Edith Cowan University
Research Online

Australian Information Security Management Conference

Security Research Institute Conferences

2006

The Information Security Ownership Question in ISO/IEC 27001 – an Implementation

Lizzie Coles-Kemp
King's College London - University of London

Richard E. Overill
King's College London - University of London

Originally published in the Proceedings of 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 5th December, 2006
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/65

The Information Security Ownership Question in ISO/IEC 27001 – an Implementation Perspective

Lizzie Coles-Kemp and Richard E. Overill
Department of Computer Science, King's College London, University of London, Strand, London WC2R 2LS, UK
elizabeth.coles-kemp@kcl.ac.uk, richard.overill@kcl.ac.uk

Abstract

The information security management standard ISO/IEC 27001 is built on the notion that information security is driven by risk assessment and risk treatment. Fundamental to the success of risk assessment and treatment is the decision making process that takes risk assessment output and assigns decisions to this output in terms of risk treatment actions. It is argued that the effectiveness of the management system lies in its ability to make effective, easy-to-implement and measurable decisions. One of the key issues in decision making is ownership. In this paper two aspects of information security ownership are considered: ownership of the asset (as per the ISO/IEC 27001 definition) and ownership of the risk treatment actions. This paper discuses how traditional information security risk assessment methodologies confuse the ownership issue and raises the question as to whether this is simply because they are re-badged computer security risk assessment methodologies or because the significance and the complexity of ownership is underestimated in many forms of information security risk assessment. This paper also presents some observations from practical attempts at implementing an organisation-wide information security risk assessment methodology. The observations were made as part of ISO/IEC 27001 certification assessment visits.

Keywords

Asset ownership, ISO/IEC 27001, information security management system, information flow modelling, risk assessment, decision making, risk treatment, super scope

INTRODUCTION

Curiously when designing and implementing an information security management system (ISMS) there is often very little emphasis on the ownership of information security. This is perhaps because it is a difficult issue to identify within an organisation because to resolve it requires an articulation of the importance, or otherwise, of information security. It is a trend that is both surprising and concerning because of the importance of ownership when assigning roles and responsibilities for security issues. Dhillon introduced the concept of responsibility structures and their work demonstrates the importance of identifying responsibility structures as a way of reducing security problems by improving communication within and understanding of the organisational context. (Dhillon 2006a)

The rise of the 'super scope' has compounded this lack of ownership modelling and lies at the root cause of many of the problems identified by ISO/IEC 27001 assessors during routine audit visits. In particular the failure to clearly identify ownership bedevils risk treatment activities and makes the decision making process within the security forum slow and ineffective. The security forum is the way ISO/IEC 27001 defines the opportunity for making security decisions. The 'super scope' brings this problem sharply into focus because whilst the traditional ISMS scope is relatively simple in terms of organisational hierarchy, the number of processes it addresses and the organisational boundaries that it traverses, the 'super scope' typically covers an entire organisation and the ownership question is therefore much more complex.

Clear Security Ownership – a Necessity for Effective Risk Management

ISO/IEC 27001 requires that the information security management system (ISMS) is assessed for its effectiveness: "Undertake regular reviews of the effectiveness of the ISMS (including meeting ISMS policy and

objectives, and review of security controls) taking into account results from security audits, incidents, results from effectiveness measurements, suggestions and feedback from interested parties" (2005a). Interestingly this clause in ISO/IEC 27001 does not directly mention the effectiveness of the risk assessment and treatment processes and yet given the dependency that the system has on the risk management process, it is essential that the risk assessment and treatment processes are effective for the rest of the management system to reach its objectives. In the next clause there is reference to the effectiveness of risk assessment but only in terms of the effectiveness of the implemented controls and the effectiveness of the decision making and sense making processes are not discussed. For the risk assessment to result in effective risk treatment, the security ownership of issues and assets must be clearly defined during the analysis or sense making part of this process. Interestingly the requirement for ownership is not established at this point.

