

Title: The Effect of Organisational Structure and Culture on Information Security Risk Processes

Event: Risk Research Symposium – 5th June 2009

Author:

Dr. Lizzie Coles-Kemp,

Information Security Group,

Royal Holloway,

Egham,

TW20 0EX

lizzie.coles-kemp@rhul.ac.uk

Abstract

Risk management is regarded by many as the corner stone of any information security management framework. The international standard for information security management, ISO 27001, defines risk management as mandatory and information security literature supports this doctrine. However, the literature is lightweight in terms of its discussion of the organisational dynamics that affect the selection and use of information security risk assessment techniques. Furthermore, there is little discussion about the processes of multi-stakeholder risk negotiation and response. As a result there is little shared knowledge of the selection criteria for information security risk assessment methods and the design of information security risk negotiation processes. This knowledge gap is a contributing factor to the development of inappropriate information security policies and the discrepancies between the information security policy and organisational behaviour that lead to information security incidents such as data loss.

In order to address this knowledge gap, an eight year ethnographic study focused on the relationship between information security management process design and organisational structure and culture. As an extension to this study, analysis on the data collected catalogued the varying uses of information security risk assessment and negotiation techniques and identified organisational aspects that affect their selection and implementation within an information security management framework. The longitudinal aspect to the base study enabled analysis of maturity paths of information security risk processes and their impact on the information security management framework. The conclusions and recommendations resulting from the analysis are presented in this paper.

Key words: information security risk, information security management, ISMS

1. Introduction

Risk assessment is regarded as an integral part of any information security management framework. This is because an information security management framework exists to enable an organisation to maximise the use of its information within a level of risk that is acceptable to the organisation. In information security management literature risk assessment processes are presented as pivotal to the success of the information security management framework. Risk assessment is used to establish the ISMS, determine the information security risks that an organisation faces, and identify the security countermeasures necessary to reduce the risks to an appropriate level. The emphasis is on an “appropriate response” to the measure of risk where appropriate is considered in the overall context of the organisation.

Risk assessment is enmeshed with additional organisational processes that construct what is termed an Information Security Management System (ISMS). An information security management system is primarily described in the information security management standard ISO 27001 [9, clauses 4-8]. It is an abstracted organisational model found in information security management literature which articulates a systematised view of the information security management functions and processes described in much of the information security management literature. The role of an Information Security Management System (ISMS) is to ensure that adequate controls are

“established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of an organisation are met.” [8, p. viii].

In this regard, an ISMS is comprised of logical management functions and management processes. The relationship between risk assessment and the other information security management processes is described in Figure One which shows that the processes interact in a continuous loop, termed the Plan-Do-Check-Act cycle (PDCA) or Deming Wheel in security management literature. The dominating decision making processes are risk based and constitute some form of risk assessment or evaluation. However the extent to which the process is a “technical”, standardised one, is highly dependent on the organisational context, as this paper discusses.

