Towards a Modelling Language for Managing the Requirements of ISO/IEC 27001 Standard

Daniel Ganji
Centre for Secure, Intelligent and Usable Systems (CSIUS)
University of Brighton
Brighton, UK
d.ganji2@brighton.ac.uk

Haralambos Mouratidis
Centre for Secure, Intelligent and Usable Systems (CSIUS)
University of Brighton
Brighton, UK
h.mouratidis@brighton.ac.uk

Saeed Malekshahi Gheytassi
Centre for Secure, Intelligent and Usable Systems (CSIUS)
University of Brighton
Brighton, UK
m.s.malekshahi@brighton.ac.uk

***Abstract*—Security standards help organisations to continually review and refine the information security procedures to remain safe and secure, however, organisations face difficulties and are concerned about understanding the requirements of the standards. The research to date from the industry and academia tended to focus on the overall description of the standard and such expositions are unsatisfactory because little is being contributed to the practicality of the Information Security Management System (ISMS) structure. The generalisability of much-published research on the standard is insufficient for organisations aiming to implement the standard. An objective of this paper is to offer a direction towards a new modelling language to assist organisations to better understand the requirements of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001 standard. The methodological approach took in developing our proposed research was found by systematically investigating the current gap in the literature and to explore the underlying needs of organisations to adopt the ISMS. This paper contributes a set of original components and concepts to holistically capture, model, and manage the requirements of the standard. Our modelling language enables information security practitioners and interested parties in organisations to develop an ISMS and promote their corporate compliance with a well-established standard.**

Keywords–information security management system; requirements engineering; ISO/IEC 27001; PDCA; ISMS.

I. INTRODUCTION

In the new global economy, organisations face tougher pressure in securing the information of their clients. Some of these pressures are through mandatory rules and regulations, such as complying with the European Union General Data Protection Regulation (EU GDPR), the interested parties' requirements, or their own requirements to safeguard their trade secret from their competitors. Increasingly, regulations demand software engineers to analyse, design and implement responsible systems to comply with laws and regulations [1]. It is an important task for organisations to meet their information security requirements and take appropriate actions to satisfy their expectations.

The number of information security breaches is getting bigger and invaders are getting smarter in ways to exploit security vulnerabilities [2] [3]. Conventional and outdated management of security systems does not answer the needs of the current structure. Improving security in an organisation is not just about expenditure on new technologies but correctly addressing the basics of information security and risk-related elements such as threat and vulnerability management, log management, backup and system hardening [4]. To date, there has been no solid evidence to absolute security and protection, however, there are available frameworks and approaches such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001 standard to promote the best practices in managing information security. Organisations need to prepare towards sophisticated approaches considering security techniques under one interconnected application known as Information Security Management System (ISMS) to preserve the confidentiality, integrity, and availability of information assets.

ISO/IEC 27001 is an international standard and applicable to all organisations, regardless of their type, size, or nature [5]. It constitutes a certifiable standard and is widely used with steady growth in a number of adoptions [6]. The standard is composed of processes, policies, and resources that can be used to systematise the security demands of an organisation. The ISO/IEC 27000 family of standards helps organisations to implement a robust approach to managing information security and building resilience. By providing compliance to a globally known standard, certification significantly reduces the need for repeated client audits.

Understanding and applying the requirements of any standard into an organisation is not always a straightforward process. From the review of the literature, it appears that opportunities exist to evaluate the implementation and effectiveness of the standard in organisations, but academic researchers as described in Section III have not taken the challenge. Our research proposes a model-driven approach to enable organisations to adopt the requirements of the standard using requirements engineering concepts.

The remainder of the paper is thus set out as follows: Current challenges are described in Section II, and the related work in Section III. In Section IV, we present the mapping methodology and mapping requirements for our proposed framework. Our modelling language and its concepts are described in Section V. Finally, our conclusions and future work will be set out in Section VI.

