Approaches to Develop and Implement ISO/IEC 27001 Standard - Information Security Management Systems: A Systematic Literature Review

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

Christos Kalloniatis
Privacy Engineering and Social Informatics Laboratory
Department of Cultural Technology and Communication
University of the Aegean
Greece
chkallon@aegean.gr

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

***Abstract*—This systematic literature review intends to determine the extent to which contribution is available to assist organisations and interested parties to understand better or comply with the requirements of the ISO/IEC 27001 international standard, known as Information Security Management Systems (ISMS). The primary aim of this paper is to explore the current literature in the ISMS as specified by the ISO/IEC 27001 standard, aiming to provide a mapping of their contributions with the requirements of the standard. An objective of this study is to explore the ways in which the literature addresses the requirements of the ISMS. This study uses semi-quantitative analysis in order to gain insights into the concepts and techniques around the ISMS and to systematically obtain data to help with identifying the research gaps. One of the findings of this review is to encourage to benefit from available literature and to develop an ISMS to promote their corporate compliance with a well-established standard. The most striking result from the review is that the majority of approaches proposed by scholars between 2005 to 2018 are with limited support in adopting the information security management system. Another important finding is that almost all available approaches fundamentally lack the motivation to focus on the analysis and application of the ISMS with no single study enable organisations to adopt the ISO/IEC 27001 standard.**

Keywords–ISO/IEC 27001; information security management systems; PDCA; requirements engineering; information security risk management.

I. INTRODUCTION

In the new global economy, organisations face tougher pressure in securing their internal and external information. Some of these pressures are through national and international laws and regulations, interested parties expectations, and organisational requirements to safeguard their business secrets from their competitors. It is a compelling task for organisations to meet the security requirements and take the necessary actions to implement and satisfy their security objectives [1]. In contrast, the continual change in technology, management use of technology and the impact on business success makes the management information systems an exciting topic in organisations [2].

To date, there has been no solid evidence to absolute security and protection, however, there are available security frameworks and techniques to promote the best practices in managing information security. Organisations need to prepare towards sophisticated approaches considering security and its associates under one interconnected application to successfully manage confidentiality, integrity, and availability of information assets. The numbers of security breaches are getting bigger and invaders are getting smarter in ways to exploit security vulnerabilities. Conventional and outdated managing of information security does not answer the needs of the current structure [3] [4]. Experts believe that more than 90% of successful cyber attacks could have been prevented by the technology available at the time [5].

Information Security Management System (ISMS) as defined by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001 is an international standard to provide requirements for establishing, implementing, maintaining and continually improving an information security practices in organisations. ISO/IEC 27001 is integrated part of the organizations processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. The standard is applicable to all organisations, regardless of their type, size, or nature [6] and it constitutes a certifiable standard and is widely used with steady growth in a number of adoptions [7]. The standard provides mapping for establishing, implementing, maintaining and continually improving an information security management system or alternatively known as Plan-Do-Check-Act (PDCA) model.

It is a strategic decision for an organisation to adopt ISMS and to preserve the confidentiality, integrity, and availability of information by applying risk management process and giving confidence to interested parties that risks are adequately managed. ISMS is composed of processes, policies, and resources that can be used to systematise the security demands of an organisation. Organisations understand that it is in their interest to follow some type of internationally recognised reference framework to create environments for information security management systems rather than doing it ad hoc [8].

The primary aim of this systematic review is to investigate in detail the available software engineering techniques on the ISMS that enable organisations to comply with the require-

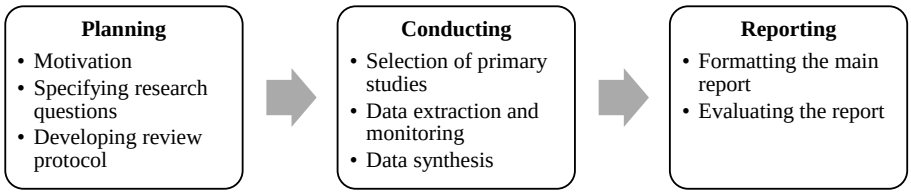

Figure 1. Summary of the phases in the systematic literature review

ments of the ISO/IEC 27001 standard. Additionally, the review explores the strengths and limitations of the current literature to establish discussion for future work.

The remaining part of the paper proceeds as follows: Section II describes the methodology used as part of this review including the phases of the review and data analysis. The results of the review are reported in Section III. Section IV discusses the findings of the review, focusing on the three research questions set out in the next section. Lastly, Section V provides a brief overview of the key findings, making suggestions for future work.

II. METHOD

This study conducted in the form of a systematic literature review by employing Guidelines for Performing Systematic Literature Reviews in Software Engineering introduced by Kitchenham et al. [9] [10] and Webster et al. [11].

The review involved a series of activities divided into three phases are shown in Figure 1. The steps in the review method documented below.

Planning phase: The initial step sketched the need for undertaking this review by considering all existing information about the ISO/IEC 27001 standard and software engineering in a thorough and impartial manner. The second step of the planning was to specify the research questions by considering the types and structure of the questions as discussed in Section II-A. The last part of the planning phase was to develop a review protocol to specifies the methods that will be used to undertake the review and reducing the possibility of a bias. The components of our review protocol include study selection procedures explained in Section II-B, study selection criteria defined in Section II-C, data extraction strategy set out in Section II-D, and synthesis of the extracted data explained in Section II-E.

Conducting: This phase implemented the steps identified in the research protocol from the former phase. The initial step identified the primary studies to provide direct evidence about the research questions. Next, to accurately recorded the information obtain from the primary studies. Finally, a descriptive synthesis of the primary studies developed to provide a summary of the results in Section III.

Reporting: The last phase involved the writing of the review findings obtained from the results section are summarised in Section IV.

A. Motivation and Research questions

The research to date from the industry and academia tend to focus on the overall description of the standard and such expositions are unsatisfactory because little is being contributed to the practicality of the ISMS structure. The generalisability of much-published research on the standard is insufficient for organisations aiming to implement the standard.

IT Governance, a provider of IT compliance solutions to organisations released an annual survey [12] 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.

