. 413-438.
- Banfield, E. (2001). *Dredge first hedge later*, Risk Professional 1/2001, S. 40-43.
- Barker, W.C. (2004), Special Publication 800-60, *Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories*, National Institute for Standards and Technology (NIST).
- Baskerville, R. L. and Wood-Harper, A. T., (1996). *A critical perspective on action research as a method for information systems research*, Journal of Information Technology, Volume 11, Issue 3, pages 235 – 246
- Beer, S. (1993). *World in Torment: A Time Whose Idea Must Come*, Presidential Address to the Triennial Congress of the World Organization of Systems and Cybernetics, New Delhi, India, January 1993. Kybernetes, Vol. 22 No. 6, 1993, pp. 15-43
- Bernstein, P. L. (1998) *Against the Gods: The Remarkable Story of Risk*, John Wiley & Sons
- Bevan, N., and Macleod, M. (1994) *Usability measurement in context*, Behaviour and Information Technology, 13, 132-145
- BIP 0051:2004 ITIL. *Service support*, British Standards Institution

- British Computer Society/Royal Academy of Engineering (2004). *The Challenges of Complex IT Projects*, Royal Academy of Engineering
- British Standards Institution (2000), ISO/IEC 17799 (BS 7799) Part 1:2000 *Information security management: Code of practice for information security management*.
- British Standards Institution, (2001). *The TickIT Guide: Using ISO 9001:2000 for Software Quality Management System Construction, Certification and Continual Improvement*.
- British Standards Institution, 1998, BS 7925-1 *Vocabulary of terms in software testing*.
- British Standards Institution, BS 25777:2008, *Information and communications technology continuity management. Code of practice*.
- British Standards Institution, BS 25999-1:2006, *Business continuity management – Part 1: Code of practice*.
- British Standards Institution, BS 25999-2:2007 *Business continuity management – Part 2: Specification*.
- British Standards Institution, BS 6079-3:2000 *Project management Part 3: Guide to the management of business related project risk*.
- British Standards Institution, BS 7799-2:2002, *Information security management systems – specification with guidance for use*.
- British Standards Institution, BS EN 61014:2003 *Programmes for reliability growth*.
- British Standards Institution, BS IEC 62198:2001 *Project risk management — Application guidelines*.
- British Standards Institution, BS ISO 8807:1989 *Information processing systems. Open systems interconnection. LOTOS. A formal description technique based on the temporal ordering of observational behaviour*.
- British Standards Institution, BS ISO/IEC 20000-1:2005, *Information technology — Service management — Part 1: Specification*.
- British Standards Institution, BS ISO/IEC 20000-2:2005, *Information technology — Service management — Part 2: Code of practice*.
- British Standards Institution, BS ISO/IEC 27001:2005 BS 7799-2:2005 *Information technology — Security techniques — Information security management systems — Requirements*.
- British Standards Institution, BS ISO/IEC 27002:2005 BS 7799-1:2005 *Information technology - Security techniques - Code of practice for information security management*, (Previously ISO/IEC 17799)

- British Standards Institution, BS ISO/IEC 27004:2009, *Information technology — Security techniques — Information security management measurements*.
- British Standards Institution, BS ISO/IEC TR 15846:1998 *Information technology. Software life cycle processes. Configuration management*.
- British Standards Institution, BS7858:2006 *Security Screening of Individuals in a Security Environment*.
- British Standards Institution, PD 6668: 2001, *Managing Risk for Corporate Governance*.
- British Standards Institution, PD CR 13694:1999, *Health informatics. Safety and security related software quality standards for healthcare (SSQS)*.
- British Standards Institution. BS 0:1997, *A standard for standards*.
- Bryant, P. C., Davis, C. A., Hancock, J. I, and Vardaman, J. M. (2010), *When Rule Makers Become Rule Breakers: Employee Level Outcomes of Managerial Pro-Social Rule Breaking*, *Employee Responsibilities and Rights Journal* 22:101-112.
- Bundesamt für Sicherheit in der Informationstechnik (2001). *IT Baseline Protection Manual*
- Cabinet Office (2002). *Security: e-Government Strategy Framework Policy and Guidelines* Version 4.0, September 2002
- Cabinet Office (2004). Central Sponsor for Information Assurance, *Protecting our information systems*, 262949/0604/D40.
- Cabinet Office (2005). e-Government Unit, *e-Government Interoperability Framework* Version 6.1, Cabinet Office, 2005.
- Cabinet Office (2005). *Transformational Government: Enabled by Technology*.
- Cabinet Office (2008). *Security Policy Framework*
- Cabinet Office e-Government Unit (2004). *e-Government Interoperability Framework, Technical Standards Catalogue*, version 6.1, 17 September 2004.
- Cadbury Committee (1992). *Report of the Committee on the Financial Aspects of Corporate Governance*
- Cappelli, D. M.,(2006). *Pay Attention! What are Your Employees Doing?* (Presentation).
- Cappelli, D., Moore, A., Trzeciak, R. (2005). *Management and Education of the Risk of Insider Threat (MERIT): System Dynamics Modeling of Computer System Sabotage*, Carnegie Mellon CyLab.
- Cappelli, D.M, Carnegie Mellon University, Keeney M. - United States Secret Service. (2004). *Insider Threat: Real Data on a Real Problem* (Presentation)

