J Comput Virol (2007) 3:143–148
DOI 10.1007/s11416-007-0040-6

EICAR 2007 BEST ACADEMIC PAPERS

On the role of the Facilitator in information security risk assessment

Lizzie Coles-Kemp · Richard E. Overill

Received: 12 January 2007 / Accepted: 7 March 2007 / Published online: 28 March 2007

Abstract In organisations where information security has historically been a part of management and for which the risk assessment methodologies have been designed there are established methods for communicating risk. This is the case for example in the banking and military sectors. However in organisations where information security is not embedded into management thinking and where the relationship between information security and the business is less clear-cut, communicating the risks to the business is less straightforward. In such circumstances it has been observed during field research that information security risk assessments frequently output findings to which the business cannot relate and the process is consequently often viewed as a "tick box" exercise, as opposed to one that provides real value to the business. In such a situation the information security risk assessment is divorced from the business process and not embedded into the organisation's processes or thinking. The research for this paper was undertaken in order to identify what needs to be done in order to ensure that businesses of this type find the risk assessment process valuable in practice.

Lizzie Coles-Kemp is a postgraduate research student in Computer Science and Richard E. Overill is a Senior Lecturer in Computer Science.

L. Coles-Kemp · R. E. Overill (✉)
Department of Computer Science,
King's College London,
Strand, London WC2R 2LS, UK
e-mail: richard.overill@kcl.ac.uk

L. Coles-Kemp
e-mail: elizabeth.coles-kemp@kcl.ac.uk

1 Introduction

Risk management lies at the core of information security management. It is the primary means by which an organisation makes decisions about the security controls that it uses [8, p. 4]. The Information Security Management standard ISO 27001 mandates that a formal risk assessment is undertaken in order to build and maintain an information security management system (ISMS). The standard also mandates that the ISMS operate in the overall context of the business and in the context of the business risks as a whole. The standard does not require a particular risk assessment methodology, only that "the risk assessment methodology selected shall ensure that risk assessments produce comparable and reproducible results" [4, p. 4, Clause 4.2.1.c.2]. It is supported by two documents produced by standards bodies, ISO/IEC TR 13335-3 and BS 7799-3, both of which outline in broad detail how a risk assessment methodology should be constructed but which do not address the aspect of communicating the risks to the business.

This does not of course mean that the risk assessment methodologies in use are necessarily incorrect but rather that the communication process between the wider business and the core team undertaking the risk assessment is not working effectively. It is often the case that the risk assessment methodologies in use comply fully with the ISO 27001 requirements and yet the organisation still struggles to demonstrate that the ISMS is being operated in the context of the business objectives and the overall business risks.

During the process of observing organisations as part of ISO 27001 audits, it was noticed that the organisations of this type found certain types of risk assessment process produced output that was easier to absorb. We consider two alternative approaches to information security risk assessment and analyse how easy it is for the output to be used by businesses

where traditionally information security is not a top level management issue. We assert that the role of Risk Facilitator is regarded by few organisations as a requirement for building an ISO 27001 compliant ISMS but yet is a critical success factor for many organisations implementing an ISMS in the context of the overall business process.

2 The criteria

The requirement of ISO 27001 is that it ensures the ISMS be linked directly to the overall business objectives and risks [4, p. 3, clause 4.1]. This mandatory requirement of the standard means that the security risks must at some point be articulated in the context of the organisation, which in turn requires that the language that is used to express the risk assessment output must be presented in such a way that it is clear how the security risks affect the business' overall activities and the risks that it faces. It must also produce findings that are understandable by the business and to do this the process must present a picture of the scope of the risk assessment that is comprehensible and yet not so simplistic that the nature of the risks is not fully apparent.

In organisations where security is highly salient to business operations: such as weapons manufacture, smart card manufacture and banking, information security is a well understood concept and the risk assessment methodologies output findings using terminology that is understood by the business. However in organisations where the drivers for security are primarily legal or regulatory compliance and market positioning, rather than the traditional view of information security expressed in terms of risks to availability, confidentiality and integrity, then the risk assessment findings need further translation. This translation is important not only for understanding but also so that the organisations can embed security into their management thinking.