From the commercial aspect, it is a rather difficult and costly task to identify the resources required to implement, measure, and manage information security. From an academic perspective, ISMS have mostly drawn from the views of practitioners [13] and our literature review indicates that ISMS has not been particularly attractive in academia with a lack of research and approaches are egregious. Management systems on information security received very limited observation and research from the academic community despite the high interest from organisations in particular for IT, operational and compliance audits [14].

The purpose of this review is to systematically evaluate and measure the current literature in compare with the requirements of the standard and gain further understanding of the gap in the literature. The review sought to answer the following research questions:

RQ1. What are the software engineering approaches that organisations could use to apply or implement the requirements of the ISMS as defined by the ISO/IEC 27001 standard? We aim to identify the software engineering techniques and tools to assist interested parties, such as information security officers, compliance managers, and top management in organisations to adopt and comply with the requirements of the ISO/IEC 27001 standard.

RQ2. What are the scholarly contributions to the literature since the introduction of the ISO/IEC 27001 standard in 2005? Research into a good security practice has a long history back to 1989 when a set of internationally recognised security evaluation criteria was developed by the Department of Trade and Industry (DTI) Commercial Computer Security Centre

(CCSC). This was further developed by British Standard Institute to British Standard BS7799-1 in 1995 and later adopted by ISO/IEC 17799 as Code of practice for Information Security Management in 2000; this document was reproduced to ISO/IEC 27001 ISMS requirements in 2005. The 2005 version of the standard was extensively revised in 2013, it became generic with more flexibility and some controls were added or changed in the new and current version of the standard. Part of the aim of this review is to trace the development of the literature within the life of the standard from its introduction in 2005.

RQ3. What are the limitations of the current research? Another aim of this paper is to critically analyse the effects of the current literature in comparison with the requirements of the standard and whether the literature provides sufficient contribution to facilitate the use of the standard for organisations.

B. Search process

Each journal and conference proceedings were reviewed and assessed by the first author, however, the papers that addressed literature of any type identified as included or excluded were discussed with the other researchers. The researcher responsible for searching the journal or conference applied the detailed inclusion and exclusion criteria to the relevant papers. The automated search strategy was followed in our research to identify the primary studies. The electronic libraries used were:

- Google Scholar
- IEEE Xplore
- Springer
- Science Direct
- Research Gate
- British Library EThOS
- ACM Digital Library
- Abstracts in New Technologies and Engineering
- Web of Science

As part of the literature studies, certain keywords and synonyms were established and included in the research. We worked on keywords and terms that these studies use to specify essential concepts of relevance to ISMS. For the retrieval in the digital libraries, a sophisticated search string was constructed using Boolean ANDs and ORs. The string given below was derived and taken as a basis to apply to the title, keywords, and abstracts of publications:

(('iso/iec 27001 standard' OR 'information security management systems' OR 'isms' OR 'information security standard' OR 'security standard') AND ('requirements engineering' OR 'compliance engineering' OR 'security requirements engineering' OR 'software engineering'))

The above search strings were assessed using the applicable elements from Peer Review of Electronic Search Strategies (PRESS) checklist by McGown et al. [15]. The validation results obtained from the PRESS assessment are set out in Table I. Some electronic libraries did not provide advanced search options that allow for the use of the search string as is. For these sites, we either extended the context of the search or separated the search into several sub-searches preserving the initial search context. The selection of primary studies was governed by the inclusion and exclusion criteria.

TABLE I. Elements from PRESS checklist

No	PRESS Element	Result
1	Are the search concepts clear?	Yes
2	Does the search string match the research question?	Yes
3	Are there any mistakes in the use of Boolean or nesting?	No
4	Are the subject headings relevant?	Yes
5	Are the subject headings missing?	No
6	Are any subject headings too broad or too narrow?	No
7	Does the search miss any synonyms?	No
8	Does the full term included for the abbreviation used?	Yes
9	Are there any spelling errors?	No
10	Are any filters used appropriate for the topic?	Yes
11	Are any potentially helpful limits or filters missing?	No

C. Inclusion and exclusion criteria

Peer-reviewed articles on the the following topics were included:

- An article published between 01 Jan 2005 and 30 June 2018: we wanted to cover the years that both versions of the standard published in 2005 and 2013, hence, it is fair to cover from the start of 2005 until the current date.
- An article should discuss the search string described in Section II-B.
- An article should propose a software engineering technique in addressing the standard: the aim of this paper is to capture the contributions from the field of software engineering.

Articles on the following topics were excluded:

- An article that is not written in English.
- White papers or informal articles: not peer-reviewed papers or articles, which provide a plain description of the standard rather than purposing a technicality were excluded.
- Duplicate reports of the same study: when several reports of a study exist in different journals the most complete version of the study was included in the review.

D. Data collection

This review does not claim to have captured every approach within the ISMS, however, the aim of this review is to have a holistic comprehension of the current state of the art in the ISMS. We recognise there could be a number of other related approaches that consider other ISMS methodologies such as ISACA COBIT or NIST Cybersecurity Framework, however, the intention of this paper is ISO/IEC 27001 standard and to achieve a fairly detailed conclusion within this topic.

The information extracted from the selected studies must reflect our research questions and indicate a desirable contribution towards the ISO/IEC 27001 standard. The initial studies of 285 papers were converged by learning their meta-data including title, abstract, keywords, and conclusion. A total of 95 papers met our objectives and aims of this review, which led us to further investigate the full text of a study. Finally, 21

papers were selected as primary studies for in-depth evaluation and participation in our review paper.

The order of reporting the primary studies in the next section is in chronological order and for the purpose of fairness and accuracy, the same amount of information about each selected study was extracted. The data extracted from each study were:

Approach title: This is a proposed title by the authors of a primary study for his/her approach or contribution. If a title was not available then we referred to the first author's full name.

Year of publication: The year when the paper was published. If a paper was published in several different sources both dates were recorded and the first date was used in any analysis.

Type: Each primary study was categorised into two terminologies including Framework or Method, the definition used for each is as follow:

- Framework: This is a process or conceptual layered structure intended to serve as a support or guideline for the building of something useful [16].
- Method: It refers to the methods the researchers use in performing an operation [17].

Scope: The scope equally measures the contribution of a study towards the PDCA model. The four stages include:

- 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.

Findings and practical implications: This term refers to analysis, discussion, results, and identification of outcomes and implications for practice in the primary studies. In case of duplicate publications, the most completed paper among those was used by referring to the versions of the report to obtain all the necessary data.

