Information Security Measurement Roles and Responsibilities

Margareth Stoll and Ruth Breu

Abstract An adequate information security management system (ISMS) to minimize business risks and maximize return on investments and business opportunities is recognized always more as key differentiator. Thus legal compliance, commercial image and competitive edge are sustainable maintained. Due to increasingly faster changing information security (IS) requirements (from market, customer, technology, law or regulations) the effectiveness and performance of the ISMS must be continually evaluated and improved. Data must be recorded, analyzed and if necessary appropriate corrective or preventive actions should be taken. For these measurement and improvement tasks we have to assign roles and responsibilities. Firstly we define different roles and their tasks for information security (IS) measurement and improvement. Starting from the approved organizational structure we assign the responsibilities for these roles to top and executive management. After we elaborate and document all relevant business processes with their supporting IT services and go on through all technical layers describing the relevant items with their dependencies and relationships. To entire processes, services and items are assigned responsibilities for the defined roles systematically, consistently and traceably. This innovative, systemic, strategic aligned approach has been implemented successfully by different medium sized organizations for several years. Based on our experiences IS awareness, IT alignment with business goals, service orientation, process and systems thinking, as well as the comprehension for the requirements of other organizational units were increased.

M. Stoll (✉) · R. Breu
University of Innsbruck, Technikerstr.
21a, 6020 Innsbruck, Tyrol, Austria
e-mail: margareth.stoll@uibk.ac.at

R. Breu
e-mail: ruth.breu@uibk.ac.at

T. Sobh and K. Elleithy (eds.), *Emerging Trends in Computing, Informatics, Systems Sciences, and Engineering*, Lecture Notes in Electrical Engineering 151,
DOI: 10.1007/978-1-4614-3558-7_2,

1 Introduction

1.1 Starting Situation

Due to globalization and ever stronger competition information management and supporting technologies have become key assets and differentiators for modern organizations. They are main performance driver for continual innovation and sustainable success. Organizations and their information and technologies are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Causes of damage have become more common, further ambitious, and increasingly sophisticated [1]. 92 % of large enterprises had a security incident in the last year with an average cost of 280.000–690.000£ for the worst incident [2]. Mobile and cloud computing, off-shoring, social networks, as well as the increasing interconnected, flexible and virtualized business complexity and dependency are still great challenges for IS.

Organizations have to meet many different legal and regulatory requirements, such as data protection, sound and integer financial practices and internet crime. Most modern corporate governance guidelines, and always more laws, make the top management responsible for the well-being of the organization. Lack of security compliance may result in loss of confidence of customers, partners and shareholders, as well as severe civil and criminal penalties for the top management. In this respect availability of the essential assets, confidentiality, data integrity and legal and regulatory compliance are central for organizations' success and integral part of good IT and corporate governance [3–5].

More than 6,600 organizations worldwide [6] have implemented ISMS in accordance to ISO/IEC 27001. This international standard provides a model for establishing, operating, monitoring, maintaining and improving an ISMS to meet the specific security and business objectives of the organization and legal, statutory, regulatory and business obligations [1, 7]. Several best practices for IS management have been developed, such as Control Objectives for Information and related Technology (COBIT) [8], Information Technology Infrastructure Library (ITIL) [9] and national guidelines, such as NIST 800-53 [10].

1.2 Purpose and Structure of the Article

An increasingly faster changing environment (market, customer, technology, law or regulations) requires continual adaption of business objectives, processes, controls and procedures. It is a widely accepted principle that an activity cannot be managed and overall not improved sustainably if it cannot be measured. Therefore the effectiveness and performance of the ISMS and the actual risk and compliance situation must be continually evaluated and improved [3–5, 8–12]. Effectively implemented security measurements demonstrate the value of IS to top

management, face informed decision making, demonstrate compliance, improve security confidence and enable stakeholders to continual improve IS [8, 10, 12, 13]. It is a critical success factor for sustainable IS [1].

IS management, business management and on the other hand software security and network security engineering have been handled for a longer period as separate areas [12]. Measurement data are obtained at different levels within an organization. They are recorded and analyzed to detect errors and security events, to identify attempted and successful security breaches, incidents, threats and external events (such as changes to the legal or regulatory environment, changed contractual obligations, and changes in the physical environment) and to define effectiveness and performance of the implemented controls and the ISMS [7]. Based on this analysis appropriate corrective and/or preventive actions are elaborated, prioritized, approved, implemented and evaluated [1, 7, 10, 11].