2.1 Management review

Within an ISO 27001 ISMS the way in which risk assessment findings are reviewed by management is typically in the management review and risk treatment processes. Traditionally risk assessment output is produced as a hierarchy of documents. The top level of the hierarchy is a 'management' summary which is supported by varying levels of assessment detail. The typical risk assessment output hierarchy is delineated by Peltier as part of the description of the Facilitated Risk Analysis and Assessment Process (FRAAP) [7, Sect. 6.4.9, pp. 186–204]. The aspect of the report that is written for the commercial part of the business is usually termed the management summary and the typical presentation for these findings is a brief document, using non-technical descriptions and providing clear explanations of the findings. In organisations that are presented with findings that automatically map to business objectives, this is all that is needed. For organisations where security is less salient for the business objectives, further reflection is required and a degree of reflexivity is needed in order to map the security requirements into the business requirements.

2.2 Comprehensible input

In order to make informed decisions about information security requirements, the business needs to be in possession of a clear picture of the risks to information in the context of the organisation's overall activities and it also needs to understand the relationship between the risks and impact of the different risk treatment options. As organisational relationships become more complicated, so too do the information systems that support them.

There are many types of complexity, including technical complexity, relationship complexity and movement complexity. Just as it is true that static elements usually contribute to a low complexity scenario, highly mobile elements often contribute to a complex scenario [3, p. 108]. The "information explosion" caused by the advent of new technology is identified as one of the contributors to the revolution in commercial activities [3, p. 10]. One of the traditional ways to make a complex problem comprehensible is to reduce it [2, p. 54]. Establishing a framework, of which risk assessment is one such approach, reduces the complexity of an information system by modularising and layering the system. This is an important activity for risk assessment because it enables the assessment team to focus on the relevant issues. However, at some point the interdependencies between the different aspects of the system need to be addressed as the interdependencies affect system behaviour [8, p. 71]. The risks to those interdependencies must therefore be analysed and assessed, just as much as the risks to the individual assets themselves. In an ISO 27001 ISMS this analysis is carried out in part during risk assessment but also in the management review process where the risks are considered in the overall context of the business. As has been identified complexity in this context has many aspects and a role is needed in the risk assessment process to support the business in its efforts to form a consolidated picture of the risk assessment scope and to ensure that the final picture supports the focus of the assessment.

3 Summary of requirements

In order for the business to build the security into the overall risk landscape of the business the management review process has a number of requirements of the risk input that it receives:

1. Risk review must be a business driven process.
2. Risk assessment findings for review must expressed the language of the business.
3. Risk assessment findings must be linked to the organisation's business activities and risks.
4. Risk assessment findings must present a picture that is comprehensible to the business from which decisions can be made.
5. The risk assessment findings need to be conveyed in such a way that they reflect the risks caused by the complexity of the information system, even if it does not reflect the complexity itself.

The fourth and fifth requirements were considered in some depth by [6, pp. 88–103] in order to "ensure that the service and systems under consideration are represented clearly, in a way that is understandable to stakeholders and hopefully in a manner that is consistent with the rest of the organisation." In essence this methodology puts forward the view that not only must the risk assessment process be linked to the overall business context but it must also be configurable so that the assessment components can be adapted to meet the requirements of each part of the business.

The five requirements place demands upon the output from risk assessment rather than upon the risk assessment methodology itself. They should be regarded as additional requirements, designed to ensure that the results are comparable, reproducible, comprehensible and useful to the business.

Observations during security management certification audits indicate that there are two approaches to achieving these five requirements: a Risk Assessor led approach and a Facilitator led approach. The following section examines an example of each.

4 Evaluation of risk assessment methodologies

We now examine two information security risk assessment methodologies, FRAAP and a combination of BS 7799-3:2006 and ISO/IEC TR 13335-3:1998. In each case we consider and compare how they meet the five requirements above and analyse the critical success factors.

4.1 FRAAP—a Facilitator led approach

Peltier's FRAAP is a qualitative risk assessment process where the key feature is that the business drives the risk assessment process and the security analyst acts as a Facilitator. The process is composed of a pre-FRAAP session, FRAAP session and post-FRAAP report generation. The purpose of the pre-FRAAP meeting is to conduct the analysis necessary to prepare the assessment scope, the assessment definitions, the process for prioritising threats and to agree logistics. The pre-FRAAP session identifies FRAAP team members and the assets that need to be formally risk assessed. The asset identification process is derived pre-screening which takes place ahead of the pre-FRAAP meeting. During the FRAAP session itself the threats are identified and the risk level identified by assessing the likelihood of the threat occurring. It is important to note that in this methodology likelihood is regarded as a combination of vulnerability and conventional likelihood. This is because vulnerabilities are not considered until controls have been implemented and the FRAAP is conducted on the assumption that security controls have yet to be implemented. In an extension of the FRAAP the 'residual risk' is also calculated by considering the level of risk once a control has been selected and implemented.