- Cappelli, D.M, Moore, A., Trzeciak, R., Shimeall, T.J., (2009) Common Sense Guide to Prevention and Detection of Insider, Threats 3rd Edition – Version 3.1, CERT, Software Engineering Institute, Carnegie Mellon University.
- Cappelli, D.M, Desai, A.G., Moore, A.P., Shimeall, T.J., Weaver, E. A., Willke, B.J. (2006). *Management and Education of the Risk of Insider Threat (MERIT): System Dynamics Modeling of Computer System Sabotage*, CERT3 Program, Software Engineering Institute and CyLab at Carnegie Mellon University.
- Carr, M.J., Konda, S.L., et al. (2003). *Taxonomy-Based Risk Identification*, Software Engineering Institute.
- Cavanagh, M. C. (1997). *Ethics and Information Systems*, The National Computing Centre Guidelines for IT Management 224.
- Cawthron, E. R. and Rowell, J. A.(1978). *Epistemology and Science Education, Studies in Science Education*, 5: 1, 31 – 59.
- CESG ,(2005). HMG Infosec Standard No. 2 *Risk management and accreditation of information systems*, as published by NISCC, Issue 1.0, August 2005.
- CESG, HMG (2009). HMG IA Standard No.6 - *Protecting Personal Data and Managing Information Risk* (originally known as the Minimum Mandatory Requirements).
- CESG, HMG (2009). IA Standard No. 1, *Technical Risk Assessment*, Issue No: 3.51.
- Checkland P. (1985). *From optimizing to learning: a development of systems thinking for the 1990s*, Journal of the Operational Research Society, 36 (9), 757 – 767.
- Checkland P., and Holwell, S. (1998). *Information Systems and Information Systems: Making sense of the field*, Wiley,
- Checkland, P. (1981). *Systems Thinking, Systems Practice*. John Wiley & Sons.
- Cohen, F. (1997). *Information System Attacks: A Preliminary Classification Scheme*, Computers and Security, 16, 29-46.
- Coles, R. and Hodgkinson, G. P. (2008). *A Psychometric Study of Information Technology Risks in the Workplace*, Risk Analysis, Vol. 28, No. 1.
- Coles-Kemp. E., (2008). *The Anatomy of an Information Security Management System*, A thesis submitted for the degree of Doctor of Philosophy, Department of Computer Science King's College London, University of London
- Crosby, P. (1979). *Quality is free: The Art of Making Quality Certain*, McGraw Hill.
- Cusumano, M. A., Mylonadis, Y., and Rosenbloom, R. S. (1992). *Strategic Maneuvering and Mass-Market Dynamics: The Triumph of VHS over Beta*, The Business History Review, Vol. 66, No. 1, High-Technology Industries (Spring,), pp. 51-94.

- Deming, W.E., (1950) *Elementary Principles of the Statistical Control of Quality*, Union of Japanese Scientists and Engineers (JUSE)
- Deming, W.E., (1986) *Out of the Crisis*, MIT Center for Advanced Engineering Study
- Defense Contract Management Command (1999), *PROCAS; Online Information Center Summary Document* November 1999, Department of Defense
- Department for Environment, Food and Rural Affairs DEFRA (2002)
- Department of Trade and Industry (2005). DTI Economics Paper No. 12, *The Empirical Economics of Standards*, June 2005
- Dourado, P. (2007) cited in '*The Little Book of Leadership*', The Leadership Hub.
- Dresner, D.G., (1992). Usability Now!, *Usability Evaluation Within an ISO 9001 Quality System*.
- Dresner, D.G., (1996). *Usability: Practical Hints and Tips for Applying Cognitive Psychology to User Interfaces*, The National Computing Centre Guidelines for IT Management 208.
- Dresner, D.G., (2005) *Using standards to mitigate risk in information systems*, A Report to Support the Transfer of Research from MPhil to PhD, Submitted after two years of part-time research for the degree of MPhil.
- Dresner, D.G., and Wood, J.R.G. (2007). *Operational risk: acceptability criteria*, The Third International Symposium on Information Assurance and Security (IAS 2007), IEEE CS Press.
- Dresner, D.G., Wood, J.R.G., *CatalysIS: Are you, or have you ever been, a vulnerability?* Report of a feasibility study into the detection of human vulnerabilities in information systems for The Technology Strategy Board, 2007.
- European Network and Information Security Agency, ENISA (2006). *Inventory of risk assessment and risk management methods*, ENISA ad hoc working group on risk assessment and risk management
- Federal Reserve Bank of San Francisco (2002). *Economic Letter, Number 2002-02*, January 25, 2002
- Financial Services Authority (2003). *The firm risk assessment framework*.
- Flechais, I., Sasse, M.A., Hailes, S.M.V., (2003) Bringing security home: a process for developing secure and usable systems, NSPW '03 Proceedings of the 2003 workshop on New security paradigms, ACM
- Flechais, I., Riegelsberger, J., Sasse, A. M., (2005). *Divide and Conquer: The role of trust and assurance in the design of secure socio-technical systems*, New Security Paradigms Workshop '05, ACM.