The question then becomes "what does the term security ownership mean?" Perhaps one of the most significant changes between BS 7799-2 and ISO/IEC 27001 is the slight modification to clause 4.1. BS 7799-2 states "The organisation shall develop, implement, maintain and continually improve a documented ISMS within the context of the organisation's overall business activities and risk" (2002) whereas ISO/IEC 27001 states "The organisation has established, implemented, operates, monitors, reviews, maintains and improves a documented ISMS within the context of the organisation's overall business activities and the risks it faces." (2005b). This view is not new and is one that is often presented in information security management. It was recently cited by Dhillon as one of a set of principles designed to help analyse secure environments "A well conceived corporate plan establishes a basis for developing a security vision" (Dhillon 2006b). However it is the first time that such views have been so strongly emphasised within an information security standard. The change to clause 4.1 can be interpreted as a strengthening of the link between the ISMS and the business, making it more difficult for organisations to disassociate the information security processes from the business objectives and the risks that the business faces. It could be argued that this clause gives ISO/IEC 27001 certification assessors the mandate to test the link between the business and the ISMS where the one clear place that the ISMS will link with the business is at the risk assessment level and therefore through the business ownership of security.

The Placement of Risk and the Significance of Security Ownership

If risk assessment is to be used as one of the primary means of linking the business context to the ISMS then the role of risk management in the wider organisational context must be understood.

There are a number of ways in which the role of risk assessment and treatment can be perceived but in the wider risk context, risk management can be seen as a combination of sense making and decision making. Sense making can be quite literally described as the process of "making sense" and best explained with the question: "How can I know what I think until I see what I say?" (Wallas 1926) This makes the case that assembling one's thoughts on a given topic can, depending on the topic's complexity, require an element of externalisation and review before a view on that topic can be fully formed. One of the ways in which risk assessment externalises the scope of the assessment is to identify the assets within the scope and assign security owners to those assets. In order for the risk management process to be successful it is essential that the security owners of the assets have been identified because it is through the identification of ownership that risk treatment action owners can be identified.

The decision making aspect of risk management is primarily found in the risk treatment discussions. A decision can be described as being composed of choice, opportunity, problems, solutions and participants (Cohen et al 1974) and the decision making process itself can be described as "making a choice from the various courses of action open to the decision maker" (McKenna 2006). Viewing risk management as an aspect of decision making is one way to start to understand the all-encompassing nature of the process and the fundamental role that security ownership has to many of the decisions that business faces. This view is further reinforced if the traditional picture of the ISMS is restructured to fully reflect the central role of risk management as part of the decision making process.

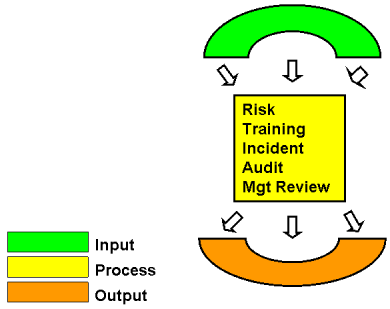

Figure 1 – The traditional view of the ISMS

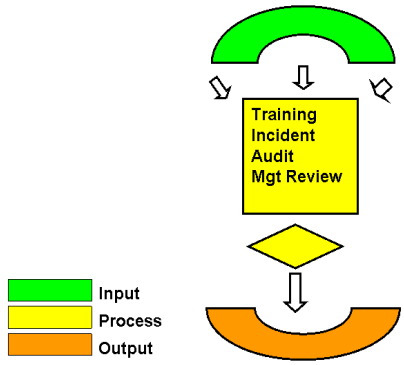

Figure 2 – Placing risk assessment and treatment as part of the decision making phase

By explaining the flow of the ISMS in this way the reality of how organisational risk assessment and treatment takes place in many aspects of organisational life is more accurately demonstrated and illustrates the fact that the effectiveness of the information security management system in large part hangs on the effectiveness of the risk management processes as part of its decision making. If risk management actions are without clear ownership then the risk management actions can not be effective. This is not a novel view, in the risk mitigation process that is defined in NIST SP 800-30 (2002), the assignation of responsibilities is a specific step within the process. Dhillon (2006c) re-enforces this view by identifying the need for ownership in a number of the stages within the risk assessment process. However in practical terms this requirement becomes more salient when the effectiveness of the ISMS is part of the assessor's scope of enquiry.