 ISBN: 978-1-61208-701-6

II. Current Challenges

IT Governance, a provider of IT compliance solutions to organisations released an annual survey [7] centred around the experience and implementation challenges of the ISO/IEC 27001 for organisations in 2016. The investigation of 250 information security professionals from 53 countries who participated in the survey were mostly certified or working towards certification (80%). 71% of respondents received either regular or occasional requests to provide the ISO/IEC 27001 certification from clients or when proposing for new business. By providing compliance to a globally known standard, certification significantly reduces the need for repeated client audits. The survey also found that a third of all respondents were concerned about understanding the requirements of the standard and 28% considered the creation and managing the standard documentation a challenging task. Other substantial challenging tasks were conducting the information security risk assessment and identifying the required controls for 22% and 14% of the respondents respectively.

Organisations understand that it is in their interest to follow some type of internationally recognised reference framework to create environments for ISMS rather than doing it ad hoc [8]. From the commercial aspect, it is rather difficult and costly task to identify the resource required to plan, implement, measure information security management system.

From an academic perspective, ISMS has mostly drawn from the views of practitioners [9] and the investigation of the literature indicates that ISMS has not been particularly attractive in academia with a lack of research and approaches are egregious. Management systems on information security have received very limited observation and research from the academic community despite the high interest from organisations in particular for IT, operational and compliance audits [10]. There is a relative paucity of scientific literature focusing specifically on the requirements of the standard; most of these studies have been on the previous version of the standard prior to 2013. In response to the real-world and academic challenges, this research contributes a model-based approach to organisations to identify and manage the requirements of the standard.

III. Related Work

Mayer proposed Information System Security Risk Management (ISSRM) [11] [12], which provided a reference conceptual model for security risk management. The author proposed a model-based approach for ISSRM, applicable since the early phases of IS development. The work focused on the modelling support to such an approach, by proposing a domain model for ISSRM. The work defined a reference conceptual model for security risk management and enhancement of the domain model with the different metrics used in a risk management method. Further, the authors developed a proposal of the Secure Tropos language and a process to use the extension in the frame of risk management.

Beckers et al. proposed PAttern-based method for establishing a Cloud specific informaTion Security management system (PACTS) [13] [14]. An approach for creating an ISMS methodology compliance to the ISO/IEC 27001 standard cloud environment with a specific interest in legal compliance and privacy. The overview of the methodology was leadership commitment, asset identification, threats analysis, risk assessment, security policies and reasoning, ISMS specification, identify relevant laws and regulations, the definition of compliance controls, instantiating privacy patterns, privacy threats analysis.

Beckers et al. proposed ISMS-CORAS [15] [16], an extension of the COROS method to support the establishment of the ISO/IEC 27001 compliant ISMS. Authors proposed a methodology following the CORAS method. CORAS is a risk management methodology based on the ISO 31000 standard.

Susanto et al. proposed Integrated Solution Framework (I-SolFramework) [17] [18] to assesses the readiness level of an organisation towards the implementation of the ISO/IEC 27001. The framework offered e-assessment and e-monitoring to analyse and perform an assessment of the readiness level of the standard implementation. E-assessment measures the standard parameters based on the framework, which is consist of six components. It helps to validate the ISMS parameters through an analytical interface such as histogram, charts and graphs, provided by a framework.

The investigation of the related work indicates that far too little attention has been paid to address all or most requirements of the standard. Limited studies were found to support most requirements of the standard. Restricted to no evidence of some requirements were detected in the literature, such as monitoring and evaluation of the information security performance, internal audit, management review to consider the effectiveness of the management system, nonconformity and corrective action to identify and eliminate the root of nonconformities, and continual improvement to improve the effectiveness of the ISMS. Majority of the literature such as PACTS, I-SolFramework, ISMS-CORAS mainly support the planning stage of the standard, which is the pre-implementation of the standard, therefore, the post-implementation is missing from the current literature.

