Interdisciplinary Description of Complex Systems 17(3-A), 485-491, 2019

PARAMETERS AND GUIDELINES OF ENFORCEABLE INFORMATION SECURITY MANAGEMENT SYSTEMS

Sándor Dombora*

[1]Óbuda University, Kandó Kálmán Faculty of Electrical Engineering
Budapest, Hungary

DOI: 10.7906/indecs.17.3.7
Regular article

Received: 8 December 2018.
Accepted: 31 August 2019.

ABSTRACT

It is increasingly important for organizations to set up an Information Security Management System (ISMS) to fulfil their business interests and their legal compliance. The main purpose of these systems is to properly protect the information owned or managed by the organization. Often, the developed ISMS complies with the external regulatory environment, but contains unenforceable rules that impede work, so it is unable to fulfil its function. In order to prevent security incidents, it is not enough to ensure legal compliance. The enforceability of these policies is gaining increasing importance in order to avoid hindering work processes. This article identifies quality parameters and guidelines in order to improve quality, enable and improve enforceability of ISMS systems, in order to fulfil their purpose, mainly protection of company information assets. By adhering to these parameters and guidelines organisations can improve their ISMS systems which enforces security of their information assets.

KEY WORDS

information security, quality parameters, implementation directives, enforceable measures

CLASSIFICATION

ACM K.6.5
JEL: D83

*Corresponding author, η: dombora.sandor@kvk.uni-obuda.hu; +36 1 666-5140;
Institute of Communication Engineering, Kandó Kálmán Faculty of Electrical Engineering, Óbuda Univeristy, H – 1084 Budapest, Tavaszmező u. 15-17. Hungary

INTRODUCTION

Organizations collect, store and process a large amount of information to achieve their goals. Several companies gather more information than necessary to run their business operations. The information is collected, stored, accessed and processed by employees. The collected information is not only valuable for the organisation but for the competitors too. In some cases, the information may be interesting for a larger public as well. The data may contain confidential information, leakage of which may cause harm not only to the organisation but to partners, users and customers too.

The information processed by organisations can be grouped by different categories. Enterprises deal with information about: products, production, personnel, customers, partners, rules and regulations, workflows, design and development, research, quality management, organisation structure, business reports, etc. information.

Depending on the nature of the information, the legal environment may require the development of security policies and regulations, as well as the implementation of security measures. For example, personal data are protected by law everywhere in the world. First, however, the meaning of personal data must be specified. The term is defined by the law applicable in each geographic region. For example, in the European Union the meaning of personal data is defined by the General Data Projection Regulation (GDPR) [1], which may be complemented by the local laws of the EU member states.

Depending on the nature of the information collected, stored and handled by the organisations, it should be protected according to the business needs and the legal environment. Several factors govern the data protection needs of an organisation. The most important ones are the following:

- supporting production with availability of authentic information,
- ensuring information integrity to improve productivity and quality [2],
- avoiding fines, caused by law breaches (GDPR [1], sectoral legislation, Act CXII of 2011 on Information Self-Determination and Freedom of Information [3], Hungarian Act L of 2013 on Electronic Security of State and Local Government Bodies [4], etc.),
- ensuring the protection of sensitive information,
- management reports based on authentic data,
- using the market advantage of the ISO/IEC 27001 certification [5].

To achieve these goals, organisations need a functioning and enforceable ISMS. Articles describing the modelling of ISMS parameters have been identified [6], and the quality improvement based on ISO27000 has already been presented [7]. Other authors refer to the information security aspects related to process resource planning [8] and IT authorisation and Identity management [9]. These works suggest a need for an ISMS quality parameter and guidelines set to help organizations set up an operating ISMS system.

To further improve information security, this paper identifies a set of parameters and guidelines whose application greatly improve the quality and enforceability of ISMS.

RESEARCH METHOD

To identify quality parameters and guidelines for ISMS action research approach was used [10].

The first step of the research was to identify and categorize the problems which block enforcement of ISMS.

The second step was to define quality parameters and development guidelines to avoid building unenforceable ISMS. The result was a set of guidelines to follow and quality parameters to build into ISMS during development.