THE ROLE OF SECURITY OWNERSHIP WITHIN TRADITIONAL INFORMATION SECURITY RISK ASSESSMENT

There are many information security risk assessment methodologies and in many of these methodologies the issue of ownership appears to be marginalised. In this section the extent is assessed to which ownership is addressed within both a typical computer security approach and a typical business focussed approach to risk assessment.

Standard Approaches to Information Security Risk Assessment

The most traditional of the risk assessment methodologies is the one described in ISO/IEC TR 13335-3 and this traditional risk assessment process has a number of phases:

Figure 2 in section 9.3.3 of ISO/IEC TR 13335-3 (1998) identifies the process flow of risk assessment as follows:

1. Identification of assets to be included in the risk assessment
2. Valuation of assets and establishment of dependencies between assets
3. Threat and vulnerability assessment on the assets within the scope of the risk assessment
4. Identification of existing or planned safeguards
5. Assessment of risks

This description provides the traditional computer security view of the risk assessment process and it is intended that the ownership is identified as part of the asset identification but no discussion or guidance on this topic is evident within the document.

The ISO/IEC TR 13335-3 approach compares with the following, more business-orientated approach, from Sherwood Applied Business Security Architecture (SABSA) where the steps in a commercial information security risk assessment are summarised in six steps by Sherwood et al (2006):

1. Identify and value the assets
2. Identify the possible threats
3. Identify and quantify these impacts by relating back to your asset list
4. Identify and quantify these vulnerabilities or weaknesses
5. Identify the possible control strategies and quantify the cost (total cost of ownership) for these controls
6. Quantify the benefits and the costs

Again the issue of ownership is marginalised and links ownership with cost of controls and yet there are two aspects of ownership to be considered: ownership of the asset and ownership of the control to treat the risk. Total cost of ownership implies a combination of both types of ownership.

In order to comply with ISO/IEC 27001 both the assets within the scope of the ISMS and the owners of those assets have to be identified (2005c). Owners are defined in ISO/IEC 27001 as “the term “owner” identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term “owner” does not mean that the person actually has property rights to the asset.” (2005d) The distinction that ISO/IEC 27001 is drawing here is an important one: the ownership of the security management aspects of an asset as opposed to ownership in terms of rights to the asset. In traditional risk analysis terms this ownership is often seen as ownership at the data set level. This is further supported by ISO 17799 which includes in control 7.12 the requirement that the ownership of assets is identified. The control states “All information and assets associated with information processing facilities should be owned by a designated part of the organisation” (2005e). The clause goes on to provide the following implementation guidance: “the asset owner should be responsible for:

- ensuring the information and assets associated with information processing facilities are appropriately classified;
- defining and periodically reviewing access restrictions and classifications, taking into account applicable access control policies.

Ownership may be allocated to:

- a business process;

- a defined set of activities;
- an application; or
- a defined set of data”

Therefore in order for the information security management system to ensure that corrective and preventive action instructions are effectively implemented, the asset identification and ownership which sits at the heart of the modelling phase of the risk assessment process must be accurate and appropriate and this must be translated into identification of owners for risk treatment action items.

Marrying the ISO 27001 Requirements with Traditional Risk Methodologies

As has already been seen, remarkably little is documented about asset identification and security ownership in information security risk assessment methodologies. This may be due to the fact that the majority of information security risk assessment methodologies are in fact largely computer security risk assessment methodologies which belong to era when assets were relatively static, easy to identify and security ownership was in large part linked to the ownership of the physical asset. In addition the use of the term “asset” is synonymous with the financial asset register and an organisation often sees its assets in terms of physical assets, software assets and information assets. A risk assessment methodology such as CRAMM (UK Government's Risk Analysis and Management Method) (2006) will try and collate those assets as a support structure for a particular “service “ where service may be a business or, more typically, a technical service. The difficulty with this “bottom up” approach is that the security ownership is ill-defined because it is unclear as to how ownership of security issues is to be assigned from within the business. For example: should they be assigned to the process or to the assets supporting the process? By trying to model assets in this way it becomes clear that security ownership is not solely a product of the sense making process but is also a product of the decision making process because in an asset model that is composed of multiple assets a method of assigning ownership for security issues is required and this is an activity that logically resides within the decision making portion of the overall risk management process. Clarity of ownership becomes critical as the scope of an ISMS increases in complexity. Small, simple, homogeneous scopes can rely on informal methods of assigning ownership but once the scope becomes complex and heterogeneous and a clear understanding of ownership is essential for the scope to be maintained.