It is axiomatic that those things for which no one is explicitly accountable are often ignored [14]. Thus we must define roles and responsibilities for all necessary tasks. According to COBIT 4.1 understanding the roles and responsibilities for each process is the key to effective governance [8].

How can we assign IS measurement and improvement roles and responsibilities efficiently, systematically, consistently and concretely? Are these assignments maintainable and traceable over a longer period?

Firstly we present the results of our literature research [II]. Based on these requirements we developed our hypothesis [III]. In Sect. 4 we explain our approach: firstly we establish the roles and describe their tasks [IV A]. In the second step we assign the IS measurement and improvement roles and responsibilities to the top and executive management [IV B]. After that we define and document all relevant IT services and their supporting items of all technical layers with their dependencies and relationships. To all these items we assign IS measurement and improvement roles and responsibilities [IV C]. Checks and quality assurance measures for the model [IV D] and the maintenance [IV E] are described next. This innovative approach is implemented successfully for several years by different medium sized organizations of distinct sectors (service, engineering and public). The obtained experiences are reflected in [V] with the project results [V A] and success factors [V B]. At the end we give an outlook and conclude [VI].

2 Research Framework

The field of defining security metrics systematically is young [12]. The problem behind the immaturity of security metrics is that the current practice of information security is still a highly diverse field. Holistic and widely accepted approaches are still missing [12].

A lot of papers are published about technical security metrics and scarcely holistic approaches. We find overall requirements for a holistic, systemic, managerial measurement approach [3, 8, 10, 11].

Measurement data must be extracted and reported to perform measurement and monitoring of the performance and effectiveness of the ISMS, to reflect the actual risk and compliance situation and to provide input for a continual improvement and for IS related management decisions [3–5, 7, 8, 10–12]. IS metrics support the detection of errors and security events and the identification of attempted security breaches, incidents and previously undetected or unknown IS issues [7, 11]. Based on this analysis appropriate corrective and/or preventive actions are elaborated, implemented and evaluated [1, 7, 10, 11]. The ISMS must be continually adapted to changing internal and external conditions to deliver sustainable business value to all stakeholders [1, 3–5, 7, 8]. Further the organization should maintain and improve the ISMS itself.

Since some years IS frameworks, standards, best practices, laws and regulations require that all stakeholders are responsible and collaborate for IS [1, 3, 4, 7, 8, 10, 11]. The management has to identify clear roles and assign responsibilities for the protection of assets and for all security processes and controls [1, 7, 8, 10, 11]. According to COBIT understanding the roles and responsibilities for each process is the key to effective governance [8]. Roles and responsibilities are required by ISO/IEC 27004 as one of the minimums of the measurement construct specification [11].

2.1 Roles and Responsibilities

The literature defines a lot of different functional roles and responsibilities for IS.

ISO/IEC 27004 distinguishes following roles [11]:

- client for measurement: the management or other interested parties,
- reviewer: validates that the developed measurement constructs are appropriate for assessing the effectiveness,
- information owner: responsible for the measurement,
- information collector: responsible for collecting, recording and storing the data and
- information communicator: responsible for first data analysis and the communication of measurement results.

The relevant stakeholders may be internal or external to the organizational units, such as information system managers or IS decision makers. Reports of measurement results can be distributed also to external parties, such as customers, shareholders, regulatory authorities or suppliers [11].

The measurement program implementation plan of the NIST performance measurement guide includes [10]:

- responsibilities for data collection, analysis, and reporting,

- details of coordination within the office of the chief information officer, relating to areas such as risk assessment, certification and accreditation, and federal information security management act (FISMA) reporting activities,
- details of coordination between the senior agency information security officers (SAISO) and other functions within the agency (e.g., physical security, personnel security, and privacy) to ensure that measures data collection is streamlined and non-intrusive.

Key IS stakeholders are the agency head, chief information officer (CIO), senior agency information security officer (SAISO), program manager or information system owner, and the information system security officer (ISSO) [10].