The third step was the implementation of an ISMS based on the developed guidelines and quality parameters in a large organisation which had several, smaller, loosely coupled subsidiaries with different information security needs.

In the last step, the developed guidelines and quality parameters were used to build several ISMS at different organisations. After a year of the ISMS implementation, these organisations were visited and interviews were made with stakeholders about the achieved result, which gave feedback and helped to improve the development guidelines and quality parameters.

THE MOST COMMON PROBLEMS OF ISMS AND THEIR CAUSES

Regarding the use of ISMS, different observations can be made. In some cases, the ISMS is developed in accordance with the applicable standards and laws, and it fulfils its function of information protection. There are cases when the ISMS is partially operational, and cases when it has no relevance to the organization, or it contains irrelevant data, too.

To identify the problems and their causes, the interviews were made with senior and middle management, and the people involved in the implementation and execution of the ISMS. By grouping, the responses received from stakeholders, categories of problems causes were identified. These categories are an inappropriate attitude of senior managers, inadequate development process, short deadline, copying other organisation's regulation, shortcomings in professional knowledge or consultancy.

By the analysis of problems related to structure, content, readability, applicability and compliance to the local and international legislation and the impact of regulations on organisations mainly the following types of shortcomings can be observed:

Problems regarding the ISMS structure:

- Almost all security rules are incorporated in one big regulation.
- All employees have to know and adhere to all security rules and regulations.
- The Information Security Regulation (ISR) contains several rules that are irrelevant to all of the employees.
- There is no role-based, segmentation of the ISMS.
- It is not clear which rules apply to individual employees.

Problems related to the content of the ISMS:

- The ISR contains general methodologies and descriptions instead of referencing them.
- The ISR it too long, up to hundreds of pages, and contains irrelevant information.

Problems related to the readability of ISMS:

- Reading the ISR takes a lot of time, and even if employees read it, they do not remember its content.
- It uses abbreviations and professional terminology, it is incomprehensible to many employees.

Problems regarding applicability of ISMS:

- The ISMS is confused and has overlapping regulations, nobody knows which rule should be applied.
- The ISMS contains contradictory rules.

- If the employees adhere to the ISMS rules, they cannot execute their diyly tasks, which stops the operation.
- The conditions (environmental, technical, economical, etc.) for execution of the ISMS are unavailable.
- The policy and regulation do not fit the operating environment.

Problems regarding compliance:

- Policies and regulations do not adhere to the legal environment.
- The ISMS is a modified version of a relevant laws or standard, but it stays theoretical, it is not integrated into the organisation workflows, it states but does not provide the required protection.

NEED FOR ENFORCEABLE ISMS

As today almost all organisations depend on information availability, confidentiality and integrity, the protection of information is a basic requirement. Failing to implement an operable ISMS is a high risk for organisations.

Analysing the problems shows that the implementation of a poorly designed ISMS, besides failing to protect the information, can cause security risks and hinders the operation of the organisation.

Furthermore, organisations should consider all the factors related to information security which affect operation and prosperity:

- The organisation's own interest in managing confidential information, providing accurate information to partners, customers and employess in order to improve organisation processes,
- Adherance to the legal environment, which enforces not only the compliance on a regulatory level, but the implementation of technical protection measures, too:
  - GDPR compliance cannot be ensured without operational ISMS and technical security measures;
  - The Hungarian Act L. of 2013 and its implementing regulation Ministry of Interior decree 41/2015. (VII. 15.);
  - Implementing information securtiy based on standards:
  - The ISO 27001 certification used to be a market advantage, but by now it has become a requirement;
  - The NIST Special Publication 800-53 helps to implement the technical controls related to information security [11].

CHARACTERISTICS OF ENFORCEABLE ISMS

When analysing ISMS problems, the following categories can be identified: inadequate structure, inadequate content, readability, applicability or compliance. By comparing the inoperable ISMS to the working ones, some characteristics can be observed, which help improve the quality and operability. The following parameter groups show these characteristics.