IV. Methodology

The ISO/IEC 27001 standard is a set of requirements for establishing, implementing, deploying, monitoring, reviewing, maintaining, updating and improving an ISMS with regard to an organisation's overall risks and opportunities. The former version of the standard was based on a process approach is known as Plan-Do-Check-Act (PDCA) model which each is defined below:

- Plan: Establish the ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security.
- Do: Implement and operate the ISMS policy, controls, process and procedures.
- Check: Assess and measure process performance against ISMS policy.
- Act: Maintain and improve the ISMS by taking corrective actions where nonconformity occurs.

An organisation must identify and implement the standard requirements in order to claim conformity with the standard. It needs to be able to distinguish these requirements from other recommendations where there is a certain freedom of choice. The standard document consists of many clauses and sub-clauses in the form of normative phrases. There is no specific method in the interpretation of the ISO/IEC 27000 family of standards, however, an approach developed by the

 ISBN: 978-1-61208-701-6

ISO to extract and interpret the clauses of the standard is available. The interpretation rules are based on the provisions of the ISO/IEC Directives, Part three, Rules for the structure and drafting of international standards, Annex H.

The requirements set out in the standard are generic and exclusions of any of the requirements specified in clause four to ten are not allowed when an organisation claims conformity to this international standard. Compliance with ISO/IEC 27001 can be formally assessed and certified by an external accredited certification body. A detailed descriptions of all requirements used as part of this paper are summarised in Table I.

V. Proposed Modelling Language

The requirements of the standard were described in the previous section. Part of the aim of this paper is to introduce a mapping between the requirements of the standard and concepts taken from the requirements engineering to assist with the implementation of the ISMS, the result of the mapping is illustrated in Fig. 1. The top part of the figure shows the requirements of the ISMS and the layers of the PDCA covering the requirement. The bottom part of the figure represents the concepts proposed in our modelling language indicating the area of relevancy with the requirements of the standard.

In this section, we present our modelling language which enables the expression of the relationships and concepts in correspondence with the ISO/IEC 27001 standard. The rest of this section focuses on presenting the various building blocks of the proposed language. First, an overview of the language components will be explained. Next, each concept will be discussed in details. The concepts attributes and relationships proposed in the modelling language are demonstrated in the meta-model, provided in Fig. 2.

The four components used in the modelling process include:

- Information security requirements elicitation: The first component captures the overall organisational structure in relation to information security.
- Information security analysis: The second component analyses the organisational standing in relation to information security.
- Management system requirements elicitation: The third component develops management system posture with the organisational structure.
- Management system analysis: The fourth component identifies and analyses the processes of the management system.

A. Information Security Requirements Elicitation

This component discusses each concept required to model the organisational structure including Actor, Constraint, Goal, Asset, and Dependency. A description of each concept and its properties are discussed below.

Actor: A concept of actor represents a person or entity that has intentionality and strategic goal relevant to the scope of the ISMS. An actor could have a direct or indirect effect, be affected by or perceive themselves to be affected by a decision or activity within the scope of the ISMS. This concept has four properties including Id, Description, Type, and Competency.

An actor is also known as a user or stakeholder, however, this interpretation may isolate the full characteristics of an actor, hence, types of actors were introduced to capture the interest of an actor within the organisation. The two types of actor are external or internal. An external actor is a person or entity from the external environment of the organisation who pays for a service or expects the level of principles in relation to the external context of the organisation as a whole, and not necessarily from the ISMS. This could be an independent person(s) like a client or an entity like a national or international authority such as governmental agencies and regulatory bodies. An internal actor is a person or entity from the internal environment of the organisation who benefits