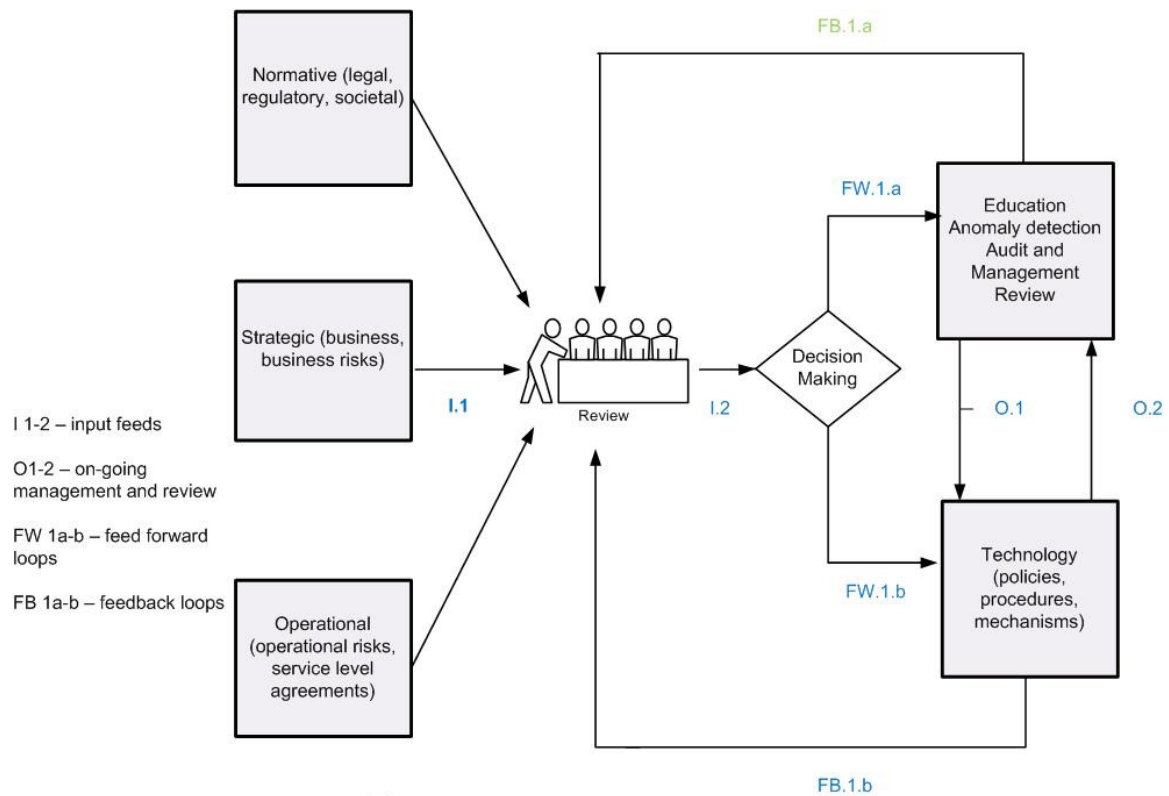


Figure One: A Granular View of Information Security Management

As the diagram in Figure One illustrates, feedback loops are used to channel the output from the processes, the policies and the mechanisms into the review function in order to maintain and improve the ISMS. As the output of all the processes are fed back into the review function, it can be seen that all management processes contribute to decision making. As the PDCA loop gains momentum the information security management functions increasingly interoperate in order to provide a cohesive system for managing security, this pattern is further explained in section five of this paper.

2. Summary of Findings

An eight year study of thirty six organisations and their implementations of ISMS analysed the relationship between organisational context and the manner in which information security management processes are implemented. This was a longitudinal study and therefore shifts in the approaches to implementation were identified and analysed. As risk assessment is pivotal to the ISMS, much of the focus of this study was on the information security risk assessment processes. The following key findings were made in relation to the implementation of such processes.

Information security management literature presents a large number of methodologies for the assessment of risk. However, interestingly, there is little discussion about the motivation for the selection of the risk assessment methodology and the risk assessment methodologies presented are explicitly characterised. Research into the structure of ISMS [6] concluded that this lack of discussion was one of the main reasons why organisations choose risk assessment methodologies on a seemingly *ad hoc* basis. Analysis of information security incidents that took place in organisations that were a part of this study concluded that the selection of an inappropriate risk assessment method resulted in a lack of visibility of the risk and therefore an inappropriate information security response in terms of both policy and the information security countermeasure selected.

This research concluded that instead of categorising information security risk assessment as statically qualitative or quantitative in approach, as information security literature traditionally does, a more accurate picture of the information security risk assessment process is formed if three dimensions to an information security risk assessment methodology are considered. These dimensions are: the degree of qualitative assessment present in the methodology, the extent to which risk assessment was run by an external specialist or individuals internal to the operational process and whether the approach was standardised or more informal in nature.