Compliance with current legislation and standards: this parameter group helps to match the legal requirements and standard's control system with the ISMS. In this category the following characteristics could be identified: building cross-references to the legal requirements, regulations and standards controls and tracking changes of these. Cross-references are needed to legal requirements and standard controls, in a way that helps to audit and verify the compliance. Without having these references it is hard to identify or match the elements of policies necessary to fulfil the external regulatory requirements, which may cause

failure in compliance. Tracking changes of external regulatory requirements generates input for updating the relevant documents of ISMS with reference to the given law and standard version. Usually, this is a process which alerts the stakeholders if relevant laws, regulations or standards are changing which imply policy updates in order to maintain compliance.

Up to date and consistent: these characteristics help to keep the ISMS consistent with business requirements and eliminate overlapping policies. Here the clear definition of policy scope, the documentation map, up to date cross-references and the single definition of terms and rules characteristics were identified. The clear scope and extent of regulations help to keep the ISMS policies consistent. The documentation map defines the scope of each policy and makes the ISMS transparent. The single definition of security rules and requirements makes them defined in only one place and referred from all other documents. The cross-references between documents, help to eliminate the overlaps while help locating related rules and definitions.

Understandable and interpretable: these characteristics make ISMS policies readable and unambiguous. In this category the clear, precise and understandable terminology and language were identified. The language of the policies must be precise, accurate and unambiguous. The security rules must not contain any uncertainty. Terminology and language of ISMS should be understandable by the target audience, even if they are not information security professionals.

Full and complete: these characteristics of the ISMS make the information protection to cover all relevant threats occurring in the organisation during execution of business processes. This means that security rules and requirements of ISMS must cover all relevant threats for the whole organisation, all departments and all employees executing workflows. The security rules and regulations must cover all the workflows of the organisation.

Necessary and sufficient rules: this is one of the most important characteristics group because this mainly influences the operability and the enforceability of the ISMS. The ISMS should provide the necessary protection level, which means the ISMS should have protection measures regarding all information assets ensuring the needed confidentiality, integrity and availability levels. This can be achieved by checking all relevant laws and standards and selecting all relevant requirements for the organisation, then developing and including the corresponding protection rules and measures in the ISMS. The more rules are built into ISMS, the more likely it is that they overlap, so keep minimal, remove unnecessary and merge overlappoing rules. Unnecessary and conflicting rules obstruct employees in executing their daily tasks. No textual parts of laws or standards should be included, they should be referenced instead. No methodology description should be included, they should be referenced, as they are regularly updated.

Hierarchical and role-based structure: the structure of the ISMS should be described in the documentation map to provide an overview of the whole regulation structure, which should be more than the cross-reference between the documents. All policies and regulations in the ISMS should be categorised, in policy, regulation, procedures and supporting documents categories. This helps to separate the diferent execution levels, however there is an interaction between these: the policy level governs the regulation level which drives the workflows producing the supporting documents. The different levels have their role and audience. The policy level contains the strategy and the policies according to which the organisation develops information security. The regulation level states the general security rules to be followed by the concerned departments and employees. The regulation level should be role-based, and the regulations should be available for the concerned departments and employees according to their role in the organisation. The procedure level should consist of

workflows for implementing and maintaining information security. The supporting documents describe setups, authorisation documents, system parameters, test results, maintenance records, incident records, problem records, change records, audit records, system parameters, etc. They are usually the results or the input of the workflows at the procedure level.

Enforceable and executable: to be able to operate the ISMS it is important to train employees, explain the structure and relationship of the policies, regulations, processes and supporting documents. In harmony with the necessary and sufficient rule characteristics these characteristics help minimising the necessary security knowledge of workers in different jobs. General security rules cover knowledge for all employees, must be covered by the Information Security Policy. Department specific rules must be covered by field security policies of the given departments. Activity related security rules must be incorporated into workflows and procedures. To be executable the overall rule system of the ISMS should not contain any conflicting and business process blocking rules. An employee needs to know only those policies, regulations and processes that affect them.

Balances risks and resources: organisations should consider the information security risks, and allocate the necessary resources based on these risks. The ISMS should consider the risks, the possible protection measures and their costs in order to allocate the necessary resources. taking into account the information security risks and resources available to the organization. This means that ISMS must not contain any security rules which imply protection measures that the organisation cannot finance.