COBIT categorize following roles [8]:

- chief executive officer (CEO),
- chief financial officer (CFO),
- business executives,
- chief information officer (CIO),
- business process owner,
- head operations,
- chief architect,
- head development,
- head IT administration,
- project management officer (PMO),
- compliance, audit, risk and security groups and
- eventual head of human resources, budgeting and/or internal control.

COBIT provides a RACI (responsible, accountable, consulted and informed) chart for each process. Accountable means "the buck stops here". This is the person who provides direction and authorizes an activity. Responsibility is attributed to the person who gets the task done. The other two roles (consulted and informed) ensure that everyone who needs to be is involved and supports the process [8].

Different authors list the steering committee, board of directors/trustees, senior executives, business unit managers, collaborators from human resources, legal, compliance, audit, and risk management, chief information security officer or also a lot of more roles [1, 15, 16].

2.2 Further Requirements

An appropriate assignment of measurement roles and responsibilities should ensure that the results are not influenced by information owners. Brotby writes that approximately 35 % of IS managers still report directly or indirectly to the chief information officer who is also responsible for the IT department. Based on his experience this creates conflicts of interest and the quest for greater IT

performance at less cost is often made at expense of security [14]. Segregation of duties or independent checks can solve that problem [1, 3, 7, 8, 10, 11, 14].

The results of measurements need to be communicated to its intended audience in a way that is meaningful and useful. How they are represented and presented can make a huge difference to whether or not well-informed decision making can be achieved [13].

The relevant stakeholders should be identified. They should be involved in each step of IS measures development [11] to ensure organizational buy-in and promote a sense of ownership for IS measuring [10]. Each stakeholder requires specific, customized measures accordingly to his IS objectives and the IS requirements for his area of responsibility [10].

3 Hypothesis

Based on this research and requirements framework we developed an innovative, efficient and easy maintainable model to assign IS measurement and improvement roles and responsibilities to all organizational levels and stakeholders well structured, systematically, consistently, accurately, traceably and maintainable to promote IS effectiveness and continual improvement.

Firstly we establish the roles for IS measurement and improvement and describe their tasks [IV A].

As a second step we assign responsibilities for the established roles to the top and the executive management [IV B]. We start top down from top management (Fig. 1 in the top), functional unit responsibilities (Fig. 1 in the 2° level), business process and/or project responsibilities (Fig. 1 3° level) and eventually further service management role responsibilities, such as the change management role or IS management role (Fig. 1 vertically, right-most). Thereby we regard all relevant legal, statutory and contractual requirements and the IS policy and business requirements.

After that we elaborate and document all relevant business processes with their supporting IT services and their dependencies and relationships [IV C]. For all these IT services we describe based on an architecture oriented approach their supporting items with their dependencies and relationships going always deeper through all technical layers (Fig. 1 lower part). Based on definitions of the IT information library (ITIL) we understand by a configuration item any component that needs to be managed in order to deliver an IT service. Configuration items typically include IT services, hardware, software, buildings, people, and formal documentation, such as process documentation and service level agreements (SLAs) [9]. At the end we assign to each configuration item the specified IS roles and responsibilities (Fig. 1 vertically, on the right). The relationships and dependencies between the items, IT services, business processes and the top management define the information and escalation flow.

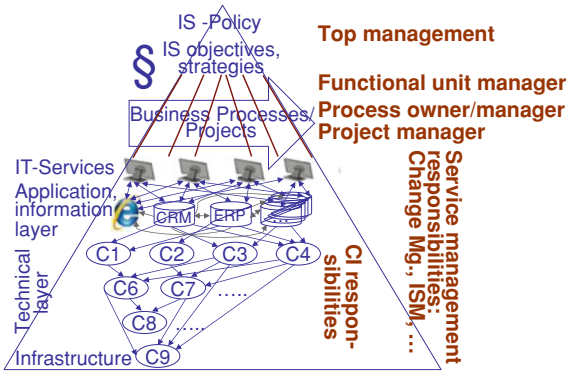

Fig. 1 Role responsibility assignment model

4 Approach

4.1 Roles and Responsibilities

Based on practical experiences of more organizations we enlarge the roles of a RACI (responsible, accountable, consulted and informed) chart to the following (see Table 1):