E. Data analysis

A set of 22 criteria as described in Table II were excerpted from the clauses and sub-clauses of the ISO/IEC 27001:2013 standard to compare and evaluate the identified studies.

The standard specifies the requirements for establishing, implementing, maintaining and continually improving an ISMS within the context of the organisation. Excluding any of the requirements is not acceptable when an organisation claims conformity to this standard, hence, a similar approach is used to measure the level of fulfilment to all requirements of the standard by each identified study.

The same definition for each criterion as specified in the standard [18] is followed, to allow the established uniform description used in our review and to avoid misinterpretation or misjudgement. These criteria were selected from the current version of the standard published in 2013, however, it is recognised that majority of the literature was published prior to 2013, therefore, a formal mapping [19] of ISO/IEC 27001:2013 clauses to ISO/IEC 27001:2005 version were used to ensure that papers published prior to 2013 are not disadvantaged in comparison with papers published post 2013.

The order in presenting the criteria do not reflect their importance or imply their implementing order; the list items are enumerated for reference purpose only.

III. Results

The following summarises the result of our review from the selected studies under the keywords that this research interested to investigate.

Chang and Ho proposed a model [20] [21] to explore the influence of organisational factors on the effectiveness of implementing the BS7799 (replaced by ISO/IEC 27001) standard. The findings defined four factors that could cause a serious impact on the success of the implementation of the information security management, they included IT competence of business managers, environmental uncertainty, industry type, and organisational size. The impact of these factors could be varied between any types of organisations. The findings indicate large organisations may benefit more in implementing information system security standards since they are more depended on formalisation and standardisation than small companies and have a greater amount of assets. Their studies were limited as only targeted 59 organisations in Taiwan but it was expected to have a similar result for another region too.

Mellado et al. proposed Security Requirements Engineering Process (SREP) [22] [23] to incorporate security requirements such as Common Criteria (ISO/IEC 15480) into the software life cycle model in a structured process. SREP used a collection of standards, processes and activities for the development of secure information systems under a systematic approach. The framework was made up of nine activities known as micro-process to form the security requirements engineering, as well as the external and visible artefacts that involve the activities. The activities included the determination of the security vision, understanding of the stakeholders, the identification of the vulnerabilities and assets, identification of security objectives and threats, risk assessment, the elicitation-prioritisation- inspection of security requirements and the repository improvement.

Anwar et al. proposed Preventive Information Security Management (PrISM) [24] system, a model to advance the security assurance and risk handling process in an ISMS with intrusion prevention capabilities. PrISM developed a network security solution including a number of services and functionalities, such as intrusion, detection and prevention capability, integrity checks, incident management and managerial reporting. The above could be incorporated in a single control panel to enable the integration, summarising and linking all the tools and functionalities together. This could assist with automating incident handling and other tasks, which could minimise the operational risks within organisations using comprehensive security monitoring.

Fenz et al. proposed OntoWorks [25] [26], which is an ontological mapping of the ISO/IEC 27001 standard supporting the certification process. Authors proposed a framework to use ontological data and enable users to access, visualise,

TABLE II. Criteria from the ISO/IEC 27001 Standard

No	Criterion	Description
1	Organisational context	Define the external and internal parameters and issues affecting the outcome of ISMS.
2	Interested parties	Identify the interested parties and their information security requirements relevant to the ISMS.
3	Determining the scope	Identify the logical or physical boundaries and applicability of the ISMS
4	ISMS	Establish, implement, and continually improve an ISMS under the requirements of the standard.
5	Leadership	Top management to demonstrate leadership and commitment with respect to the ISMS that are compatible with the strategic direction of the organisation.
6	Policy	Establish directions and making references to IS objectives and appropriate to the purpose and context of the organisation.
7	Roles	Top management to assign and communicate the responsibilities and authorities relevant to information security for reporting performance of the ISMS within the organisation.
8	Risk & opportunities	Systematically determine the potential risks and opportunities that may be involved in a projected activity or undertaking.
9	Information security objectives	Define measurable information security objectives.
10	Resources	Identify the resources needs to manage the ISMS.
11	Competence	Identify the necessary ability of a persons knowledge and skills doing work under its control that affects information security performance.
12	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.
13	Communication	Apply internal and external communication process relevant to the ISMS.
14	Documented information	Create, update, and control documented information required by the standard and necessary for the effectiveness of the ISMS.
15	Operational planning	Plan, implement and control the process needed to meet information security requirements including risk and opportunities, and information security objectives.
16	IS risk assessment	Perform security risk assessment.
17	IS risk treatment	Implement information security risk treatment.
18	Monitoring & measurement	Evaluate the information security performance and its effectiveness.
19	Internal audit	Conduct regular internal audits and systematically evaluate the effectiveness of the implemented and maintained ISMS.
20	Management review	Top management to review the organisation ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness.
21	Nonconformity & corrective action	React and evaluate nonconformity occurrences, review and deal with appropriate corrective actions.
22	Continual improvement	Recurring activity to continually improve the suitability, adequacy and effectiveness of the ISMS.

and reason on ontological data. Their contribution helped for audit preparation and rule-based compliance checks regarding ISO/IEC 27001 controls. As some of the operations delivered as partial automation, this will increase the automation process within the certification process, resulting in saving costs and resources. Fenz et al. [27] later proposed security ontology to be used to increase the efficiency of the compliance checking process by introducing a formal representation of the ISO/IEC 27002 standard.

Mellado et al. proposed Security Requirements Engineering Process for Software Product Lines (SREPPLine) [28], [29], this was a solution for managing security requirements at an early stage of the product line development driven by security standards. This framework was structured management of the security requirements to facilitate the conformance of the software product line products to relevant security standards such as ISO/IEC 27001 and ISO/IEC 15408. The proposal consisted of two sub-process including the product line security domain engineering and the product line security application requirements engineering. These sub-processes responsible for four phases of requirements engineering, such as requirements elicitation, requirements analysis and negotiation, requirements documentation, and requirements validation and verification. Mellado et al. [30] later used Secure Tropos framework for Software Product Lines requirements engineering for elicitation of security requirements and their analysis on both a social and technical dimensions.