Analysis From the summary of the FRAAP process above a number of conclusions can be drawn with regards to how well the FRAAP meets our business risk requirements.

Risk review must be a business driven process—by introducing the role of Facilitator this risk assessment process automatically avoids some of the more common mistakes of information security risk assessment methodologies. This is a process that clearly has the business at its heart because the stakeholders are required to own and drive the process, all the assessment activities require the involvement of the stakeholders and the output is the result of the assessment of the stakeholders.

Risk assessment findings must use the language of the business—the examples of the post-FRAAP output provided by Peltier demonstrate an interesting finding: none of the outcomes are articulated in the language of the business, all findings are articulated in the traditional language of information security [7, pp. 186–191]. In addition all the definition examples from a pre-FRAAP session are articulated in the traditional information security language [7, pp. 167–171]. However with the appropriate facilitation there is no reason why the language can not be more representative of the business.

Risk assessment findings must be linked to the organisation's business activities and risks—whilst FRAAP has the possibility of linking findings to the organisation's business activities and presenting a picture that is comprehensible to the business, this is very much dependent on the facilitation of the session and the involvement of the stakeholders. Therefore a FRAAP Facilitator needs to have not only facilitation skills but both business and information security analysis knowledge.

Risk assessment findings must present a picture that is comprehensible to the business from which decisions can be made—the degree to which this is possible depends on the involvement of the business in the assessment process, the extent to which the output is linked to the context of the business, the language of the findings and the general overall

quality of the process. While there is nothing in FRAAP which prevents this, there is also little to assist it.

The risk assessment findings need to reflect the risks caused by the complexity of the information system, even if it does not reflect the complexity itself—for this to be possible, the scope definition, likelihood analysis and threat identification needs to be of a high quality, carefully structured and aligned with the requirements of the business. The methodology used to carry out the scope analysis needs to produce output that the business can recognise and therefore the same methodology is not guaranteed to work repeatedly for different organisations.

Whilst FRAAP does not provide a detailed risk assessment methodology, it does provide a framework for showing how a Facilitator led process can produce findings that are more easily comprehensible by a business not used to information security. Organisations are increasingly organic in their structure and therefore require more complex problem solving and problem management methodologies, of which risk assessment is one such methodology. A more complex methodology requires greater support from the Facilitator. Whilst the business must articulate the scope, the assets, and perform the threat and vulnerability analysis, it is the Facilitator who must guide the organisation by helping the organisation to select the most appropriate methodology at each stage in the assessment and then by supporting the organisation in using the methodology to articulate the different aspects of risk. Furthermore the Facilitator can be used to help communicate the risk message to the wider business community.

Therefore whilst the Facilitator led approach supports the business and produces output the business will understand, the approach must be supported by a technically appropriate risk assessment methodology.

4.2 ISO/IEC 13335—an Assessor led approach

ISO/IEC 13335 is divided into four different parts, where the first part identifies the overall process and shows the different components necessary to complete a risk assessment. ISO/IEC 13335-1:2004 identifies the overall process for managing information and communications technology security. In this part of the standard the fundamental security concepts are explained, next the policy and strategy principles are explained, followed by a description of the necessary organisational structure for implementing security and finally the management function and in particular the process of risk management is explained. This section of the standard is useful because it defines the principles which underpin an information security framework and explains in more detail the structures which support the framework.

ISO/IEC TR 13335-3 is a technical report which provides guidance on implementing a risk assessment, together with a range of possible risk calculation models. ISO/IEC TR 13335-4 identifies the countermeasures that can be used to control the identified risks.

ISO/IEC TR 13335-3 identifies four approaches to risk analysis ranging from the baseline approach to the detailed risk assessment methodology. Section 9.3.3 of ISO/IEC TR 13335-3 identifies the process flow of risk assessment is as follows:

- Identification of assets to be included in the risk assessment
- Valuation of assets and establishment of dependencies between assets
- Threat and vulnerability assessment on the assets within the scope of the risk assessment
- Identification of existing or planned safeguards
- Assessment of risks

BS 7799-3:2006 provides a similar framework but spends more time on the assessment process. In the description of the assessment process roles and responsibilities are defined and the processes for risk treatment and management of residual risks are specified. In this standard the risk assessment is performed by the Risk Assessor, who, unlike the organisation supported by the Facilitator in FRAAP, actually performs the risk assessment.

Analysis A number of conclusions can be drawn in relation to the business requirements that were defined earlier in this paper.