TABLE I. REQUIREMENTS OF ISO/IEC 27001:2013 STANDARD

Requirement	Description
Organisational context	Define the external and internal parameters and issues affecting the outcome of ISMS.
Interested parties	Identify the interested parties and their information security requirements relevant to the ISMS.
Determining the scope	Identify the logical or physical boundaries and applicability of the ISMS.
ISMS	Establish, implement, and continually improve an ISMS under the requirements of the standard.
Leadership	Top management to demonstrate leadership and commitment with respect to the ISMS that are compatible with the strategic direction of the organisation.
Policy	Establish directions and making references to IS objectives and appropriate to the purpose and context of the organisation.
Roles	Top management to assign and communicate the responsibilities and authorities relevant to information security for reporting performance of the ISMS within the organisation.
Risk and opportunities	Systematically determine the potential risks and opportunities that may be involved in a projected activity or undertaking.
Information security objectives	Define measurable information security objectives.
Resources	Identify the resources needs to manage the ISMS.
Competence	Identify the necessary ability of a persons knowledge and skills doing work under its control that affects information security performance.
Awareness	Persons working under the organisation's control to be aware of the information security policy and their contribution to the effectiveness of the ISMS.
Communication	Apply internal and external communication process relevant to the ISMS.
Documented information	Create, update, and control documented information required by the standard and necessary for the effectiveness of the ISMS.
Operational planning	Plan, implement and control the process needed to meet information security requirements including risk and opportunities, and information security objectives.
IS risk assessment	Perform security risk assessment.
IS risk treatment	Implement information security risk treatment.
Monitoring & measurement	Evaluate the information security performance and its effectiveness.
Internal audit	Conduct regular internal audits and systematically evaluate the effectiveness of the implemented and maintained ISMS.
Management review	Top management to review the organisation ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness.
Nonconformity & corrective action	React and evaluate nonconformity occurrences, review and deal with appropriate corrective actions.
Continual improvement	Recurring activity to continually improve the suitability, adequacy and effectiveness of the ISMS.

 ISBN: 978-1-61208-701-6

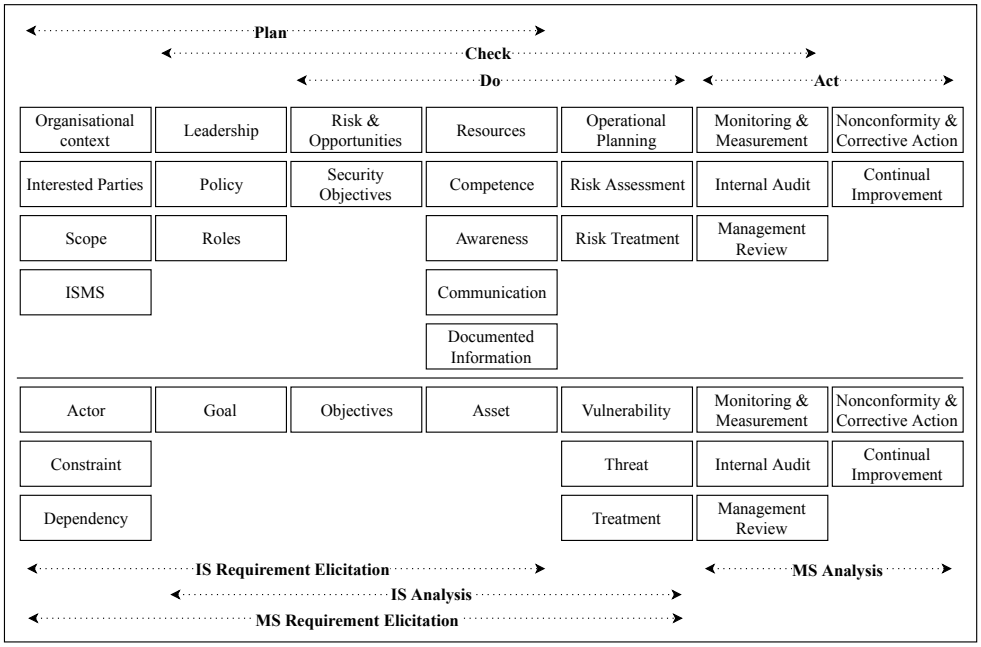

Figure 1. Language mapping to the requirements of the ISO/IEC 27001 standard

from the success of the ISMS or contribute to the success of the ISMS. This could be an employee, a contractor who works under the supervision of the organisation, or a group of interested parties such as shareholders or owners who may only have a financial interest in the organisation.