- Furnell, S.M., and Phyo, A.H., (2003). *Considering the problem of insider IT misuse*, Network Research Group, University of Plymouth.
- Garud. R., and Kumaraswamy, A. (2005). *Vicious and virtuous circles in the management of knowledge: the case of infosys technologies*, MIS Quarterly Vol. 29 No. 1, pp. 9-33/March 2005.
- Gotterbarn, D., and Rogerson, S., (2005). *Responsible risk analysis for software development: creating the software development impact statement*, CAIS.
- Grafton, W., Bytheway, A., and Edwards, C., (1997). *Understanding user perceptions of information systems success*, The Journal of Strategic Information Systems, Volume 6, Issue 1, Pages 35-68.
- Hayden, L., (2010) *IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data: A Practical Framework for Measuring Security and Protecting Data*, McGraw-Hill Osborne
- Harris, R., (2002). *Emerging Practices in Operational Risk Management*, Federal Reserve Bank of Chicago.
- Hedlund, G. (1994). *A model of knowledge management and the N-Form Corporation*, Strategic Management Journal.
- Heisenberg, W. (1927) *Ueber den anschaulichen Inhalt der quantentheoretischen Kinematik and Mechanik* Zeitschrift für Physik 43 172-198 (cited in the Stanford Encyclopedia of Philosophy, (<http://plato.stanford.edu/entries/qt-uncertainty/>))
- Herzog, P., (2004). *Calculating Risk Assessment Values*, Institute for Security and Open Methodologies (ISECOM).
- Higgs, D., *Review of the role and effectiveness of non-executive directors*. (2002).
- Hillson D., and Murray-Webster, R., (2007). *Understanding and Managing Risk Attitude* (2nd edition), Gower Publishing.
- House of Lords (2007). *Fifth Report of the House of Lords Science and Technology Select Committee* (10 August 2007), HL 165-II, p396 – 403.
- Humphrey, C., and Scapens, R. W. (1996) *Rhetoric and case study research: response to Joni Young and Alistair Preston and to Sue Llewellyn*, Accounting, Auditing & Accountability Journal, Vol. 9 Iss: 4, pp.119 – 122
- IEEE Computer Society (2004). *Guide to the Software Engineering Body of Knowledge* (SWEBOK).
- IEEE Std 16085 (2003). *IEEE Standard for Software Life Cycle Processes—Risk Management*, (Previously IEEE Std. 1540-2001 and now ISO/IEC 16085:2006).
- IEEE, (2004). *The Software Engineering Body of Knowledge*

- Information Security Forum (2007). *The Standard of Good Practice for Information Security*.
- International Standards Organisation, PD ISO/IEC Guide 73:2002, *Risk Management – Vocabulary – Guidelines for use in standards*.
- International Standards Organisation. ISO/IEC 9126-1:2001 *Software engineering – Product quality – Part 1: Quality model*.
- International Standards Organisation. ISO/IEC 12207:1995 *Information technology — Software life cycle processes*, International Standards Organisation
- International Standards Organisation. ISO/IEC 15288:2002 *Information Technology – Life Cycle Management – System Life Cycle Processes*, International Standards Organisation
- International Standards Organisation, ISO/IEC TR 15504:1999 *Information technology - Software process assessment*.
- International Standards Organisation, PD ISO/IEC TR 18044:2004 *Information technology — Security techniques — Information security incident management*.
- ISO/IEC 25030:2007 *Software engineering - Software product Quality Requirements and Evaluation (SQuaRE) - Quality requirements*.
- International Standards Organisation. ISO/IEC 38500:2008 *Corporate governance of information technology*.
- James, H.L., (1996). *Managing Information Systems Security: a Soft Approach*, IEEE.
- Jiantao, P., (1999). *Dependable Embedded Systems, Software Reliability*, Carnegie Mellon University.
- Joch, A., (December 1995). *Nine ways to make your code more reliable*, Byte.
- Kaplan, Robert S., and David Norton, (1992). *The Balanced Scorecard: Measures that Drive Performance*, Harvard Business Review 70, no. 1 (January-February 1992): 71-79.
- Kaplan, B. and Maxwell, J.A., (1994) *Qualitative Research Methods for Evaluating Computer Information Systems*, in *Evaluating Health Care Information Systems: Methods and Applications*, J.G. Anderson, C.E. Aydin and S.J. Jay (eds.), Sage, Thousand Oaks, CA, 1994, pp. 45-68.
- Khalil, O., Claudio, A., and Seliem, A., (2006) *Knowledge management: the case of the Acushnet Company*, SAM Advanced Management Journal.
- Kontio, J., (1998). *The Riskit Method for Software Risk Management*, version 1.00, University of Maryland
- Kuntz, T., (1998). *The Titanic Disaster Hearings*, Pocket
- Lacey, D., (2008). *Talking about a revolution*, Infosecurity, Elsevier, October 2008