Unlike FRAAP, this risk assessment methodology is documented as a standard and in the standard documentation there is little example output and little in the way of guidance notes for implementation. The first three requirements require risk to be articulated in the context of the business. If BS 7799-3:2006 is taken to be the risk framework and ISO/IEC TR 13335-3 is taken to be as a specification of the assessment methodology, then there is the possibility that these requirements might be fulfilled. However it is entirely dependent on the role of the Risk Assessor which is defined in BS 7799-3:2006. If the Risk Assessor is able to conduct the analysis in the context of the business, then the first three requirements might be met. It should be noted that the standard states that the Risk Assessor must have some business awareness and understanding [1, sect. 5.8, pp .15–16]. Whilst BS 7799-3:2006 specifies that risk assessment should be conducted in the context of the business, there is no guidance as to how this should be achieved and no specification of ownership in the assessment process, a feature which was dominant in FRAAP. It could be argued therefore that the methodology is very weak in this area and open to misinterpretation, such that the Risk Assessor could be regarded as the owner of the risk assessment process. If this happens then the business is likely to become a passive partner in the assessment

process, merely supplying information rather than constructing information.

The last two requirements refer to the picture that is presented to the business. *Risk assessment findings must present a picture that is comprehensible to the business from which decisions can be made, the risk assessment findings need to reflect the risks caused by the complexity of the information system, even if it does not reflect the complexity itself.* There is nothing in either standard that automatically results in assessment output that is aligned with the business context. The fulfilment of this requirement is solely in the hands of the Risk Assessor and its interpretation as to how the risk input and output should be constructed.

This methodology is strongest in its introduction of a multi-methodology for risk calculation. ISO/IEC TR 13335-3 introduces the idea of different calculations, depending on the aspect of risk that is to be calculated. Therefore the methodology is focused on the technicalities of risk assessment, rather than the method for conducting an assessment and communicating the findings. Of course the effectiveness of the calculations is entirely dependent on the robustness of the rest of the methodology. Therefore whilst this latter methodology gives the Risk Assessor better tools to work with in terms of producing calculations, without a facilitated process to perform the threat and vulnerability analysis, the calculations are potentially useless to the business.

5 The need for a skilled Risk Facilitator

The two risk assessment approaches that have been discussed in this paper are typical of information security risk assessment methodologies. It is clear that the methodologies presented in this paper are capable of producing output that meets our five requirements. However it is the role of Facilitator that makes this more likely and yet neither ISO 27001 nor its supporting risk guidance documents, BS 7799-3 and ISO TR 13335-3, mention such a role. As a result, many businesses for which information security is not highly salient to the organisation's culture or the nature of their business use risk assessment methodologies that are conformant to the standard but are nevertheless unable to produce risk assessment findings that they can recognise.

It is noticeable that the methodologies reviewed here spend remarkably little time discussing the approach for analysing assets and scope. All the methodologies require that this activity is undertaken but given the fact that the risk assessment fails if this step is incomplete, it is surprising that so little guidance is given on this step in any of the methodologies. Asset and scope identification can be complicated because in order to capture the essence of the information system and its business use, a methodology needs to be developed for defining risk assessment scopes and the attributes of the assets within them. Complex systems have a number of properties: aggregation, non-linearity, flows and diversity [2, pp. 13–21]. It takes considerable skill to identify information assets with these properties and as a result they are often identified as static elements with fixed values and ownership instead; if a change in these properties is to be captured then another static picture must be taken of the asset and a new set of values must be assigned. These aspects of information flow cannot be identified by an external assessor or by any one individual. It requires both internal and external knowledge of how the system works, the business context in which the system operates, and the value of the information as it flows through the business process. A Facilitator is needed to bring together all these views and to ensure that they are presented in a balanced and coherent form.

Metaphors may be regarded as a way of tagging information in complex systems [2, Chap. 5] and may be viewed as a means of simplifying complex systems. Typical risk assessment metaphors are numbers, words reflecting impact and static colour, which are one dimensional, rather like a palette of distinct colours. The skilled Facilitator has to be able to select the appropriate metaphor for the business and be able to consider non-traditional metaphors if necessary. For example, it is possible that in certain situations by using continuous colour, which reflects the spectrum of risk, some of the complexity of the scope can be preserved in the risk assessment process, without making the assessment harder to understand.