Finally, this research concluded that there is a pattern to the development of the information security risk assessment with an organisation and that this pattern constitutes a refinement of the information security risk assessment process where the three dimensions interact in different ways as ISMS embeds further into the operational processes within an organisation. The pattern is driven by a number of factors, including: maturity of the ISMS, organisational culture and organisational state. These are not discrete factors, but combine in different ways to affect the choice of risk assessment process. Disruptions to the pattern are caused by a number of contextual interventions, including: pace and type of organisational change, use of technology and type of organisation.

Given that risk assessment is an enmeshed part of the ISMS, if there is a lack of visibility of aspects of the risk assessment process, the effectiveness of an ISMS is only partially evaluated and some aspects of risk assessment and its contribution to information security management are not identified. Equally some information security risks remain invisible to the organisation.

3. Research Approach

A research framework consisting of ethnographic data collection methods and qualitative, thematic analysis was implemented longitudinally into a research bed of 36 organisations. Snap shot

ethnography was used, by observing the organisations multiple times over a five year lifespan. The role of the researcher was to observe, listen and ask questions but not to implement information security solutions.

In addition to observations, semi-structured interviews were undertaken with multiple key stakeholders at several levels in each organisation and by reviewing information flows and information security decision making cycles. The inductive approach enabled the researcher to allow research questions to emerge and draw out the key points by enabling the subjects to articulate their perspectives using their own narratives. A reflective process was used to reduce or neutralise biases and all the findings were fed back both to the research participants and to a third party panel.

In tandem with the field research, a literature search was undertaken in order to clarify the description of an ISMS and to understand the perceived role of risk assessment within the ISMS structure.

Iterative qualitative content analysis was then performed against the following characteristics:

- i. The type and construction of the risk assessment processed used;
- ii. Type of organisation, the culture and organisational state of the section of the organisation involved in the risk assessment ;
- iii. The job profile of the stakeholders include din the risk assessment process;
- iv. The rate of organisational change that the scope of assessment is being subjected to and the causes of the change.

The longitudinal nature of the research enabled shifts in these characteristics to be identified and further analysis to be conducted on the effect that the shifts had on the risk assessment process.

4. *Types of Risk Assessment*

There were a wide range of risk assessment methodologies documented in the literature that are on a continuum between qualitative and quantitative approaches to assessing risk. There is some discussion of the role of the facilitator [12] but not in any depth and not in terms of being a factor that differentiates risk assessment methodologies [5]. There is no discussion of the difference between standardised and informal risk assessment, it is assumed that all information risk assessment is standardised. This insistence that all risk assessment is standardised, results in a blind spot for the ISMS because organisations are not uniform in nature. Some organisational units have a greater tendency to use *ad hoc* informal information security risk assessment and culturally it is very

difficult and often inappropriate for a change to take place. This results in a tension between the organisational unit and the approach to security management and often reduces the visibility of information security risks by the ISMS.

The main discussion in information security management literature, therefore, revolves around the issue of quantitative versus qualitative risk assessment methodologies. The qualitative end of the spectrum is typified by Peltier's high level, unstructured, qualitative risk assessment methodology FRAAP [12] and the quantitative end of the spectrum is typified by approaches such as the risk assessment methodology CCTA Risk Analysis and Management Method (CRAMM) [3].

This research concluded that initially an organisation selects a risk assessment methodology that is more quantitative in nature, but as the ISMS matures, qualitative approaches become more dominant and the approach that is more likely to be presented as the standardised methodology within an organisation. The following reasons are typically given when explaining why qualitative risk assessment becomes the more dominant methodology in information security management:

“What is more commonly found, and indeed often much more useful from a management decision support perspective, is to treat operational risk assessment on a purely qualitative basis” [13, p. 452].