- Lacey, D., James, B. E., (2010). *Review of Availability of Advice on Security for Small/Medium Sized Organisations*, Information Commissioner's Office
- Leveson, N., and Turner, C.S., (1993). *An Investigation of the Therac-25 Accidents – Part V*, IEEE Computer, Vol. 26, No. 7, July 1993, pp. 18-41
- Logica, (1987). *Quality Management Standards for Software*
- Lopez, J. A., (2003). *Overview of the Basel Committee's Second Working Paper on Securitization*, Economic Research Department, Federal Reserve Bank of San Francisco, 2003
- Magklaras, G.B., and Furnell S.M., (2002). *Insider Threat Prediction Tool: Evaluating the probability of IT misuse*, Computers and Security Vol 21, No 1, pp62-73.
- Myers, M.D., (1997) *Qualitative Research in Information Systems*, MISQ Discovery on May 20, 1997 (citing Kaplan and Maxwell 1994).
- Morton, W., (2002). *Managing Risk: A Practical Guide*, National Computing Centre Guidelines for IT Management 265, 2002.
- National Audit Office, *New IT systems for Magistrates' Courts: the Libra project*, Report by the Comptroller and Auditor General, HC 327 Session 2002-2003: 29 January 2003.
- National Computing Centre, The, (1989). *The Starts Purchasers Handbook*.
- National Computing Centre, The, (2000). *A Guide to Reviews from Desk Checks to Inspections*.
- National Computing Centre, The, (2003). *Survey: Risk Management in IT*.
- National Computing Centre, The, (2004). *Information Security Policy and Practice*.
- National Computing Centre, The, (2004). *The National Computing Centre Guidelines for IT Management 289: Protect and Survive - Defending against application hacking*.
- National Computing Centre, The, (2005). *An analysis of surveys for the Small Business Service of the Department of Trade and Industry*.
- National Hi-tech Crime Unit, (2004). *Hi-Tech Crime: The Impact on UK Business*.
- NISCC, (2002). Technical Note 04/02 *The Security of 802.11 Wireless Networks*.
- NISCC, (2005). Policy and Best Practice 00759 NISCC Best Practice Guide. *Protecting Data Centres*.
- Nonaka, I., and Hirotaka T., (1995). *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*, New York, NY: Oxford University Press.
- Nonaka, I., Toyama, R., and Konno, N., (2000). *SECI, Ba and Leadership: a Unified Model of Dynamic Knowledge Creation*.

- Office of Government Commerce (2003), *Successful Delivery Toolkit*, Version 4.02, October, OGC.
- Organisation for Economic Cooperation and Development, (2002). *Guidelines for the Security of Information Systems and Networks*, OECD.
- Orlikowski, W. J. and Baroudi, J. J., (1991) *Studying Information Technology in Organizations: Research Approaches and Assumptions*, Information Systems Research, Vol. 2, No. 1, March 1991, pp. 1-28
- Parliamentary Office of Science and Technology. (2003). *Government IT Projects (POST)*.
- Phyo, A.H., Furnell, S.M., (2003). *Data gathering for insider misuse monitoring*, Network Research Group, University of Plymouth.
- Phyo, A.H., Furnell, S.M., (2004). *A detection-oriented classification of insider IT misuse*, Network Research Group, University of Plymouth.
- Pickford, J. (Ed.), (2001). *Mastering Risk Volume 1: Concepts*, Financial Times,
- Popper, K., (1963). *Conjectures and Refutations*, London: Routledge and Keagan Paul, pp. 33-39
- Price Waterhouse (1988). *Software Quality Standards: the Costs and Benefits*
- Price Waterhouse Coopers, (2004). *Information Security Breaches Survey 2004*, Department of Trade and Industry.
- Price Waterhouse Coopers, (2006). *Information Security Breaches Survey 2006*, Department of Trade and Industry.
- Price Waterhouse Coopers, *Information Security Breaches Survey, 2010*, Department for Business Innovation and Skill, 2010.
- Price Waterhouse Coopers. (2010). *Information Security Breaches Survey 2010*, Department of Trade and Industry.
- Professor Anthony Giddens, Reith Lectures, (1999).
- http://news.bbc.co.uk/1/hi/english/static/events/reith_99/week2/week2.htm.
- Randazzo, M.R., Keeney, M., Eileen Kowalski, E. (National Threat Assessment Center, United States Secret Service) Cappelli, D.M., Moore, A., (CERT® Coordination Center, Software Engineering Institute), (2005). *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*.
- Ranum. M., (2005). *The six dumbest ideas in computer security*, Information Security Bulletin, Volume 10, 285 – 290.