CONCLUSIONS

Stevanovic [12] compares two information security standards, and in conclusions shows two essential differences: the implementation cost difference and the main focus of the standards: security and business result achievement. Implementing information security based on ISO 27001 standard in small and medium-sized organisation is not straightforward and needs guidelines [13]. Several inoperable and unenforceable ISMS caused unnecessary costs to the organisations while they left huge security gaps in the system. As external regulatory environment compliance is a must, resources are limited, costs are influenced by the security measures to be implemented, an enforceable risk-based ISMS can be the solution. To achieve this development guideline and quality parameters to improvement enforceability of ISMS were outlined. After implementing ISO/IEC 27001 based ISMS using the guidelines and parameters identified and presented in this article in more than 8 organisations, and getting feedback from them, the gudelines could be improved and the quality parameters could be refined. Therefore, these guidelines and quality parameters are suitable tools for the development of optimised, enforceable and risk-based ISMS. Keeping in mind them and incorporating into the regulation, organisations will be able to improve their ISMS quality and enforceability.

REFERENCES

[1] European Parliament: *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).*
Official Journal of the European Union **59**, 1-88, 2016**,**
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN,

[2] Barafort, B.; Humbert, J.P. and Poggi, S.: *Information Security Management and ISO/IEC 15504: the link opportunity between Security and Quality.*
In: 6th International SPICE Conference 2006. Proceedings of the SPICE 2006 Conference, Luxemburg, 2006,

[3] Hungarian Parliament: *Act CXII of 2011 on Information Self-Determination and Freedom of Information.*
Magyar Közlöny **88,** 25449-25482, 2011,
http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/mk11088.pdf,

[4] Hungarian Parliament: *Act L of 2013 on Electronic Security of State and Local Government Bodies.*
Magyar Közlöny **69,** 50241-50255, 2013,
http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/mk13069.pdf,

[5] ISO: *ISO/IEC 27001:2005, Information technology Security techniques - Information security management systems – Requirements*

[6] Chander, M.; Jain, S. and Shankar, R.: *Modeling of information security management parameters in Indian organizations using ISM and MICMAC approach.*
Journal of Modelling in Management **8**(2), 171-189, 2013,
http://dx.doi.org/10.1108/JM2-10-2011-0054,

[7] Gillies, A.: *Improving the quality of information security management systems with ISO27000*.
The TQM Journal **23**(4), 367-376, 2011,
http://dx.doi.org/10.1108/17542731111139455,

[8] Michelberger, P. and Horváth Zs.: *Security aspects of process resource planning*.
Polish Journal of Management Sudies **16**(1), 142-153, 2017,
http://dx.doi.org/10.17512%2Fpjms.2017.16.1.12,

[9] Keszthelyi, A. and Michelberger, P.: *From the IT Authorisation to the Role- and Identity Management.*
In: 4th IEEE International Symposium on Logistics and Industrial Informatics LINDI 2012. IEEE, Smolenice, pp.173-177, 2012,
http://dx.doi.org/10.1109/LINDI.2012.6319483,

[10] Avison, D.E.; Lau, F.; Myers, M.D. and Nielsen, P.A.: *Action Research.*
Communications of the ACM **42(**1), 94-97, 1999,
http://dx.doi.org/10.1145/291469.291479,

[11] NIST: *NIST Special Publication 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations.*
http://dx.doi.org/10.6028/NIST.SP.800-53r4,

[12] Stevanovic, B.: *Maturity Models in Information Security.*
International Journal of Information and Communication Technology Research **1**(2), 44-47, 2011,

[13] Valdevit, T.; Mayer, N. and Barafort, B.*: Tailoring ISO/IEC 27001 for SMEs: A Guide to Implement an Information Security Management System in Small Settings.*
In: O'Connor, R.V., et al., eds.: *Software Process Improvement.* EuroSPI. Communications in Computer and Information Science **42**, Springer, Berlin & Heidelberg, 2009,
http://dx.doi.org/10.1007/978-3-642-04133-4_17.