Boehmer proposed a methodology [31] [32] to measure the effectiveness of the implementation and operation of an ISMS in organisations. The methodology delivered a solution to form an assessment through audits checking of the internal controls. Internal controls included administrative controls, physical controls, and technical controls.

Mayer proposed Information System Security Risk Management (ISSRM) [33] [34] [35], providing 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.

Ekelhart et al. proposed AUtomated Risk and Utility Management (AURUM) [36] [37], a risk management methodology to support the NIST 800-30 risk management standard. The methodology focused on the risk management approach by conducting various techniques such as questionnaires, on-site interviews, document reviews, and automated scanning tools to gather the required information under an ontological framework. AURUM provides risks assessment management by understanding the organisation characterisation followed by vulnerability identification, threat identification, risk likelihood determination, control analysis, control recommendations with appropriate controls, cost/benefit evaluation, impact analysis, modelled and taken from best practise standards such as the IT Grundschutz. This is a methodology for supporting information security risk management through modelling the organisation's assets within an ontological framework.

Valdevit et al. proposed an approach [38] [39] on how to adopt ISO 27001 on SMEs and their specific needs in implementing the ISMS. They developed their approach to knowledge gained in SMEs for several years in several disciplines and sectors. This was an approach where researchers

and practitioners work together, towards a number of activities including problem diagnosis, active intervention, and reflective learning. Authors described their approach as a "blend of theoretical reviews and experiments".

Hensel and Lemke-Rust proposed an approach [40] of Braun [41] to business engineering was chosen for the integration of ISO/IEC 27001 into an enterprise architecture. Authors integrated an ISMS into a systematic business engineering. The approach consisted of four layers such as strategic layer considered the internal and external requirements of an organisation and its strategic alignment; organisation layer considered the overall organisation process vision and defines the roles and responsibilities of the ISMS; the information system layer considered the information assets and information architecture of the organisation including software component and platform view; infrastructure and technology layer considered the infrastructure used for conducting a risk analysis of an ISMS.

Schneider et al. proposed Heuristic Requirements Assistant (HeRA) [42], an assistant tool to enable the identification and analysis of security requirements by applying experience-based tool rather than dependency on experts. An approach to provide knowledge about security best practises to developers and designers with limited experience. This approach is based on modelling the flow and enabling the stakeholders to exchange, learning and reusing relevant experiences about security requirements at the project requirements level.

Muller et al. introduced a tool [43] [44] to supports cloud service providers and consumers under a security management platform. A Security Management Platform (SMP) to specify the security requirements and measure the effectiveness of implemented controls for cloud service providers and consumers to conjointly manage information security. The system management platform consisted of three steps: service provider and consumer identify the security requirements for a cloud service in order to prepare a specific service level agreement based on agreed requirements, service provider manage and maintain the implementation and operation of security controls in a traceable and transparent manner, service provider is responsible to measure the specified requirements, identified in the first step and periodically to generate reports and incident reports about implemented controls to stakeholders.

Gillies proposed 5S2IS [45], an approach to facilitate SMEs to implement and comply with ISO/IEC 27000 standard. The proposed approach developed a two-dimensional matrix with the use of ISO/IEC standard and the Capability Maturity Model (CMM). It included draw up a plan to understand the organisation expectation and achieve the ISMS, define policies and processes to reach the organisation goals, identify the non-compliances with the goals through measurement, analyse and identify the growth and improvement of performance through monitoring, embed the ISMS in the organisation and plan to attain for certification if applicable.

Susanto et al. proposed Integrated Solution Framework (I-SolFramework) [46] [47] [48] to assesses the readiness level of an organisation towards the implementation of ISO 27001. The framework offered e-assessment and e-monitoring to analyse and performed an assessment of the readiness level of ISO 27001 implementation. E-assessment measure ISO 27001 parameters based on the framework; it consisted of six layers component including organisation, stakeholder, tools and technology, policy, culture and knowledge with 21 controls. It helped to validate the ISO/IEC 27001 parameters through an analytical interface such as histogram, charts and graphs, provided by a framework.

Montesino et al. proposed Security Information and Event Management (SIEM) [49]. A framework to enable the organisation to evaluate their compliance with IS standards and their implementation effectiveness by automatically generating ISO 27001 based on IT security metrics [50]. Authors findings indicated about 30% of the security controls of ISO/IEC 27001 standard can be automated. SIEM technology consisted of two main functions of security information management system, which handles the collection, reporting and analysis of log data; and security event management, which monitors real-time data and manages incident of security-related events. SIEM based solution is proposed to centralise and incorporate a list of ten automated controls including asset inventory, account management, log management, system monitoring, malware protection, vulnerability scanning and patch management, security configuration assessment and compliance checking, information backup, physical security, incident management.

Azuwa et al. proposed Supervisory Control and Data Acquisition (SCADA) [51] [52], An approach to measure the effectiveness of network security management in SCADA. This method specifically assisted to enable a measurement approach to the effectiveness of ISO/IEC 27004 measurement standard. It initially identifies security controls followed by a risk management approach to develop risk-based requirements and prioritisation of security control implementation. This step included the identification of threats and vulnerabilities and their impacts. The third stage was to develop an effective measurement and metric through questionnaires and interviews, perception and experts knowledge, certified organisations and SCADA owners.

Beckers et al. proposed a methodology [53] [54] to analyse security requirements engineering methods to support the development and documentation of an ISMS according to ISO/IEC 27001. Authors described the aims to improve the result of ISO 27001 implementation through proper establishment and documentation of an ISMS.

Chatzipoulidis et al. proposed a risk management approach [55] called "to be" environment by focusing on analysing threats, evaluating and treating vulnerabilities in the information society. The author described information society as a dynamic information security management system and proposed a concept to enhance the role of e-government to support public administration and cognitive resource for policymakers. The "to be" environment methodology identified risks by characterising the elements of risks and summarising critical threats of cyberbullying and cyberstalking attack patterns; identification of risk by analysing cultural dynamics and assessment of the current and planned controls of the system in place; evaluation of risk by producing a list of critical risks, prioritised based on set criteria; and risk treatment to lessen risks to meet the risk appetite level.