The last property of an actor is the competency level, which indicates the ability to apply knowledge to intended goals within the scope of the ISMS. An actor must have the necessary competence for doing work under his/her control that affects its information security performances.

Constraint: A concept of constraint represents the restrictions that an actor may have within the scope of the ISMS. A constraint could limit the operation of goals or access to assets. Constraint represents boundaries that do not permit specific action to be taken or prevent a certain goal from being achieved. Constraints are often beyond the control of an organisation, these are conditions or expectations that actors wish to introduce and impose to the organisation. A constraint concept has three properties including Id, Description, and Type.

Consideration to all constraints are an important part of an ISMS, however, not all constraints are equal in their nature and an application of a constraint could be designated based on relevance and priority. Some constraints may have specific instructions on how they should be satisfied whilst some others may be more flexible and could be satisfied by a number of means, therefore, it allows the organisation to prioritise and effectively plan its resources. In the light of above, two types of constraints were introduced, obligatory or advisory. An obligatory constraint means the organisation has no control or negotiation capability over the implementation or dismissing such a constraint. An obligatory constraint could be introduced by any types of an actor but it is likely to be instructed by external actors such as governmental and regulatory bodies or as part of a contractual obligation with another entity. An advisory constraint means the organisation has some flexibility or negotiation capability to apply alternative means to satisfy a constraint. An advisory constraint could be introduced by both the internal and external types of actors.

Asset: A concept of asset refers to organisational assets and anything that has value for the organisation. An asset includes tangible or intangible items and not only refers to the monetary value of an item. An asset concept has four properties including Id, Description, Classification, and Ownership.

Information assets should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. Classification property categorises assets into three types of public, confidential, restricted. An organisation is responsible to define or extend the number of categories in accordance with the information classification scheme and suitable to their needs.

The last property is asset ownership. Each asset owner should be identified, this is an actor who owns an asset and could be different from an actor who uses the asset in the organisation. The owner is not necessarily a person but it could be a number of people or an entity such as a department in the organisation that owns an asset or group of assets.

Goal: This concept refers to the actor's strategic interest [19] or duty. Each actor could have a number of goals within the scope of the ISMS. A goal could be initiated by an internal actor such as an employee to being able to do their job such as accessing customer's account or from an external actor such as clients to access their services provided by the organisation. This concept has two properties including Id and Description.

A Goal could be divided into smaller goals known as sub-goals. Goals are an important part of a management system and they could lead the management system to success or failure if not identified and addressed correctly.

Dependency: A concept of dependency derived from the Secure-Tropos methodology [19], which express the relationship between an actor with a goal depending on another actor, goal or asset to accomplish its goal. The former actor called the depender and the latter is called dependee. The types of the