- The *accountable* is responsible for and decides the measurement requirements, provides direction and authorizes and reviews the effectiveness and performance. Thereby business and IS policy and strategies, legal, statutory, regulatory and contractual requirements, and the conducted risk assessment must be regarded. Additionally decision and authorization for continual improvements are part of his responsibilities. Measurement results are communicated to the accountable on request or by escalation, if measurement results exceed certain defined thresholds and/or time scales.
- The *responsible* contributes to the establishment of measurements and is responsible for their implementation. He controls the data collection, recording and analysis, communicates the results and proposes and implements possible improvements.
- *The responsible for execution and operating* is responsible for the measurement operation (collection and recording) and the improvements as part of his daily work.
- The *supportive* contribute and sustain him.
- The *informed and consulted* role contributes information and consultations to the responsible and eventually to the accountable and receives for this reason the measurement results.

The IS manager provides methods including possible metrics, evaluates and controls the effectiveness, performance and improvement of the whole system, conducts internal audits, proposes possible improvements, secures synergies and

Table 1 Overview of assigned roles and their tasks

Role	Tasks
Accountable	responsible for measurement requirements, provides direction, authorizes and reviews measurements, decides and authorizes improvements
	receives measurement results on request or by escalation
Responsible	responsible for implementation
	proposes and implements possible improvements
Responsible for execution and operating	responsible for measurement
	improves and adjusts as part of the daily work
Supportive for execution and operating	contributes to measurement
Informed and consulted	receives measurement results to consult and support responsible and eventually accountable

promotes IS awareness and knowledge exchange. His role is more based on coaching, mentoring, coordinating, training and offering method support and expertise than one practical operation.

4.2 Management Responsibilities

We document in collaboration with the top management her IS roles and responsibilities regarding the organization chart, the approved organizational structure and IS policy, as well as all relevant legal and statutory regulations.

The functional unit responsibilities and eventually IT service management role responsibilities are taken from the approved organization chart and defined organizational structure.

After we analyze and optimize all business processes for IS objectives and requirements [17]: all management processes, core business processes including support processes, resources processes and optimization processes. In that way we define the responsible and eventually supportive or consulted and informed IS roles for all process steps over the whole value network and the accountable for each business process, the process manager. Further for each process step necessary documents and data with data protection class and required archiving methods for all archive types are identified.

The project responsibilities are copied from the established project documentation or the project management database.

4.3 Item Responsibilities

The greater challenge and effort is to analyze, structure and define the configuration model with all relevant items. We start top down from the business

processes and bottom up from the physical infrastructure concurrently involving all collaborators concerned. Asset inventory, contract analysis, job descriptions, the documentation of the organizational structure and the organization chart provide helpful information. The necessary information is elaborated regarding the IS policy and all relevant IS requirements using different diagram techniques, brainstorming, and document analysis in workshops and by interviews.

In that way the IT service "Project management", for example, is defined as 100 % depending directly on two different servers and the local area network. Further we need for 50 % the internet, because the functionality of this application is limited, if the web services are not available. The local area network for example depends further on switches, cabling and others. Thereby we construct a configuration tree with upper or father items (e.g. "project management") and items, which support a service for the identified item, child or lower items (e.g. local area network). For each IT service the IS requirements concerning availability, confidentiality and integrity are defined. These requirements are inherit down through the whole tree regarding the dependency levels (e.g.50 % for the internet). Further all metrics for availability (e.g. uptime, unplanned downtime, mean time between failures and others) are inherit bottom up: if the network is down and project management depends on it (father), project management is down too. The priority and reaction time for corrective and preventive actions are calculated thereby on the inherited IS requirements.

The data protection requirements assigned to applications and archives by the business process analysis [IV B] are inherited to all child items, such as servers, networks, archives and rooms. The highest data protection requirement of all upper items must be regarded. In that way the responsible of each item receives clear and overall strategic and business aligned IS objectives and can define appropriate metrics, reports and overall corrective or preventive actions. A security breach, such as a too weak password for the access to sensitive data, for example, is scored higher and escalates earlier than the same breach regarding the access to personal data. Further details to the applied metrics, communication channels and corrective or preventive actions will be presented in other publications.