Asosheh et al. proposed a framework [56] for implementing an ISMS within a large-scale enterprise to assist them in identifying related activities in establishing and implementing an ISMS including the risk assessment and treatment procedures. The process consisted of five steps according to

ISO/IEC 27003 implementation guidance such as obtaining management approval for initiating the ISMS project. The steps included a preliminary scope identification and preparing definitions for ISMS and a business plan to have the management approval. Defining ISMS scope, boundaries and ISMS policy, which helps to produce a final document to set the boundaries for the ISMS policy and scopes, conducting information security requirements analysis that aims to identify assets and needs of asset owners, and risk management.

Beckers et al. proposed PAttern-based method for establishing a Cloud specific informaTion Security management system (PACTS) [57] [58] [59] [60]. An approach for creating an ISMS methodology compliance to the ISO 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 [61] [62], an extension of the COROS method to support the establishment of an ISO/IEC 27001 compliant ISMS. Authors proposed a methodology following CORAS method. CORAS is a risk management methodology based on the ISO 31000 standard, therefore, providing compliance to ISO 31000 standard, consideration of legal concerns tool support for document generation. CORAS-ISMS support security management compliant with ISO/IEC 27001 standard.

IV. Discussion

In this section, we discuss the answers to our research questions described in Section II-A.

RQ1. What are the software engineering approaches that organisations could use to apply or implement the requirements of the ISMS as defined by the ISO/IEC 27001 standard?

An overall description of the primary studies are shown in Table III where appending each study Title, Year of publication, Type of contribution indicating Framework (F) or Method (M), Scope(s) of the PDCA model covered by each study, and depth of fulfilment at each Stage of the Plan, Do, Check, and Act. A summary of each study was described in the previous section.

Our speculation with respect to the PDCA model is that very little attention is given at the Check stage where only five studies out of 21 provided contribution to the relevant part of the standard. Check specifically deals with assessment and measurement process performance against the ISMS.

Act stage tends to have less to almost no contribution where only one study out of 21 identified to address the relevant part of the standard. Act maintains and improves an ISMS by taking corrective actions where nonconformities occur. Interestingly, even some of the proficient concepts like ISMS-CORAS or ISSRM did not target any of the named stages of the standard in their studies.

RQ2. What are the scholarly contributions to the literature since the introduction of the ISO/IEC 27001 standard in 2005?

The chart in Figure 2 depicts the overall fulfilment percentage of each study towards the requirements of the standard in chronological order from 2005 to 2018.

TABLE III. Overall description of primary studies

Title	Year	Type	Plan	Do	Check	Act
Chang, Shuchih Ernest	2006	M	+	-	-	-
SREP	2007	F	+	+	-	-
PrISM	2007	M	-	-	+++	++
OntoWorks	2007	F	-	+	++	-
SREPPLine	2008	F	++	+	-	-
Boehmer, Wolfgang	2008	M	+	+	-	-
ISSRM	2008	M	++	+++	+	-
AURUM	2009	M	+	++	-	-
Valdevit, Thierry	2009	M	+	-	-	-
Hensel, Veselina	2010	M	+	++	-	-
HeRA	2011	M	+	-	-	-
SMP	2011	F	+	-	++	-
5S2IS	2011	F	+	+	++	-
I-SolFramework	2012	F	++	-	-	-
SIEM	2012	F	-	+++	-	-
SCADA	2012	M	-	++	-	-
Beckers, Kristian	2012	M	+	+	-	-
"to be" environment	2013	M	+	++	-	-
Asosheh, Abbass	2013	M	+	+++	-	-
PACTS	2013	M	++	++	-	-
ISMS-CORAS	2013	F	++	+++	-	-

Note:
F = Framework
M = Method
- = Not fulfilled
+ = Partially fulfilled = Number of criteria per scope:
Plan [1-5], Do [1], Check [1], Act [1]
++ = Mostly fulfilled = Number of criteria per scope:
Plan [6-10], Do [2], Check [2], Act [1]
+++ = Fulfilled = Number of criteria per scope:
Plan [11-14], Do [3], Check [3], Act [2]

The trend indicates the current studies are fragmented and it is a challenging task for organisations to benefit from the current literature. Alternatively, they require to apply a number of studies in conjunction with each other that may result to an inconsistent, unmanageable, and intractable output. Whilst the existing work could help with rather smaller sections of the standard and used as a point of reference but they are inadequate to realise the full requirements of the standard.

Our findings suggest that the majority of studies proposed between 2005 to 2018 are incomplete and they mostly provide a partial fulfilment to the requirements of the ISO/IEC 27001 standard. This review provides evidence with respect to a gap in the field of the ISMS.

The graph in Figure 3 reveals that a reasonable quantity of the studies were produced between 2006-2008, after the publication of the first version of the standard in 2005; the attention dropped until around 2010.

Half of the studies carried out between 2011 to 2013 and it appears the consideration to the ISMS was higher prior to the publication of the second version of the standard in 2013 than after. This shows an inconsistent and contradicts association between the first version and the second version of the standard. A possible explanation could be the fact that other standard documents in the family of ISO/IEC 27000 were revised and published between 2011-2013, such as a revised publication of ISO/IEC 27003 in 2010, ISO/IEC 2005 in 2011, ISO/IEC 27006 in 2011, ISO/IEC 27007 in 2011, ISO/IEC 27008 in 2011.

The most striking result to emerge from the data is that the expansion of further research dropped sharply after 2013 and no study was detected after the revised publication of the standard in 2013, which should have caused some spark in

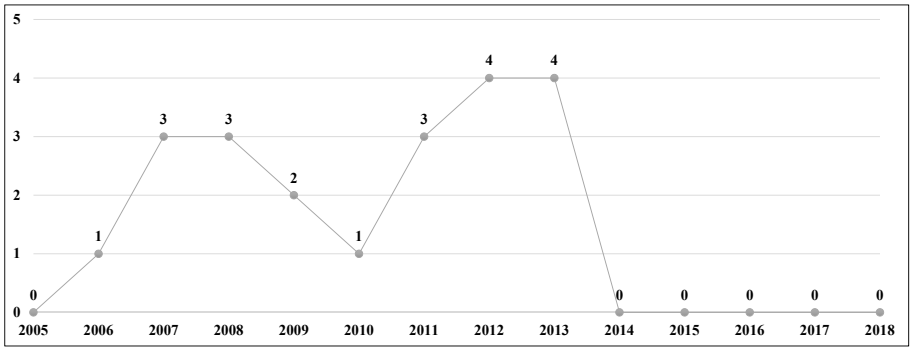

Figure 2. Overall fulfilment of each study towards the requirements of the ISO/IEC 27001 standard in (%)

academia. It is interesting to note that almost all papers (20) were published between 2007 to 2013.