- Riegelsberger, J., Sasse, M.A., McCarthy, J.D., (2005) *The mechanics of trust: A framework for research and design*, International Journal of Human-Computer Studies, Volume 62, Issue 3, Pages 381-422
- Sasse, M.A., (2003) *Computer security: Anatomy of a usability disaster, and a plan for recovery*, CHI 2003, Workshop on HCI and Security Systems, ACM Press.
- Sasse, M.A., Brostoff, S., and Weirich, D. (2002). *Transforming the 'weakest link' — a human-computer interaction approach to usable and effective security*. In R. Temple & J. Regnault (Eds.), *Internet and wireless security* (pp. 243-258). London: IEE.
- Schein, E. H. (1976) *The Clinical Perspective in Fieldwork*, Sage University Papers Series on Qualitative Research Methods, Vol. 5, Thousand Oaks, CA, Sage.
- Schultze, U., and Stabell, C., (2004) *Knowing what you don't know? Discourses and contradictions in Knowledge Management Research*, Journal of Management Studies.
- Seddon, J., (1998) *The Case Against ISO 9001*, ISO 9000 NEWS 4/1998, International Standards Organisation.
- Shaw, E.D., Ruby, K.G., and Post, J. M., (1998). *The Insider Threat To Information Systems, Security, Awareness Bulletin No. 2-98*, Department of Defense Security Institute.
- Standish Group, (2003). *The CHAOS Report*
- Stewart, T. A., (1997). *Intellectual Capital: The new wealth of organizations*, Nicholas Brealey.
- Stoneburner, G., Goguen, A., and Feringa, A., (2002). (NIST) Special Publication 800-30 *Risk Management Guide for Information Technology Systems, National Institute for Standards and Technology*
- Swann, G. M. P., (2000). *The Economics of Standardization*. Department of Trade and Industry
- Tanenbaum, A. S., (1980). *Computer Networks*, Prentice-Hall, Inc.
- The Local eGovernment Standards Body, (2005). *Prospectus for operating an e-standards service*
- Thomas, M., (1997) *Unsafe Standardization*, Computer, November. 1997, pp. 109–111.
- Toynbee, A., (1949). *The Prospects of Western Civilization*, New York, Columbia University Press, by arrangement with Oxford University Press
- Tuglular, T., (2000). *A Preliminary Structural Approach to Insider Computer Misuse Incidents*, EICAR Best Paper Proceedings.

- Turnbull, N., (1999). *Internal Control: Guidance for Directors on the Combined Code*, Institute of Chartered Accountants in England and Wales, 1999
- Turner, K., (2002). *Safety-Critical Systems: An Approach for Radiotherapy Equipment*, Department of Computing Science and Mathematics, University of Stirling.
- US Office of the Under Secretary of Defense (2004). (Acquisition, Technology and Logistics) / Defense Systems.
- Vara, V., (2007). Ten Things Your IT Department Won't Tell You, The Wall Street Journal, 30 July 2007
- W3C, (2003). *World Wide Web Consortium Process Document*, World Wide Web Consortium 18 June 2003
- William Knight, (2005). *Don't let standards threaten innovation*, Computing, 10 February 2005

This page intentionally blank.