To each item we appoint exactly one collaborator as accountable. The accountable of each configuration item assigns the responsible role and the responsible for execution and operating role to exactly one collaborator each. Further he allocates all execution and operating roles and the informed and consulted roles to collaborators. In that way the assignment of responsibilities is as low as possible and the roles and responsibilities are distributed among all collaborators.

If measurement results exceeds defined thresholds or on request the results are communicated to the responsible of the father configuration item and on further escalation or on request also to the accountable of the father configuration item. All responsible and accountable of upper configuration items can receive on request or by escalation measurement results. In that way all measurement results are accessible also on request or by escalation to the top management.

Thus we assign all planning, operational and communication tasks for IS measurement to responsible, as well as corrective, preventive and improvement responsibilities to ensure sustainable IS.

On the top of the configuration model the IT services are linked to the business processes. Thereby the configuration model is connected with the management responsibilities [IV B].

4.4 Checks and Quality Assurance

We furthermore integrate consistency and accurateness checks [9]:

- Is there assigned to all configuration items exactly one accountable, responsible and responsible for executing and operating? Are responsible or accountable roles assigned only to internal collaborators?
- Are all relevant external suppliers registered as supportive for execution and operating?
- Has somebody assigned too many duties? Has some assigned too less duties? Is somebody involved in too many tasks?
- Are duties assigned to all collaborators?
- Are all configuration items, detected by network and system analysis, part of the configuration model?
- Is the configuration model consistent with the actual organizational structure and organization chart?

4.5 Maintenance

If an assigned accountable person changes, the structural organization is modified. Thereby the accountable is updated in the database.

The assigned accountable is responsible and has the access rights to change the distribution of all other role responsibilities to his collaborators. It is of his interest to assign clearly all new responsibilities to prevent eventual discussions, problems, duplication of work or uncompleted services.

5 Project Results

The presented concept for establishing and implementing IS measurement and improvement roles and responsibilities has been implemented since 2006 successfully by different medium sized organizations of distinct sectors (service, engineering and public). Implementing IS awareness, process and system thinking

and defining the configuration model in a well structured, systematic and consistent way were great challenges.

5.1 Achieving Project Objectives

The described concept leads to the following case study results collected by measuring the project process and interviewing the concerned management and collaborators:

- *Efficiency*: Establishing the whole configuration model and assigning management and configuration item roles and responsibilities required in medium sized organizations a work effort of approximately 1–2 weeks. This effort clearly varies based on the size and complexity of the organization. It depends overall on the IT services, the information risks that the organization faces, applicable legal, regulatory and contractual requirements and other success factors [V B]. To implement such a model for a telecommunication service provider needs for example essentially greater effort than for the IT department of an enterprise. The strategic alignment of all items with corporate objectives and business needs, the awareness of business drivers, process and system thinking and the understanding for the work and requirements of other functional and technical organizations' units was increased. Thus potential side effects and unplanned impacts of changes were reduced. The awareness for the supporting technology and supported business processes was enhanced and consequently the effectiveness of entire enterprise promoted.
- *Well structured, systematic, consistent and accurate roles*: Based on the developed configuration model the role responsibilities are defined over all layers and for all levels of the whole value network well structured and systematically. Due to the consistence checks [IV D] the assigned role responsibilities are consistent. For the collaborators a clear assignment of their responsibilities and tasks is essential in all organizations. Therefore they control the assigned roles continually and accurately. The developed model is an optimal basis for balanced, consistent and objective oriented IS improvement.
- *Traceability*: The role responsibilities were clearly assigned and all changes were documented, approved and communicated in a traceable way. All historical changes of responsibilities have been documented by versioning.
- *Maintainable*: Due to the great importance for management and collaborators to assign roles and responsibilities clearly, the documentation was maintained until today actually and accurately in all organizations.

Opposite to these advantages are the work effort for the establishment of the configuration model and the assignment of role responsibilities.

5.2 Success Factors

The IS measurement and improvement roles and responsibilities must be designed for the appropriate level of details, accordingly to business objectives, regulatory, statutory, legal, contractual and stakeholder security requirements.

Clearly this model must be best adapted and scoped to the organization and continual maintained. Such a model cannot be purchased and introduced as standard. A good knowledge and appreciation of business impacts and priorities and overall the involvement of all collaborators and managers concerned are imperative.