RQ3. What are the limitations of the current research?

Table IV demonstrates a detailed review of all 21 studies and their contribution at each criterion identified in the previous section; It provides the overall strength and limitation of the study. The indicative asterisk (*) in the table denotes the fulfilment of a criterion.

On average, some criteria are shown to have attracted the majority of the literature than others. The areas where significant differences have been found include Organisational context (1), Interested parties (2), Determining the scope (3), Documented information (14), Operational planning (15), and Information security risk assessment (16).
On the other hand, little to no evidence of some criteria was detected such as Leadership (5), Policy (6), Resources (10), Competence (11), Awareness (12), Communication (13), Monitoring and measurement (18), Internal audit (19), Management review (20), Nonconformity and corrective action (21), and Continual improvement (22).

The results in the previous section indicated that far too little attention has been paid to address all or most requirements of the standard. Whilst some research were produced in years in question, but only two studies attempted to investigate the ISMS at a proficient level, which meeting between 10 to 14 criteria out of 22. No study was found to reach the advanced level, meaning to support more than 15 criteria out of 22. The evidence affirms that the majority (57%) of the selected studies are at the developing stage, which means they are only able to fulfil up to four (18%) requirement of the standard.

The average fulfilment rate of all the 21 studies is 23% which is equivalent to five out of 22 requirements. Excluding any of the 22 requirements specified in Table II is not acceptable when an organisation claims conformity to the standard. Taken together, the current studies are incomplete and the current literature requires further expansion. The number of studies at each category stands as below:

Basic = 7	Developing = 12
Proficient = 2	Advanced = 0

This interpretation contrasts with findings in Table III which provide detailed results about the scope of each study at the PDCA model.

A considerable number of studies mostly fulfil the requirements of the Plan (26%) and Do (52%) stages, whilst, very few studies attempted to address Check (19%) and Act (3%) stages. Additionally, it reveals that nearly two-thirds of papers were considered as a Method whereas only seven papers were identified as a Framework. It is also worth noting that a distinct number of other papers which were dismissed during the selection process and not considered for the purpose of this systemic literature review were identified as Method.

A note of caution is due here since not every study selected as part of our review claimed to specifically meet each and every requirement of the standard and it could be argued that those study only focused on the indicated criteria, however, this suggests that there is a rudimentary gap in the knowledge.

V. Conclusion

ISO/IEC 27001 standard provides mapping for establishing, implementing, maintaining, and continually improving an information security management system. It is a strategic decision for organisations to adopt ISMS and systematise the security demands rather than doing it ad hoc.

The aim of this paper is to systematically investigate the approaches, which assist organisations to develop, implement, and comply with the ISMS as defined by the standard published between 2005 to 2018. The review examined the approaches, which are thought to contribute to the requirements of the ISO/IEC 27001 standard.

The results of this study indicate that there is no concept that facilitates organisations in designing and complying with the ISO/IEC 27001 standard, this means covering all the 22 requirements of the standard. The result indicates that a very limited number of studies attempted to investigate the ISMS at the proficient level which meets at least half of the requirements of the standard. No study was found to address all parts of the ISMS. The average fulfilment rate of all 21 studies is 23% which is equivalent to addressing up to 5 out of 22 requirements.

The majority of the primary studies were produced prior to the 2013 and the current literature requires attention in expanding, promoting, and the introduction of techniques to organisations and enable them to achieve and strategically integrate their organisational goals with their information security objectives.
The most obvious finding to emerge from this study is that substantial potential exists for academic researchers to investigate the ISMS under a holistic approach. The current literature

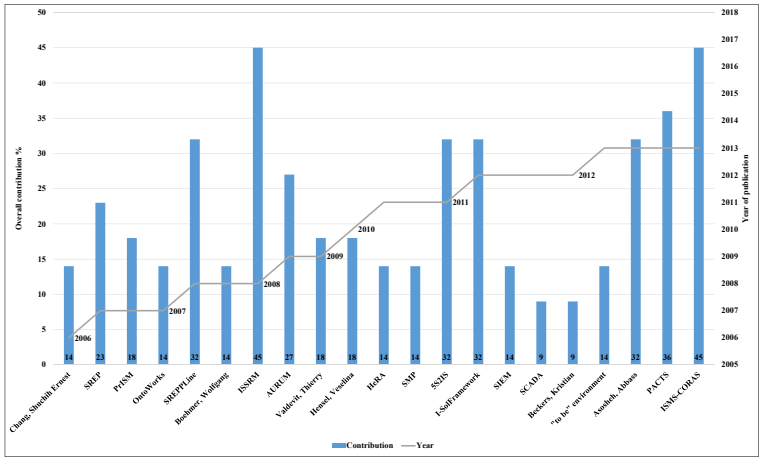

Figure 3. Timeline comparison of each study in (%)

TABLE IV. Detailed view of the studies

Title	Plan														Do			Check			Act		Overall
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	
Chang, Shuchih Ernest	*	*									*												Developing
SREP	*	*						*	*							*							Basic
PrISM																		*	*	*		*	Developing
OntoWorks															*			*	*				Developing
SREPPLine	*	*	*				*	*	*							*							Basic
Boehmer, Wolfgang								*	*						*								Developing
ISSRM	*	*	*				*	*	*						*	*	*			*			Proficient
AURUM	*	*						*	*							*	*						Basic
Valdevit, Thierry	*		*									*		*									Developing
Hensel, Veselina	*	*														*	*						Developing
HeRA	*	*		*																			Developing
SMP														*				*		*			Developing
5S2IS	*		*		*				*						*			*		*			Basic
I-SolFramework	*	*	*			*		*		*	*												Basic
SIEM															*	*	*						Developing
SCADA															*	*							Developing
Beckers, Kristian														*		*							Developing
"to be" environment								*								*	*						Developing
Asosheh, Abbass	*			*				*	*						*	*	*						Basic
PACTS	*	*		*	*			*						*	*	*							Basic
ISMS-CORAS	*	*	*	*				*	*					*	*	*	*						Proficient

Note:
Developing = Fulfil up to 4 criteria out of 22
Basic = Fulfil between 5 to 9 criteria out of 22
Proficient = Fulfil between 10 to 14 criteria out of 22
Advanced = Fulfil more than 15 criteria out of 22

lacks motivation in purposing new initiatives in the field of the ISMS and ISO/IEC 27001 standard.