 ISBN: 978-1-61208-701-6

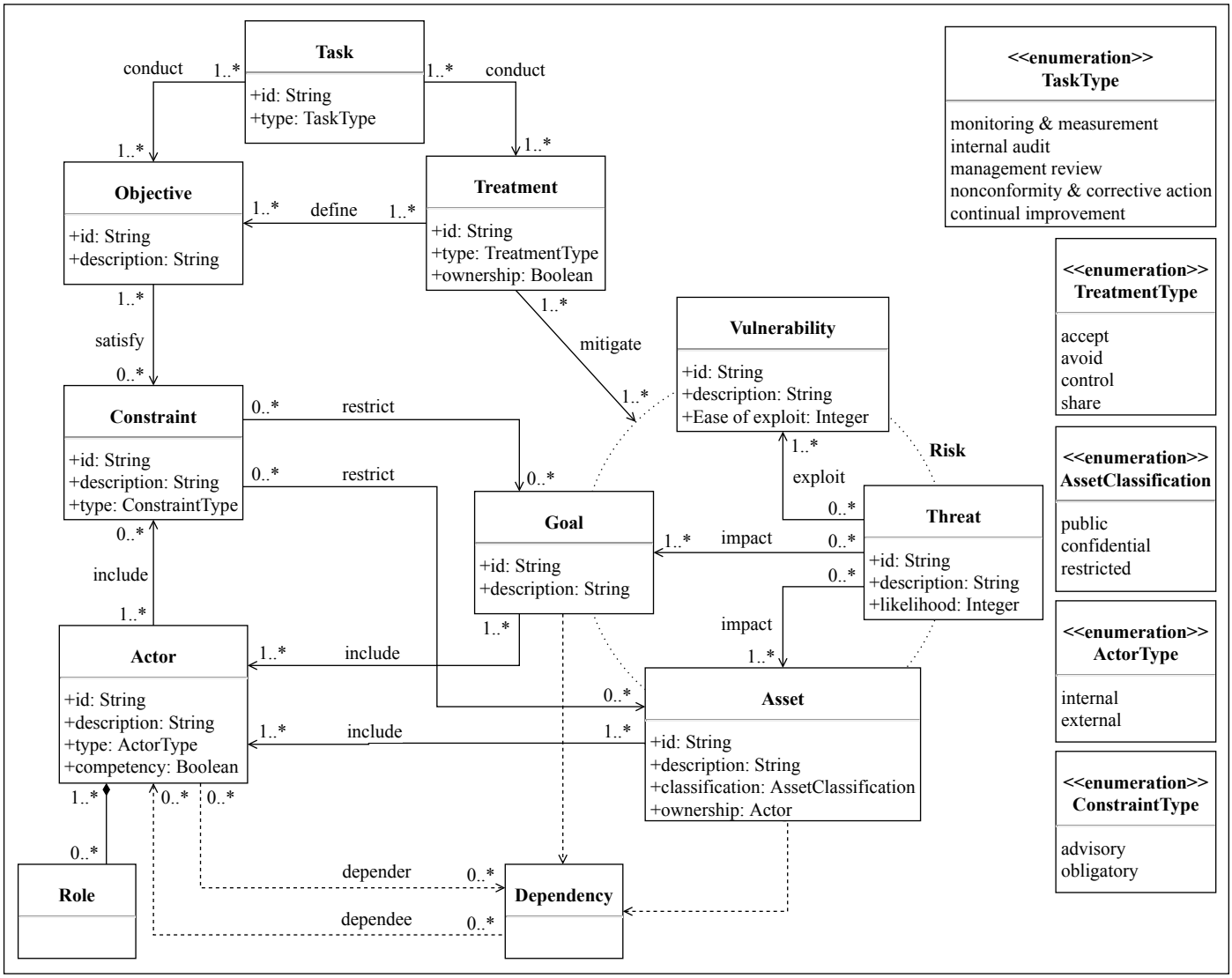

Figure 2. Proposed meta-model

dependency describe the nature of an object between dependee and depender is refereed as dependum. A dependency concept has no properties.

B. Information Security Analysis

This component exercises the concepts required to model the analysis of the organisation in relation to information security. The analysis is performed around a risk management methodology which enables to better understand the impacts of the information security risks on the organisational goals and assets by introducing concepts such as Vulnerability, Threat, and Treatment. A description of each concept and its properties are discussed below.

Vulnerability: A concept of vulnerability refers to a weakness of a goal, asset, or treatment which can be exploited by one or more threats. A threat that does not have a corresponding vulnerability may not result in risk. A vulnerability concept has three properties including Id, Description, and Ease of exploit. Ease of exploit determines a chance of vulnerability to happen and will be the subject of a successful attack.

Threat: A concept of threat refers to the potential cause of an unwanted incident, which may result in harm to a goal or asset. A threat has the potential to harm assets such as information, process, and systems and therefore organisation. A threat concept has three properties including Id, Description, and Likelihood. Threats may be of natural or human origin and could be accidental or deliberate. Both accidental and deliberate threat sources should be identified and assess their likelihood. Likelihood or probability indicates the severity of the cause of a threat.