The Rise of the Super Scope and its Implications for Security Ownership

Traditionally a certification scope to ISO/IEC 27001 (BS 7799-2) has been small, homogeneous with a relatively flat decision-making structure. In many cases the extent of the scope has been a single department, for example HR or IT, a single office with one prime organisational unit or a business function contained within a single organisational unit. In this type of scope a traditional computer security risk assessment asset model works relatively well. The number of information assets is relatively small and the security ownership is often aligned to the IT infrastructure. It is relatively easy for the decision making process to assign ownership in this case as the decision making hierarchy is relatively flat and ownership travels across few organisational unit boundaries, if any.

However this ‘pillar’ model of asset ownership does not scale to the more complex ISMS scopes. These scopes are in many ways ‘super scopes’ and have the following characteristics: complex decision making hierarchies, the risk assessment of process which crosses multiple organisational units and scopes which have a high saliency for the business objectives of an organisation. It is noticeable that a super scope may not be a large scope but it does have increased organisational complexity in comparison with its smaller, business unit-centric cousin. The complexity of the scope means that security ownership is no longer so clear-cut and the sense making and decision making processes need to be modified in order to accommodate this change.

Modifying the Sense Making Process for the Super Scope

One asset definition model that appears to fit the super scope rather well is one that is reminiscent of the seven-layer TCP/IP model and to the CRAMM asset model but it allows for both general and process-specific models to be built. It is a four-tiered model, constructed as follows in descending order:

- Business process layer
- Application layer
- Network layer
- Infrastructure layer

This is a business approach which enables the risk assessment to directly link to the business aims and objectives. It is a multi owner model where the different layers may have different security owners. The order of precedence in terms of ownership between the layers and the assignment of security issues is identified as part of the decision making process. In many ways this model is aligned with the information system security classes presented by Dhillon where the three classes of strategic, administrative and operational are presented as a way of identifying types of decisions which belong to different aspects of the business. In such a model Dhillon points out that there is often a degree of overlap between the layers. (Dhillon 2006d) This is equally true of the four-layer model proposed here where ownership of security issues has to be negotiated.

Modifying the Decision Making Process of the Super Scope

As has already been identified, in order to make effective risk treatment decisions the ownership of security issues needs to be clearly defined. Perhaps the most common place for this to take place is in the decision making opportunity entitled the “security forum”. This is a vehicle which is identified by ISO/IEC 17799:2005 as an opportunity for the discussion of security issues with the relevant parties.

In a multi-owner model a possible approach is to define a facilitator role as part of the risk treatment process and which uses the security forum to support the relevant stakeholders in the risk assessment to identify risk treatment actions and as part of that role ensures that ownership is assigned. The security forum need not necessarily include stakeholders from one organisation only. There are numerous implementation examples where a security forum includes parties from multiple organisations and at this point a facilitator to help assign ownership becomes even more significant.

The role of a facilitator is not a new one in information security risk assessment methodology. The prime example of the risk management process that uses a facilitator is FRAAP - the Facilitated Risk Analysis and Assessment Process (FRAAP) (2005). The process was designed by Peltier and 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. In this approach the facilitator is present in both the risk assessment and treatment processes. Peltier is not the only analyst to point out the need for a facilitator. 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 knowledge of the different aspects of information security (Kleckner 2001), whereas FRAAP requires general facilitation skills. It is argued that both aspects are required and as part of the role the facilitator must also help the organisation to assign security issue ownership with in the decision making process.