The role of Facilitator is not a new one in information security risk assessment methodology. Not only is it a role presented by Peltier in FRAAP but Kleckner has also outlined the need for a Facilitator in an information security risk assessment. Unlike the definition of the role in FRAAP, Kleckner's description of the role requires a knowledge of the different aspects of information security [5], whereas FRAAP requires general facilitation skills. We argue that a combination of both skill sets is necessary. In addition, we contend that the Facilitator requires a knowledge of information systems and business process modelling, a range of tools and methodologies for presenting and analysing complex problems, translation skills between the different layers of the risk hierarchy, an educationalist's approach to risk assessment, and a detailed knowledge of the mechanics of risk assessment.

6 Observations

Over the course of 5 years, ten companies were observed during a 3 year period. All of these organisations are introducing formal security management processes for the first time and none of these organisations include information security as part of their business objectives. In each case information

security is considered by some as an operational risk but not considered as an aspect of the main business risks and in each case the driver for implementing a form of formal information security management is either contractual requirements or marketing requirements. All of these organisations provide a service, rather than product manufacture. The services are predominantly outsourced IT services, although some small-scale logistics services and professional advisory services are also provided by some of the organisations. The size of organisation varies considerably but in each case the size is less than 500 employees.

In all cases the initial risk assessment that was performed was an Assessor-led risk assessment. In each case the risk assessment focused on the IT assets and the information that supported these assets. In each case in the initial assessments there was no assessment of the business processes that were impacted by the risks. In the majority of cases the Assessor was an external resource and initially the interaction with the business was minimal in each case. The business responded to questions that were asked of it and reviewed the risks as they were presented. However in each case the risks were not related to the overall business objectives, nor to the main risks that the business faced at that time. The risks were expressed in terms of impact to confidentiality, integrity and availability and it was left to the business to link the security risks to the business risks but without the tools to do so. In each case the ISO 27001 requirement to link the ISMS with the overall business context coupled with requirement to demonstrate the effectiveness of the ISMS and its controls, changed the nature of the risk communication in that the business was forced to articulate its requirements for information security and specify how it expected to verify that its requirements had been met. These requirements in themselves did not change the risk assessment methodology used but did change the way in which the risks were discussed and reviewed. However in over half the cases the risk assessment methodology was changed, mainly to make the reporting of risks easier for the business to understand and so that business process risk could be included in the assessment. In each case an element of facilitation had to be introduced into the risk communication process in order that the risks were fully understood by the business but also so that the business could translate these risks into the context of the business objectives.

In each case facilitation led to a re-articulation of the security risks in the context overall business risks. The facilitation also led to the development of a metrology framework against which the effectiveness of security management and its controls could be measured and verified against business objectives. The inclusion of a facilitated risk communication had a number of additional benefits. Fifty percentage of the businesses reported an improvement in the effectiveness and the efficiency of their business processes that they directly attributed to the implementation of a security management and in most cases this was reflected back into the security risk assessment. The result in these cases was that the terminology of the risk assessment gradually began to change and reflected the risks not only to the IT assets but also to the business processes. In each case a member of the business rather than the IT community, led the facilitation process, although in the majority of cases there was support by the IT or technical manager. Where the risk communication was improved and the facilitation role was successful, information security management was embedded into the business process and into business thinking. Security did not necessarily become more salient to business requirements but it did become a more automatic part of the business culture.

7 Conclusion

Whilst traditional risk assessment methodologies, which were developed to tackle computer security problems in the 1970s, are still needed today they are not by themselves sufficient for addressing today's dynamic corporate information security management issues as they impact on the entire business process. The role of Risk Facilitator as prescribed in this paper is aimed at remedying the manifest deficiencies of traditional risk assessment communication experienced by certain types of organisation by introducing a degree of reflexivity and opening effective channels of communication between all the stakeholders involved in the business process.

References

1. BS 7799-3: British Standards Institute (2006)
2. Czerwinski, T.: Coping with the Bounds: CCRP (1998)
3. Daellenbach, H.G., McNickle, D.C.: Management Science—Decision Making Through Systems Thinking. Palgrave MacMillan (2005)
4. ISO/IEC 27001: International Standards Organisation (2005)
5. Kleckner, M.: Facilitating the Qualitative Security Assessment: Overview of the Process of Defining and Delivering Security Requirements for Application Systems. SANS Institute (2001)
6. McEvoy, N., Whitcombe, A.: Structured risk analysis. In: Davida, G., Frankel, Y., Rees O. (eds.) InfraSec2002, LNCS 2437. Springer, Heidelberg (2003)
7. Peltier, T.R.: Information Security Risk Analysis, 2nd edn. Auerbach Publications (2005)
8. Sherwood, J., Clark, A., Lynas, D.: Enterprise Security Architecture—a Business-driven Approach. CMP Books (2006)