Treatment: This concept refers to mitigate a risk arising from the impact of threats to assets or goals by exploiting a vulnerability. A treatment concept has three properties including Id, Type, and Ownership approval. A treatment type may involve one or more mitigating approach including accept, avoid, transfer, and reduce. Ownership approval indicates that a mitigating approach is approved by the responsible risk owner. The risk owners' approval for the information security risk treatment plan and acceptance of the residual information security risks is a mandatory requirement of the standard.

 ISBN: 978-1-61208-701-6

C. Management System Requirements Elicitation

This component utilises the concept to develop management system posture along with the organisational structure in relation to the information security. The description of the Objective and its two properties are discussed below.

Objective: It refers to the achievement of a specific result from the ISMS. Information security objective could be defined by targeting the aim of a treatment control or a policy to satisfy a constraint raised from actors. An objective concept has two properties including Id and Description.

D. Management System Analysis:

This component identifies the mandatory processes of the management system that involves the analysis of the outcomes from the concepts developed in the previous components. The structure of the ISMS is analysed and measured against the requirements of the standard to ensure that the ISMS is effective. The description of Task and its properties are discussed below.

Task: A concept of task refers to general mandatory requirements of the management system to ensures that processes of the ISMS are developed, implemented and working as expected. A task concept has two properties including Id and Type. Type refers to specific constitutions of the management system. Task types are monitoring and measurement, internal audit, management review, nonconformity and corrective action, and continual improvement.

The first type of task is the monitoring and measurement, a mandatory requirement for an organisation to evaluates the information security performance and the effectiveness of the ISMS. An example is to monitor the treatment controls identified in the risk management and evaluate their effectiveness with the expected target. This activity could be automated using tools or physically observe and measure the effectiveness of such treatment control. A role for performing monitoring and measurement and an interval for measuring and effectiveness should be identified. A person responsible for evaluating the results of monitoring and measurement should be identified.

The second type is the internal audit, a mandatory requirement of the management system to ensures that the organisation conforms to the requirements of the standard and own requirements for its ISMS. Internal audit should be carried out at a planned interval. The organisation should develop an audit programme, including the frequency, methods, and responsibilities for delivering the audit. Suitable auditors should be identified and the results of the internal audit to be reported to the relevant management.

The third type is the management review, a mandatory requirement for the top management to review and assess the outcome of the management system at an interval period. The management review should consider the status of the previous management reviews, feedback from actors, results of the internal audit, and monitoring and measurements. The outcome of the management review should include decisions related to continual improvement and any need for changes to the ISMS should be noted.

The fourth type is the non-conformity and corrective action, it is a task to model the cause of the non-conformities and identify the root causes. It is a mandatory requirement for an organisation to implement necessary corrective actions against the cause of the non-conformities.

The last type of task is the continual improvement, a task that requires an organisation developing ISMS to improve the suitability, adequacy and effectiveness of the ISMS.

VI. Conclusion

The work proposed in this paper extends existing research efforts in security requirements engineering, building upon concepts from software engineering and deliver a language to coherently model and capture the requirements of an information security management system.

In this paper, we focus on bridging the gap in requirements engineering with information security management system. The intention is to align the development of secure systems in organisations towards the requirements of the standard. We presented a model-driven approach to employ a number of requirements engineering concepts to holistically manage the requirements of the standard under four inter-related components. The work goes beyond the aim of the research in relation to the security requirements engineering and it contributes in understanding the key concepts in successfully preparing and applying the ISMS and how it can be developed as a process to address the specific needs of the normative standards like ISO/IEC 27001 standard.

Further research to enhance all four components and expand a series of complete processes to work along with the concepts of the language is required. In future investigations, our proposed risk methodology will be evolved as well as the introduction of new attributes to the task concept.