In the absence of the knowledge in the literature, there is abundant room for further progress in determining a technique which, could handle the ISMS under a unified approach. The evidence from this review suggests that there is a gap in the current approaches to satisfy the requirements of the ISO standard and fresh and comprehensive approaches are beneficiary and recommended in advancing the ISMS.

Future research should be carried out to examine more closely the links between all four scopes of the PDCA model. More research is needed to develop a deeper understanding of the relationships between ISO/IEC 27001 standard and requirements engineering and greater efforts are required to ensure that future approaches to account for all requirements of the standard.

REFERENCES

[1] D. Ganji, H. Mouratidis, and S. Malekshahi Gheytassi, "Towards a Modelling Language for Managing the Requirements of ISO/IEC 27001 Standard," in 5th International Conference on Advances and Trends in Software Engineering (SOFTENG). Valencia, Spain: IARIA, 2019, pp. 17–23.

[2] J. P. Laudon and K. C. Laudon, Essentials of MIS, global edition, 12th ed. Pearson Higher Education & Professional Group, 2016.

[3] E. Targett, "6 months, 945 data breaches, 4.5 billion records," 2018, (Accessed: 2019-11-01). [Online]. Available: https://www.cbronline.com/news/global-data-breaches-2018

[4] The Breach Level Index, "Data breach database," (Accessed: 2019-11-01). [Online]. Available: https://breachlevelindex.com/data-breach-database

[5] K. C. Laudon and J. P. Laudon, Management information systems: managing the digital firm, 10th ed. Pearson Higher Education & Professional Group, 2007.

[6] International Organization for Standardization, "ISO/IEC 27001

Information security management," (Accessed: 2019-11-01). [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html

[7] International Organisation for Standardisation, "The ISO survey of management system standard certifications 2017," International Organisation for Standardisation, Geneva, Switzerland, Tech. Rep., 2017.

[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] B. A. Kitchenham, "Guidelines for performing systematic literature reviews in software engineering," Keele University, Keele, UK, Tech. Rep., 2007.

[10] ——, "Procedures for performing systematic reviews," Keele University, Keele, UK, Tech. Rep., 2004.

[11] J. Webster and R. T. Watson, "Analyzing the past to prepare for the future: writing a literature review," MIS Quarterly, vol. 26, no. 2, 2002, pp. xiii–xxiii.

[12] "ISO 27001 global report," IT Governance, Tech. Rep., 2016.

[13] E. Coles-Kemp, "The anatomy of an information security management system," Ph.D. dissertation, King's College London, University of London, 2008.

[14] 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.

[15] J. McGowan, M. Sampson, and C. Lefebvre, "An evidence based checklist for the peer review of electronic search strategies (PRESS EBC)," Evidence Based Library and Information Practice, vol. 5, no. 1, 2010, pp. 149–154.

[16] M. Rouse, "Framework," 2015, (Accessed: 2019-11-01). [Online]. Available: http://whatis.techtarget.com/definition/framework

[17] C. R. Kothari, Research methodology: methods and techniques. New Age International Publishers, 2004.

[18] "ISO/IEC 27001:2013 Information technology - security techniques - information security management systems - requirements," International Organization for Standardization, Geneva, Switzerland, Tech. Rep., 2013.

[19] British Standard Institution, "Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013," British Standard Institution, Tech. Rep., 2014.

[20] S. E. Chang and C. B. Ho, "Organizational factors to the effectiveness of implementing information security management," Industrial Management & Data Systems, vol. 106, no. 3, 2006, pp. 345–361.

[21] S. E. Chang and C.-S. Lin, "Exploring organizational culture for information security management," Industrial Management & Data Systems, vol. 107, no. 3, 2007, pp. 438–458.

[22] D. Mellado, E. Fernandez-Medina, and M. Piattini, "A common criteria based security requirements engineering process for the development of secure information systems," Computer Standards & Interfaces, vol. 29, 2007, pp. 244–253.

[23] ——, "A comparison of the common criteria with proposals of information systems security requirements," in 1st International Conference on Availability, Reliability and Security. Vienna, Austria: IEEE, 2006.

[24] M. M. Anwar, M. F. Zafar, and Z. Ahmed, "A proposed preventive information security system," in 2007 International Conference on Electrical Engineering. Lahore, Pakistan: IEEE, 2007, pp. 1–6.

[25] S. Fenz, G. Goluch, A. Ekelhart, and E. Weippl, "Information security fortification by ontological mapping of the ISO/IEC 27001 standard," in Pacific Rim International Symposium on Dependable Computing. Melbourne, Victoria, Australia: IEEE Computer Society, 2007, pp. 381–388.

[26] S. Fenz, "Ontology-based generation of IT-Security metrics," in ACM Symposium on Applied Computing. Sierre, Switzerland: ACM, 2010, pp. 1833–1839.

[27] S. Fenz, S. Plieschnegger, and H. Hobel, "Mapping information security standard ISO 27002 to an ontological structure," Information & Computer Security, vol. 24, no. 5, 2016, pp. 452–473.

[28] D. Mellado, E. Fernandez-Medina, and M. Piattini, "Security requirements variability for software product lines," in 3rd International Conference on Availability, Reliability and Security. Barcelona, Spain: IEEE, 2008, pp. 1413–1420.

[29] ——, "Towards security requirements management for software product lines: a security domain requirements engineering process," Computer Standards & Interfaces, vol. 30, 2008, pp. 361–371.

[30] D. Mellado, H. Mouratidis, and E. Fernandez-Medina, "Secure Tropos framework for software product lines requirements engineering," Computer Standards & Interfaces, vol. 36, no. 4, 2014, pp. 711–722.

[31] W. Boehmer, "Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001," in 2nd International Conference on Emerging Security Information, Systems and Technologies. Cap Esterel, France: IEEE, 2008, pp. 224–231.

[32] ——, "Cost-benefit trade-off analysis of an ISMS based on ISO 27001," in International Conference on Availability, Reliability and Security. Fukuoka, Japan: IEEE, 2009, pp. 392–399.