Appendix A. References for Project Delta δ: The risk of human vulnerabilities in information systems

- Barker, W.C. (2004), Special Publication 800-60, *Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories*, National Institute for Standards and Technology (NIST).
- Cappelli, D. M.,(2006). *Pay Attention! What are Your Employees Doing?* (Presentation).
- Cappelli, D.M,- Carnegie Mellon University, Keeney M. - United States Secret Service. (2004). *Insider Threat: Real Data on a Real Problem* (Presentation)
- Cappelli, D.M, Desai, A.G., Moore, A.P., Shimeall, T.J., Weaver, E. A., Willke, B.J. (2006). *Management and Education of the Risk of Insider Threat (MERIT): System Dynamics Modeling of Computer System Sabotage*, CERT3 Program, Software Engineering Institute and CyLab at Carnegie Mellon University.
- Cohen, F. (1997). *Information System Attacks: A Preliminary Classification Scheme*, Computers and Security, 16, 29-46.
- Flechas, I., Riegelsberger, J., Sasse, A. M., (2005). *Divide and Conquer: The role of trust and assurance in the design of secure socio-technical systems*, New Security Paradigms Workshop '05, ACM.
- Furnell, S.M., Phyo, A.H., (2003). *Considering the problem of insider IT misuse*, Network Research Group, University of Plymouth.
- Herzog, P., (2004). *Calculating Risk Assessment Values*, Institute for Security and Open Methodologies (ISECOM).
- James, H.L., (1996). *Managing Information Systems Security: a Soft Approach*, IEEE
- Magklaras, G.B., Furnell S.M., (2002). *Insider Threat Prediction Tool: Evaluating the probability of IT misuse*, Computers and Security Vol 21, No 1, pp62-73.
- Phyo, A.H., Furnell, S.M., (2003). *Data gathering for insider misuse monitoring*, Network Research Group, University of Plymouth.
- Phyo, A.H., Furnell, S.M., (2004). *A detection-oriented classification of insider IT misuse*, Network Research Group, University of Plymouth.
- Randazzo, M.R., Keeney, M., Eileen Kowalski, E. (National Threat Assessment Center, United States Secret Service) Cappelli, D.M., Moore, A., (CERT® Coordination Center, Software Engineering Institute), (2005). *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*.

- Shaw, E.D., Ruby, K.G., and Post, J. M., (1998). *The Insider Threat To Information Systems, Security, Awareness Bulletin No. 2-98*, Department of Defense Security Institute.
- Stoneburner, G., Goguen, A., Feringa, A., (2002). (NIST) Special Publication 800-30 *Risk Management Guide for Information Technology Systems, National Institute for Standards and Technology*
- Tuglular, T., (2000). *A Preliminary Structural Approach to Insider Computer Misuse Incidents*, EICAR Best Paper Proceedings.

Appendix B. Project catalogue

Label	Project
Alpha α	An analysis of surveys for the Small Business Service of the Department of Trade and Industry where a 'Top 10' view of risks to information systems was derived. This highlights what the research problem is.
Beta β	Research and development of a project Brief for the British Standards Institution (BSI), ' <i>Using Standards to Mitigate Risk in Information Systems</i> ' which made the justification of why guidance is needed to promote standards should be promulgated as risk treatments.
Gamma γ	A project to establish a catalogue of which standards treat risks associated with information assurance.
Delta δ	Research and development of tools to detect where there are risks as a result of human vulnerabilities in information systems.
Epsilon ϵ	The development of the Accredited UK (AUK) General Segment – a standard to manage the risk in the supply of ICT by small to medium-sized ICT suppliers ²⁰³
Zeta ζ	Work with the Local e-Government Standards Board (LeGSB ²⁰⁴) to define a process for the development and adoption of standards, and to pilot a process to 'certify' the acceptance of standards.
Eta η	Fieldwork: Housing association – recommending an information systems risk (security) strategy.
Theta θ	Fieldwork: Construction – supporting a firm in its identification of risk and the selection of controlling treatments to mitigate them.
Iota ι	Fieldwork: Pensions and actuarial services – a review of risk management (information security) policies in a financial services firm.

²⁰³ A segment is an ICT discipline such as network design and installation, software development, or ICT consultancy. Each discipline is expected to manage risk by carrying out its own specialist activities *and* a set of activities that are carried out in every ICT business. It is the latter set of activities that are defined in the 'General Segment'.

²⁰⁴ Eventually becoming the e-Standards Body (e-SB)

This page intentionally blank.

Appendix C. Achievements based on this research

A.1. Projects

Information Assurance for SMEs (IASME) with the University of Worcester (2009 -)

Development of The National Computing Centre Standard for IT Departments
(and 4 pilot assessments) 2009

Information Governance Watch, exploring a standards observatory for the Technology
Strategy Board, *March 2009*

Assessing to the Accredited UK standard for ICT suppliers
Communications Consultancy and Software Segments
October 2008 -

CatalysIS: Are you, or have you ever been, vulnerability? *November 2007*

A Catalogue of Publicly Available Information Assurance Guidance, and Maintaining a
catalogue of standards and best practice advice for effective information assurance,
for the Central Sponsor for Information Assurance
March 2007

Development of the Accredited UK General Expectations standard for ICT suppliers *2006*

IT Risk Assessment and Guidance Tool, Small Business Service of DTI/Business Link

Using Standards to Mitigate Risk in Information Systems: Project Brief
*Prepared by The National Computing Centre for The British Standards Institution in
response to: the work programme of Committee IST/15 Software Engineering in
collaboration with BSI Publications 2004*

Local e Government Standard Board: Standards Development and Adoption Process (2004)

A.2. Books

Information Security Management: A standards approach. A Best Practice guide for decision
makers in IT, The National Computing Centre, ISBN 0-85012-885-4, 2006

Armstrong, J., Rhys-Jones; M., Dresner, D., Managing Risk: Technology and
Communications, Lexis Nexis, ISBN/ISSN 0-7545-2468-X (Chapter 7: Managing
Operational ICT Risk with Standards and Best Practice) 2004

A.3. Conferences and seminars

Amulets, kitemarks and certificates: How to nail IA standards to the pedestal of trust
Seminar for CESG, *October 2009*

The human face of information assurance - A tool box to keep a smile on it
Seminar for the Home Office, *July 2009*

Emerging trends, Redstone seminar, *July 2009*

Business Oriented Security Strategy, Symantec seminar, *May 2009*

Policy management for IT Governance, British Standards Institution Conference, *May 2009*

Chairing the England North Branch of the Institute of Information Security Professionals
(seminar meetings *January, April, September 2009*) including 'I'm certified therefore
I'm secure. So many badges to choose from' (How *The National Computing
Centre IT Department Standard* provides one rule to ring them all.)

Information security, (ISO/IEC 27001 in 13 Steps), DLM Forum Members Meeting, Prague,
April 2009

Standards, Innovation, and the Toynbee Conflict at Information Governance Watch,
March 2009

Representing the user view at the ENISA/Cyber security KTN workshop, *March 2009*

From here to . . . ity: . . . a route map to standards (. . . and what needs standardising),
Civil IA Products and Services Coordination Group (CIPCOG) Standards and Policy
Conference *Sept 2008, (London)*

Are you now, or have you ever been, a vulnerability? (The people/technology balance),
Symantec Seminar *June 2008, (Manchester)*

Security: the other inconvenient truth: the tackling the 'green' agenda satisfies your security
requirements too, NCC Conference 2008 – Sustainable IT *June 2008*

PKI for Aspiring Dummies, ISACA Northern England Chapter *February 2008*

Finding Risk One of the Top 10 IS/IT Risks, IT Hot Spots - The Sequel
Institute of Internal Auditors *January 2008 (Manchester)*

Acceptable risk across the enterprise, NCC Enterprise Architecture Workshop
December 2007

The risk of success, NCC Business Continuity Conference *September 2007*

Risks are your responsibility! What are they and what can you do about them?
NCC IT Governance Seminar
*May 2005 (Manchester), November 2005 (London), June 2006 (Cardiff),
and March 2007 (Birmingham)*

Robust service delivery through standards, NCC Professionalism Workshop
December 2006

Risks are your responsibility! What are they and what can you do about them?
Presentation to a joint NCC/BSI IT Governance Conference
November 2005

Top Ten IS/IT Risks (and what to do about them)

A paper presented to a joint conference of the Northern Chapters of
the Institute of Internal Auditors (IIA)
and Information Systems Audit and Control Association (ISACA)
October 2005

Enrolling the fifth column: Don't teach security, teach risk management

Presentation at the 'Teaching Security' conference at the University of Leeds
January 2005

Leadership Lecture/Case Study: Fulfil your digital obligations in 13 steps, Infosecurity North

October 2004

A.4. Papers and articles

The Challenge Remains for Escrow, NCC Weekly News, 11 May 2010

Privacy should be a social norm, Pulse,

The Journal of the Institute of Information Security Professionals, Spring 2010, Issue 3

NCC Guidelines for IT Management 332

Business Oriented Security Strategy: when did you last see your data? January 2010

Information Governance Watch, report from an exploratory workshop, *24 March 2009*

Whose data is it anyway? A fresh view on cost-effective security measures

Public Sector Executive, *December 2008*

NCC Guidelines for IT Management 275 *Desert Island Standards II, November 2008*

Are you now, or have you ever been, a vulnerability? - Fresh view on an old problem

Conspectus, IT Infrastructure and Security Review, *November 2008*

NCC Guidelines for IT Management 319 *Information Systems Continuity - a framework for
accountability, continuity, quality, security, sustainability and maturity, October 2008*

Computer Weekly Security Think Tank:

- What are the national threats from hackers, *Sept 2008*
- How do you protect from malware your mobile employees and customers, who lie beyond the network frontier? *May 2008*
- Has the government got the business case for ID cards right? *April 2008*
- What tools can be used to prevent or mitigate employee wrongdoing? *March 2008*

HMRC fiasco offers risk culture lessons *Computer Weekly, 8 January 2008*

With Professor J. Robert (Bob) G. Wood, Operational risk: acceptability criteria, The Third International Symposium on Information Assurance and Security (IAS 2007, Manchester)
IEEE CS Press, 2007

Dr Who and the fable of the exploding door – defence in depth
Computer Weekly, 2 November 2007

Make sure SOA truly starts with service, *Computer Weekly, 21 November 2007*

Security means quality means governance,
Public Sector Executive magazine, December 2005

Top Ten IS/IT Risks
An analysis of surveys for the Small Business Service of the Department of Trade and Industry, February 2005

The Standard Response,
IT Adviser, The Magazine for Members of The National Computing Centre, July/August 2005

With William Roebuck, NCC Legal Guideline 5
ICT Legal Compliance, September 2005

Creating a metathesis or 'Thesis writing: the great leveller', a co-developed paper for the doctoral school at the School of Informatics
University of Manchester, 2005 (Wood-Harper, Trevor, al Balushi Taiseera; Ding, Yishu; Dresner, Daniel; Gledson, Ann; Hargreaves, Katharine; Khan, Mukaram; Kuo, Chen-Li; Lee-Klenz, Soonhwa)

How risk can be mitigated by standards, 2005 (*Academic report*)

How risk can be mitigated by standards, 2004 (*Business report*)

Managing Risk and Your Business,
IT Adviser, The Magazine for Members of The National Computing Centre, March/April 2004

A.5. Education and training

Information Asset Management, ½ day workshop, January 2010, (Maidenhead)

Internal Audits of Business Continuity, One day workshop, *October 2009, (London)*

Information Security in the Public Sector

Training Programme for the Chinese Ministry of Finance, *July 2009, (Manchester)*

IT Governance, workshop for the British Standards Institution, *May 2009, (London)*

Assessor Training – accrediting new assessors for AccreditedUK
April and May, 2009 (Manchester)

IT Governance workshop, *February 2009 (Edinburgh), March 2009 (Cardiff)*

Security: From Risk to Treatment, One day workshop:

April 2008 (NCC, Manchester), July 2008 (London), September 2008 (Manchester), February 2009 (London)

CS639/COMP60391/COMP61421 Computer (and Network) Security Module of the University of Manchester Advanced Computer Science MSc, 2004, updated 2005, 2006, 2007, 2008, 2009, 2010²⁰⁵

Dredge first, hedge later: Keeping risk business-focused (Aspects of information risk - being proportionate)

Construction Industry Computing Association (CICA) Workshop, 7 November 2007

Information Security Management: A standards approach

One day workshop: March 2006 (NCC, Manchester)

A.6. Action research/field work

IT Department Accreditation including a government agency, an examining body, and a university administration body (2009 – 2010)

ISO/IEC 27001 implementation in construction (2010)

A route map for compliance to security (ISO/IEC 27001) and business continuity (BS 25999/25777) standards in construction (2010)

A route map for compliance to security standards (ISO/IEC 27001) in construction (2009)

Awareness of Information Assurance for the IT department of a county constabulary (2009)

Good practice in IT services (ISO/IEC 20000) – a review for a financial service firm (2009)

Business continuity advice (BS 25999/BS 25777) for a financial service firm (2009)

Information security audit in finance – life policy trading *(2008 and 2010)*

Software quality standards implementation *(2008)*

Round table investigation into compliance and standard in finance
– venture capitalist *(2008)*

Information security management project in the construction sector *(2007 - 2008)*

Security analysis and policy development in finance – pensions and actuarial services *(2007)*

Information security management project in the social housing sector *(2007)*

Piloting the Local e Government Standard Board Standards Certification Process *(2005)*

²⁰⁵ 44 students (2004), 34 students (2005), 71 students (2006), 57 students (2007), 61 students (2008), 82 students (2009), 45 students (2010).

A.7. Other activity

Commentary and contributions to the following, developing standards:

- BS 25777 IT Service Continuity Management (2008)
- PAS77 - IT Service Continuity Management (May 2006)
- BS 31100 Code of practice for risk management (July 2007)
- PAS 74 Internet safety - Access control systems for the protection of children online - specification (June 2006)

Commentary on the BIS Information Security Breaches Survey 2010

Commentary on the BERR Information Security Breaches Survey 2008

Response from: The National Computing Centre to the House of Lords Science and Technology Committee Investigation of Personal Internet Security, *October 2006*

Commentary on the DTI Information Security Breaches Survey 2006

MPhil/PhD transfer report: Using standards to mitigate risk in information systems
30 November 2005