The present paper was limited by the absence of an assessment example to better understand the effectiveness of our research, however, our model-based language is currently under evaluation by applying our approach to a UK health insurance provider aiming to comply with the ISO/IEC 27001 standard. The preliminary feedback suggests that our approach has been successful in capturing the requirements of the standard and the experimentation from the top management has shown positive results in understanding the importance of the ISMS for the establishment. This has given confidence to the organisation that the implementation of the ISMS through a structured process would enhance operational excellence and reduce liabilities.

References

[1] T. D. Breaux and A. I. Anton, “Analyzing regulatory rules for privacy and security requirements,” IEEE Transactions on Software Engineering, vol. 34, no. 1, 2008, pp. 5–20.

[2] E. Targett, “6 months, 945 data breaches, 4.5 billion records,” 2018. [Online]. Available: https://www.cbronline.com/news/global-data-breaches-2018

[3] Breach Level Index, “Data breach database,” 2018. [Online]. Available: https://breachlevelindex.com/data-breach-database

[4] S. Moore, “Gartner Says Worldwide Information Security Spending Will Grow 7 Percent to Reach $86.4 Billion in 2017,” 2017. [Online]. Available: https://www.gartner.com/newsroom/id/3784965

[5] ISO, “ISO/IEC 27001 Information security management.” [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html

[6] ISO, “The ISO survey of management system standard certifications 2017,” International Organisation for Standardisation, Tech. Rep., 2017.

[7] IT Governance, “ISO 27001 global report,” IT Governance, Tech. Rep., 2016.

[8] B. Von Solms, “Information Security governance: COBIT or ISO 17799 or both?” Computers and Security, vol. 24, no. 2, 2005, pp. 99–104.

[9] E. Coles-Kemp, “The anatomy of an information security management system,” Ph.D. dissertation, King’s College London, 2008.

[10] E. W. Bernroider and M. Ivanov, “IT project management control and the Control Objectives for IT and related Technology (CobiT) framework,” International Journal of Project Management, vol. 29, no. 3, 2011, pp. 325–336.

[11] N. Mayer, “Model-based management of information system security risk,” Ph.D. dissertation, University of Namur, 2008.

[12] N. Mayer, “A cluster approach to security improvement according to ISO/IEC 27001,” in 17th European Systems & Software Process Improvement and Innovation Conference (EUROSPI’10), Grenoble, France, 2010.

[13] K. Beckers, I. Cote, S. Faßbender, M. Heisel, and S. Hofbauer, “A pattern-based method for establishing a cloud-specific information security management system,” Requirements Engineering, vol. 18, no. 4, 2013, pp. 343–395.

[14] K. Beckers, M. Heisel, I. Côté, L. Goeke, and S. Güler, “Structured pattern-based security requirements elicitation for clouds,” Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013, 2013, pp. 465–474.

[15] K. Beckers, M. Heisel, B. Solhaug, and K. Stolen, “ISMS-CORAS : a structured method for establishing an ISO 27001 compliant information security management system,” Sintef, Tech. Rep., 2013.

[16] K. Beckers, “Supporting iso 27001 establishment with CORAS,” Pattern and Security Requirements: Engineering-Based Establishment of Security Standards, 2015, pp. 1–474.

[17] H. Susanto, M. N. Almunawar, and Y. C. Tuan, “Information security challenge and breaches : novelty approach on measuring ISO 27001 readiness level,” International Journal of Engineering and Technology, vol. 2, no. 1, 2012, pp. 67–75.

[18] H. Susanto, M. N. Almunawar, Y. C. Tuan, and M. S. Aksoy, “I-Solframework: an integrated solution framework six layers assessment on ultimedia information security architecture policy compliance,” International Journal of Electrical & Computer Sciences IJECS-IJENS, vol. 12, no. 01, 2012, pp. 20–28.

[19] H. Mouratidis and P. Giorgini, “Secure Tropos: a Security-Oriented Extension of the Tropos Methodology,” International Journal of Software Engineering and Knowledge Engineering, vol. 17, no. 02, 2007, pp. 285–309.

 ISBN: 978-1-61208-701-6