The research concluded that there is an alternative explanation for the emergence of this type of methodology and that providing useful input to the organisational decision making process is not only achieved through qualitative risk assessment [10]. The alternative explanation emerged as a result of analysis of the interviews held with information security managers and risk assessors over the lifespan of the research. The emergence of the qualitative approach as an ISMS matures is largely due to the fact that members of the organisation become specialists in information security as the organisation learns how to view itself from an information security perspective and therefore qualitative judgments become more easily obtainable and more accurate. It is also important to note that quantitative risk assessment methodologies have a much greater emphasis on asset modelling and threat and vulnerability modelling and therefore are of value to an organisation when it first considers information security as at this stage an organisation undergoes a process of learning about its information and sets an initial baseline for the threats and vulnerabilities that it faces.

All 36 organisations in this study changed or adapted their risk assessment processes throughout the lifetime of the study and all organisations adapted their processes to include more qualitative and simpler risk assessment methodologies. However, in instances where quantitative risk assessment

was replaced completely with qualitative risk assessment methodologies there was a greater likelihood that some information security risks were not identified and as a result security incidents took place. In two of the organisations studied, incidents took place which was demonstrated to be as a direct result of lack of quantitative risk assessment of the IT architecture.

When analysing the motivation for selecting a specific information security risk assessment methodologies, it became clear that organisations were not viewing risk assessment methodologies as a single entity. In order to understand the motivation, the structure of the risk assessment methodology needed to be understood from the organisational perspective.

4.1 The structure of Risk Assessment

Whilst there is a large body of documentation on risk assessment methodologies within the security management literature, the literature standardises on the underlying construction, which can be summarised in the following steps [13, p. 190]:

- i. Identify and value the assets;
- ii. Identify the possible threats;
- iii. Identify and quantify these impacts by relating back to your asset list;
- iv. Identify and quantify these vulnerabilities or weaknesses;
- v. Identify the possible control strategies and quantify the cost (total cost of ownership) for these controls;
- vi. Quantify the benefits and the costs.

In the case of information security, assets are information assets or assets that relate to information and threats are potential attacks that may take place on the information assets. The quantification of the benefits and costs leads on to the risk treatment phase in which decisions are made as to which risks must be responded to and the type of response that is to be carried out.

The assumption in the security management literature is that a risk assessment methodology is a single entity, rather than the sum of its methods. This was not the finding of this research. It was the finding of this research that whilst an organisation may adopt an overall approach to risk assessment, different organisational units in different organisational contexts will select different methods to be deployed within the risk assessment process. It was the conclusion of this research that the selection of methods deployed within an information security risk assessment methodology was based on a number of factors: the objective of the risk assessment, time available to gather the

data for each stage of the assessment, the rate of change of the context affecting each stage of the assessment, the degree of precision necessary, the types of stakeholders both available and necessary for each stage and the culture in which the risk assessment operates.

Therefore risk assessment methodologies are not a single entity and if they are viewed as such, the likelihood of the wrong methods being deployed in the wrong context, increases. This leads to a greater possibility of certain types of risks being overlooked at the level of the organisational unit. For example, the methods used to identify technological threats and vulnerabilities are different to the methods used to identify business process and organisational threats and vulnerabilities. This is because the objective of the risk assessment is different in each case. In the case of technological threats and vulnerabilities deductive quantitative testing and attack analysis methods are used in order to determine attack paths and theoretical weaknesses. The deductive approaches are used because the problem the risk assessment needs to analyse is heavily de-contextualised and in this environment there is a linear connection between the different risk variables. In the case of organisational process and organisational threat and vulnerability analysis qualitative scenario based assessments are more appropriate methods because dependencies between the different components are of more importance, the problem is no longer a discrete one and the risk is understood in terms of the impact on the organisational process.

4.2 Risk Assessment Type - Conclusions

From the research a number of conclusions were drawn about the selection of different risk assessment methods:

- Qualitative/quantitative risk assessment methods are selected based on the type of problem, degree to which accuracy is required and the time needed to identify the impact and likelihood values to the necessary level of accuracy [11].
- Standardised/informal risk assessment methods are selected depending on the time available to make a risk decision and whether risk decision making is regarded as part of operational activity or an externalised process.
- Internal/externally driven risk assessment methods are selected depending on the degree and manner in which the risk assessment activity is embedded into the operational process and the extent to which facilitators are used to synthesise the output from the different risk assessment methods. In some environments there is a heavy use of facilitators, in other environments policy designers and auditors are used to synthesise the outputs.