[33] N. Mayer, P. Heymans, and R. Matulevicius, "Design of a modelling language for information system security risk management," in 1st international conference on research challenges in information science. Ouarzazate, Morocco: IEEE, 2007, pp. 121–132.

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

[35] ——, "A cluster approach to security improvement according to ISO/IEC 27001," in 17th European Systems & Software Process Improvement and Innovation. Grenoble, France: Springer-Verlag Berlin Heidelberg, 2010.

[36] A. Ekelhart, S. Fenz, and T. Neubauer, "AURUM: a framework for information security risk management," in 42nd Hawaii International Conference on System Sciences. Big Island, HI, USA: IEEE, 2009, pp. 1–10.

[37] ——, "Ontology-based decision support for information security risk management," in Fourth International Conference on Systems. Gosier, Guadeloupe, France: IEEE, 2009, pp. 80–85.

[38] T. Valdevit, N. Mayer, and B. Barafort, "Tailoring ISO/IEC 27001 for SMEs: a guide to implement an information security management system in small settings," in Software Process Improvement: 16th European Conference, EuroSPI, vol. 42. Alcala (Madrid), Spain: Springer, Berlin, Heidelberg, 2009, pp. 201–212.

[39] T. Valdevit and N. Mayer, "A gap analysis tool for smes targeting ISO/IEC 27001 compliance," in 12th International Conference on Enterprise Information Systems, Funchal, Madeira - Portugal, 2010, pp. 413–416.

[40] V. Hensel and K. Lemke-Rust, "On an integration of an information security management system into an enterprise architecture," in International Workshop on Database and Expert Systems Applications. Bilbao, Spain: IEEE, 2010, pp. 354–358.

[41] C. Braun, F. Wortmann, M. Hafner, and R. Winter, "Method construction - a core approach to organizational engineering," in ACM symposium on Applied computing. Santa Fe, New Mexico: ACM, 2005, pp. 1295–1299.

[42] K. Schneider, E. Knauss, S. H. Houmb, S. Islam, and J. Jurjens, "Enhancing security requirements engineering by organisational learning," Requirements Engineering, vol. 17, no. 1, 2012, pp. 35–56.

[43] I. Müller, J. Han, J.-G. Schneider, and S. Versteeg, "Tackling the loss of control: standards-based conjoint management of security requirements for cloud services," in 4th International Conference on Cloud Computing. Washington, DC, USA: IEEE Computer Society, 2011, pp. 573–581.

[44] ——, "Idea: a reference platform for systematic information security management tool support." in Engineering Secure Software and Systems. Madrid, Spain: Springer-Verlag Berlin Heidelberg, 2011, pp. 256–263.

[45] A. Gillies, "Improving the quality of information security management systems with ISO 27000," The TQM Journal, vol. 23, no. 4, 2011, pp. 367–376.

[46] 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.

[47] ——, "A novel method on ISO 27001 reviews: ISMS compliance readiness level measurement," Computer Science Journal, vol. 2, no. 1, 2012, pp. 19–29.

[48] 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, vol. 12, no. 01, 2012, pp. 20–28.

[49] R. Montesino, S. Fenz, and W. Baluja, "SIEM-based framework for security controls automation," Information Management & Computer Security, vol. 20, no. 4, 2012, pp. 248–263.

[50] R. Montesino and S. Fenz, "Automation possibilities in information security management," in European Intelligence and Security Informatics Conference. Athens, Greece: IEEE, 2011, pp. 259–262.

[51] M. P. Azuwa, R. Ahmad, S. Sahib, and S. Shamsuddin, "A propose technical security metrics model for SCADA systems," in International Conference on Cyber Security, Cyber Warfare and Digital Forensic. Kuala Lumpur, Malaysia: IEEE, 2012, pp. 70–75.

[52] M. P. Azuwa and R. Ahmad, "Technical security metrics model in compliance with iso/iec 27001 standard," International Journal of Cyber-Security and Digital Forensics (IJCSDF), vol. 1, no. 4, 2012, pp. 280–288.

[53] K. Beckers, S. Faßbender, M. Heisel, and H. Schmidt, "Using security requirements engineering approaches to support ISO 27001 information security management systems development and documentation," in 7th International Conference on Availability, Reliability and Security. Prague, Czech Republic: IEEE, 2012, pp. 242–248.

[54] K. Beckers, S. Faßbender, M. Heisel, J.-C. Kuster, and H. Schmidt, "Supporting the development and documentation of ISO 27001 information security management systems through security requirements engineering approaches," in 4th International Symposium on Engineering Secure Software and Systems. Eindhoven, The Netherlands: Springer, Berlin, Heidelberg, 2012, pp. 14–21.

[55] A. Chatzipoulidis, A. Belidis, and T. Kargidis, "A risk management approach to information society," The University of the Fraser Valley Research Review, vol. 4, no. 3, 2013, pp. 42–56.

[56] A. Asosheh, P. Hajinazari, and H. Khodkari, "A practical implementation of ISMS," in 7th International Conference on e-Commerce in Developing Countries with focus on e-Security, vol. 11. Kish Island, Iran: IEEE, 2013.

[57] 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.

[58] K. Beckers, M. Heisel, I. Côté, L. Goeke, and S. Güler, "Structured pattern-based security requirements elicitation for clouds," in International Conference on Availability, Reliability and Security. Regensburg, Germany: IEEE, 2013, pp. 465–474.

[59] K. Beckers, S. Faßbender, and M. Heisel, "A meta-model approach to the fundamentals for a pattern language for context elicitation," in 18th European Conference on Pattern Languages of Program. Irsee, Germany: ACM, 2013, p. 28.

[60] K. Beckers, H. Schmidt, J.-C. Kuster, and S. Faßbender, "Pattern-based support for context establishment and asset identification of the ISO 27000 in the field of cloud computing," in 6th International Conference on Availability, Reliability and Security. Vienna, Austria: IEEE Computer Society, 2011, pp. 327–333.

[61] K. Beckers, M. Heisel, B. Solhaug, and K. Stolen, ISMS-CORAS : A structured method for establishing an ISO 27001 compliant information security management system. Springer, Cham, 2014.

[62] K. Beckers, Supporting ISO 27001 establishment with CORAS. Springer, Cham, 2015.