As for the whole ISMS the commitment and support from management as well as from all levels of staff, and overall the daily application and usage of such tools and methods by relevant stakeholders are essential and key success factors.

Corporate culture, organization and technology must be consistent and integrated optimally according to the business objectives and to collaborators needs and requirements in order to sustain business success. If such a tool is only used to blame and abuse collaborators than the collaborators will try to prevent with all means the introduction and maintenance of the model. A confident based, cooperative, team and objective oriented culture promotes such a collaborative IS.

Adequate tools, technical staff skills, sufficient IT infrastructure and IT support are also important for a successful implementation. Based on the complexity of a configuration model an adequate objective oriented database with high IS level (confidentiality, availability, integrity and traceability) sustains IS effectiveness, performance and improvement. An optimal connectivity with other systems supports change management and system inventory. It should be very simple and intuitive to handle. All collaborators should be able to find their assigned role responsibilities and to update information effectively in accordance to assigned access rights.

6 Conclusion and Outlook

We presented a practice approved, efficient, traceable and easy maintainable model to assign clear IS measurement and improvement roles and responsibilities to all organizational levels well structured and systematically.

IS governance, business management and on the other hand software security and network security engineering have been handled for a longer period as separate areas [12]. The innovation of this model is overall the integration of these approaches, the fully strategic alignment and the systemic, systematic and consistent approach for IS measurement, reporting and improvement. It shows up also eventually diverse or disparate technologies and applications and contributes thereby to more IT performance, resource and cost efficiency. The assigned responsibilities to IS roles can be checked continually to balance workload and improve adequate skills.

As a by-product IS awareness, IT alignment with business goals, service orientation, process and system thinking, as well as the comprehension for the requirements of other organization units were increased.

It is the basis of our holistic, systemic and collaborative IS framework. Due to excellent project experiences in several organizations there should be enhanced a holistic, systemic, collaborative and management oriented IS approach by regarding all success factors [V B].

Accordingly the informatics curricula should regard also more IT management aspects based on a holistic, systemic approach.

References

1. ISO, ISO/IEC 27002 (2005) Information technology, security techniques, code of practice for information security management, ISO, Geneva
2. PricewaterhouseCoopers LLP, information security breaches survey (2010) technical report, www.pwc.co.uk/pdf/isbs_survey_2010_techni-cal_report.pdf. Accessed 28 july 2010
3. von Solms SH, von Solms R (2009) Information security governance, Springer, New York
4. Da Veiga A, Eloff JHP (2007) An information security governance framework. Inf Manag Syst 24:361–372
5. Sowa S, Tsinas L, Gabriel R (2009) Business oriented management of information security. In: Johnson ME (ed.) Managing information risk and the economics of security, Springer, New York, pp 81–97
6. ISO, ISO Survey (2008) www.iso.org/iso/survey2008.pdf. Accessed 28 july 2010
7. ISO, ISO/IEC 27001 (2005) Information technology, security techniques, information security management systems requirements, ISO, Geneva
8. IT governance institute, control objectives for information and related technology (Cobit) 4.1 (2007) IT governance institute, Rolling Meadows
9. Office of government commerce (OGC) (2007) ITIL Service Design, The Stationery Office (TSO), Norwich
10. National institute of standards and technology (2008) Performance measurement guide for information security, NIST special publication 800-55 Revision 1, Gaithersburg
11. ISO, ISO/IEC 27004 (2009) Information technology, security techniques, information security management measurement, ISO, Geneva
12. Savola R (2007) Towards a security metrics taxonomy for the information and communication technology industry. In Proceedings of the IEEE 2nd international conference on software engineering advances, p 60
13. Humphreys E (2007) Implementing the ISO/IEC 27001 information security management standard, Artech House, Boston
14. Brotby K (2009) Information security governance, a practical development and implementation approach, John Wiley and Sons, Hoboken
15. Ray B (2007) Information lifecycle security risk assessment. Comput Secur 26:26–30
16. Wood C (2003) Information security roles and responsibilities made easy, Information Shield, Houston
17. Stoll M, Laner D (2010) Information security and system development. In: Sobh T et al (eds) Novel algorithms and techniques in telecommunications and networking. Proceedings of the IEEE TeNe 08, Springer, Berlin, pp 35–40