IMPLEMENTATION OBSERVATIONS

Super scopes appear to be on the increase and one of the major impacts of the complexity associated with such scopes is the resulting complexity in the information security management processes. The processes that are most strongly impacted are those involving risk management. A super scope requires a more complex decision making process which in turn implies a more complicated structure for decision making. It also requires a more complex risk assessment process which in order to be appropriate for the organisation typically needs to be a

multi-methodology so that the appropriate type of assessment takes place at the appropriate layer within the organisation. Another aspect of the super scope which needs to be carefully thought out is that of asset inventories and the assignment of ownership. Observations from the field show that many super scopes still adopt a computer asset approach to identifying assets and this results in problems, not only within the risk assessment process itself, but the degree to which the risk management process can demonstrate itself to be effective.

The following are three examples of observed approaches to asset identification and ownership. All examples were observed in super scopes.

One-tiered Asset List with Business Ownership

In this example the asset list is IS-focused and the asset list is divided into a list of information systems that are regarded as essential to the business. There are two lists, a top twenty and a top fifty list of assets. Business owners are assigned to each asset and the asset is valued by identifying the impact of loss of that asset to the business. A two tier system of risk assessment is carried out. Firstly a high-level risk assessment is performed and then a more technical risk assessment at project level is completed. Risk treatment decisions are made at specially convened meetings where information security analysts act as facilitators. Ownership for risk treatment actions is assigned to the asset owner, although the asset owner may choose to delegate the risk treatment action.

The effectiveness of the decision making process appears weak in this model. The business owners appear unwilling to make risk treatment decisions and the most frequent decision is that of risk acceptance. The attendance of business owners at these meetings is also fairly low and erratic resulting in a relatively low rate of decision making indicating that they do not see the risk treatment process as one that is of a high priority. Given that in a super scope these assets are essential to the business, this finding is surprising and raises questions about how far the risk management processes have been integrated into the business.

The risk assessment findings do not seem to identify any significant risks and yet in a super scope it would be expected that at least some aspect of critical assets were at risk, even if this was a risk to be accepted. This leads to questions about the quality of the assessment itself and whether the correct inputs are being included in the initial analysis. One of the key inputs into the risk assessment process is the asset list and ownership assignment.

Maintaining a centralised asset list seems to prove difficult in super scopes and the frequency with which asset lists are reviewed seems to decrease over the certificate lifecycle. In addition the accuracy of the list is also questionable as ownership change is not captured. It becomes clear that in order to manage the asset inventory and the ownership mappings a number of processes must include the maintenance as part of their remit, including change control, management review and internal audit.

One-tiered Asset Ownership with Centralised Ownership

In this example the asset ownership and therefore the security issues are owned by a centralised information systems function. The security ownership of all issues associated with the information sits with this central function and controls to address the issues are decided centrally. In this model there is no business ownership. The asset ownership model follows the traditional hardware, software, information asset listings. The risk assessment which accompanies it is a traditional information security risk assessment that considers the impacts on confidentiality, integrity and availability to each of the assets listed and is closely aligned to computer security risk assessment methodologies.

Whilst the decision making process is relatively fast in this model, the effectiveness of the decisions is erratic. It relies on the co-operation of the business that uses the assets and this is not always obtained in this model. Areas where the central information systems function can not make decisions, is largely ignored in this process, leaving areas of risk decision making uncontrolled and erratic. There is also a tendency to select technical controls and not consider other control types, including: training and awareness, policy controls or locally administered technical controls. This does not necessarily result in the most effective risk treatment decisions being made each time.

The risk assessment output from this type of model has the feel of a computer security risk assessment and has little resemblance to the way in which the business perceives its involvement in security issues and security management. It is particularly noticeable that the risk assessment output in this type of model contains no mention of assets once they leave the centralised IS structure and attempts are made by security managers to deem such instances of assets "out of scope". This particularly applies to information assets as they are moved on to memory stick or use non-digital communication.

It is also difficult from such risk assessment output to re-construct the business involvement in the security issues, even though the business was typically used to generate the findings in the first place. This makes it very difficult to trace business ownership or even obtain business buy-in for subsequent risk treatment proposals.