5. *Pattern of Refinement*

All 36 organisations researched started out with one approach to risk assessment where the methods used were more quantitatively oriented, externally driven and standardised. The pattern of refinement that is undergone in each organisation to develop a more granular selection of risk assessment methods is primarily linked to the maturity of the ISMS, which charts the extent to which an ISMS is embedded into individual organisational units as part of the organisational processes. This research concluded that there are six stages of ISMS maturity, as summarised in Table One. Each stage of maturity increases the extent to which the structure and ownership of the security management processes are devolved from centralised control.

The appearance of risk decisions in a range of decision making fora in Stage Three is significant because this is the first move towards differentiating between information security risk assessment findings that are organisational and business process in nature, technological in nature and aspects of information security risk that are relevant to issues that are regarded as business risk. In Stage Four observation of these fora and analysis of the documentation related to such fora, show that this development also indicates that by this stage, information security risk assessment is starting to be regarded as an embedded part of operational activity. This research concluded that the categorisation of risk, found in [1, pp. 2-5], is extremely useful when analysing how the pattern of ISMS maturity affects risks identified through ISMS processes and therefore the risk assessment methods deployed. This categorisation can be seen in Table One.

ISMS Maturity Stage	Characterisation	Implications for Risk Assessment
Stage One: Externalised information security management processes designed and implemented by an external resource.	Information security risks are expressed using the specialist information security language;	Standardised use of risk assessment. Risk assessment decisions made in one location.
Stage Two: All management processes operational	Interaction between the management processes formal and externalised.	Risk assessment starts to take input from the other management processes.
Stage Three: The PDCA cycle starts to move independently with increasingly less intervention by the process owners. Processes and functions start to interact with a wider stakeholder community and as a result risks are expressed in operational as well as specialist language.	Information security risks are expressed using a combination of the specialist information security language and risks that reflect the language of the operational processes.	Risk decisions are made in a number of fora.
Stage Four: Information security management processes begin to embed into operational activity.	Information security risk assessment included as part of operational activity.	Security appears as an agenda item in operational fora but the information security risks are those that are directly identifiable as part of operational activity
Stage Five: Role of the embedded activities within the security management system decided.	Risk assessment processes devolved to operational units. Information security risk awareness grows. Risk registers deployed at operational unit level.	The range of risks starts to evolve from the physically related information security risks to risks that are not directly visible to the operation but are perceived as having a direct impact.
Stage Six: Embedded security management processes driving the day to day security management.	Risk registers showing an increased diversification in range of risks.	Embedded security management processes able to identify risks to physical assets, processes and procedures and technology.

Table One: Stages of ISMS maturity related to the development of risk assessment processes

5.1 Organisational Factors

There are a number of organisational factors that disrupt the pattern of developing information security risk assessment from a process that uses one universal set of methods within an information security risk assessment methodology to a set of multiple methods resident within an overall framework of risk assessment. These factors can be categorised as organisational state and organisational culture.

The effect that the organisational state has on decision making was discussed by Bass [2] and Cohen *et al* [4]. Bass concludes that not all decision making follows a standardised decision making cycle of the type described in [13, p. 160]. Bass asserts that there is a complex interaction between organisational factors which result in organisations missing steps or emphasising certain steps but not others. In the case of information security risk assessment, the research concluded that organisational state has a significant influence on how an organisation refines its risk assessment method selection. From the observations of risk assessments being carried out and analysis of the resulting documentation and from the analysis of the interviews with information security managers and risk assessors, it was concluded that organisational state was a factor that affected not only the focus of the risk assessment, but also, the manner in which it was carried out, the methods selected and the negotiation that took place afterwards.

Another important disruption is culture. Drenth [7] makes the point that an organisation has structures and mechanisms that it uses to standardise its management structures but it also has operational processes which determine how that structure is responded to. The manner in which risk assessment is refined, could be characterised as part of this response. Strauss [63] makes the point that there are a number of forms of participation. The dimension of risk assessment which characterises the extent to which the process that deploys the risk assessment methodology is internal or external, is one aspect of participation. Another, important aspect is risk negotiation. There were many models of risk negotiation that were identified as part of this research. Within an ISMS structure there is a well-defined process for risk negotiation, termed risk treatment. Initially an organisation handles information security risk negotiation as an activity external to any other processes.

This research was not able to generalise a pattern of development for risk negotiation, neither was it able to determine the organisational mechanisms which shape the risk negotiation models.

However, some conclusions were drawn on the influence of culture and organisational state. The main factor that determined the risk negotiation approach in the organisations studied was culture, although organisational state did have an influence, particularly in terms of the availability, focus and empowerment of stakeholders.

6. *Conclusion*

In information security management, risk assessment is a process that enables the organisation to learn about its relationship with information security, better understand the nature and structure of its information and calibrate its information security responses to perceived dangers to information and continue to calibrate as the environment changes. As an ISMS becomes absorbed into the organisation, there is a wider deployment of the information security risk assessment process. Organisations naturally start to adapt their use of the risk assessment process and the methods they select to conduct the risk assessment. The difficulty is that part of this evolution can take vital parts of the risk assessment process out of the visibility of the ISMS review processes, in particular the audit process. An ISMS needs to have full visibility of all its risk assessment activity both in order to determine which information security risks are salient and to identify which aspects of information security risk are not visible to the information security risk process. In order to achieve this visibility, the dimensions to an information security risk assessment methodology need to be detected and evaluated as part of the ISMS review processes.

References

- [1] Adams, J.: Cows, Cholera and Cars – The Management of Risk and Uncertainty. In Policy Analysis, No. 335, (1999), p.4
- [2] Bass, B. M.: Decision-making and Organizational Culture. In.: Drenth, P.J.D., Koopman, P.L., Wilpert, B. (eds), Organizational Decision-Making under Different Economic and Political Conditions. (1996) pp. 159-164
- [3] CCTA Risk Analysis and Method Management, <http://www.gammassl.co.uk/topics/hot5.html>
- [4] Cohen, M., D., March, J., G., Olsen, J. P.: A Garbage Can Model of Organizational Choice. In.: Administrative Science Quarterly, vol. 17(1) (1972) pp. 1-25
- [5] Coles-Kemp, L., Overill, R. E.: On the Role of the Facilitator in Information Security Risk Assessment, J Computer Virology 3 (2) 143-148 (2007).
- [6] Coles-Kemp E, The anatomy of an information security management system, PhD Thesis, University of London (2008).
- [7] Drenth, P.: Culture Consequences in organizations. In.: Drenth, P.J.D., Koopman, P.L., Wilpert, B. (eds), Organizational Decision-Making under Different Economic and Political Conditions. (1996) pp. 199-206.
- [8] ISO/IEC 17799: Information technology – Security techniques – Code of practice for information security management. International Standards Organisation (2005)
- [9] ISO/IEC 27001: Information technology - Security techniques - Information security management systems – Requirements. International Standards Organisation (2005)
- [10] McEvoy N, Whitcombe A, G. Davida, Y. Frankel and O.Rees (Eds): Structured Risk Analysis, InfraSec2002, LNCS 2437, (2002) pp. 88-103
- [11] NASA, Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners (2002), pp. 6-17
- [12] Peltier, T.R: Information Security Risk Analysis. Auerbach Publications (2005)
- [13] Sherwood J., Clark A., Lynas D.: Enterprise Security Architecture – A business-driven approach. CMP Books (2005)