Asset list maintenance in this type of model is relatively easy but at the expense of ignoring the more volatile, mobile data assets. The asset list is very IS focused and does not have much bearing on the business use of the assets.

Multi-tiered Asset Ownership with Transversal Process Ownership

The multi-tiered asset ownership is perhaps the model that super scopes are most likely to gravitate to because the model proves the most effective way to embed security ownership into the organisation. The asset model is based on the business process which runs transversally across the organisation. The business processes are tiered and the security management processes are embedded within each tier. There are several tiers of ownership: business ownership which owns the process end to end and functional ownership which own the components that support the process. Often the component ownership is maintained by pillar functions within the organisation. Security issue ownership is achieved through the various security fora by assigning ownership of issues to process owners who may delegate the risk to "risk custodians", who is often the functional owner supporting an aspect of the process. A risk might be treated at the process, application, network or physical asset layer and a decision is made in the security forum as to the best course of action.

There are two possible sources of conflict in this model: a conflict between the process owner and a potential risk custodian who does not wish to assume such a role, and a conflict between process owners where a change desired by one process owner conflicts with the functionality desired by another process owner. In each instance a security forum facilitator tries mediate locally. If the local mediation fails, the issue is escalated to another forum.

It is noticeable that this model has also scaled across organisational boundaries and been used in the management of third party services where information is shared between parties. In this type of model decision making is often faster, the types of solutions that are selected, more diverse and it produces an output that is more likely to engage the business. Asset lists are maintained as part of standard business process maintenance and can be modified to scale across organisational boundaries.

CONCLUSION

ISO/IEC 27001 assessors must take the issue of security issue ownership modelling into account when they assess an ISMS because the effectiveness of the information security management processes are completely dependent on this model as it is the mechanism through the which the business engages with security and assumes security as part of its day to day operation. This requirement entails that there must be much better models of asset definition and of decision making within information security risk processes that are capable of effective implementation within complex scopes and that are enshrined as part of the guidance that supports the ISMS standard.

REFERENCES

British Standards Institute, (2002), BS 7799-2:2002, clause 4.1.

Cohen et al, (1974), A Garbage Can Model of Organisational Choice, *Organisational Science Quarterly*, 2.

CRAMM (UK Government's Risk Analysis and Management Method), 2006, http://www.cramm.com/ (last accessed November 2006)

Dhillon, G. (2006a), Information Systems Security – Text and Cases, Wiley, 100.

Dhillon, G. (2006b), Information Systems Security – Text and Cases, Wiley, 126.

Dhillon, G. (2006c), Information Systems Security – Text and Cases, Wiley, 158-169.

Dhillon, G. (2006d), Information Systems Security – Text and Cases, Wiley, 114-121.

International Standards Organisation, (2005a), ISO/IEC 27001:2005, clause 4.2.3.b.

International Standards Organisation, (2005b), ISO/IEC 27001:2005, clause 4.1.

International Standards Organisation, (2005c), ISO/IEC 27001:2005, clause 4.2.1.d.1.

International Standards Organisation, (2005d), ISO/IEC 27001:2005, p. 4, fn 2.

International Standards Organisation, (2005e), ISO/IEC 17799:2005, clause 7.1.2.

International Standards Organisation, (1998) , ISO/IEC TR 13335-3:1998, fig. 2, sect 9.3.3

Kleckner, M. (2001), SANS Institute, 'Facilitating the Qualitative Security Assessment: Overview of the Process of Defining and Delivering Security Requirements for Application Systems'.

McKenna, E. (2006) , Business Psychology and Organisational Behaviour, Psychology Press, 227-262.

National Institute of. Standards and Technology (2002), "Risk Management Guide for. Information Technology Systems", http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (last accessed November 2006)

Peltier, T. (2005), Information Security Risk Analysis, Auerbach Publications

Sherwood, J. Clark, A. Lynas, D. (2006), Enterprise Security Architecture – A business-driven approach, CMP Books, 190.

Wallas, G. (1926),The Art of Thought, Harcourt Brace.

COPYRIGHT

Lizzie Coles-Kemp, Richard E. Overill ©2006. The author/s assign SCISSEC & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SCISSEC & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors