DE GRUYTER
OPEN

Considerations on the implementation steps for an information security management system

Răzvan Cristian IONESCU
The Bucharest University of Economic Studies, Bucharest, Romania
razv77@gmail.com

Ioana CEAUȘU
The Bucharest University of Economic Studies, Bucharest, Romania
ioana.ceausu@fabiz.ase.ro

Cristian ILIE
The Bucharest University of Economic Studies, Bucharest, Romania
dgaeur@gmail.com

Abstract. *News about various information security attacks against companies appears almost every day. The sources of these attacks vary from cyber-criminals who want to steal companies' data to demand a ransom, to current or former employees who want to create damage to the organization. The best way to defend organizational critical assets is to implement an Information Security Management System that secures all sensitive assets from confidentiality, availability and integrity perspective. An Information Security Management System offers top management a framework for sensitive information flow control. This framework includes with a risk assessment that considers the security threats and vulnerabilities of the company's assets. Companies usually implement Information Security Management System only after they have a functional quality management system, which brings clarity and optimization to the company's processes. Current approaches on creation and implementation of effective Information Security Management System are very theoretical and thus difficult to use in practice. The main objective of this paper is to present an Information Security Management System implementation method in the case of a small company by defining the basic steps in achieving a fully functional Information Security Management System. The proposed methodology considers the top management Information Security Management System objectives, organizational context, risks assessment and third parties expectations fulfillment.*

Keywords: information security management system, ISMS implementation steps, ISMS implementation methodology, Organizational security, ISMS for small and medium enterprises, protection of company's data, ISMS design.

Introduction

Any organization is exposed to various information security attacks that can target its sensitive information. These kinds of attacks are possible, as vulnerabilities can be exploited by specific threats, thus the result of such exploitation is the impact on the financial state and the reputation of the companies.

The solution is to adopt an Information Security Management System (ISMS) based on the security risks the companies have, correlated with their business objectives. The approach is to implement several chronological and logical steps, aligned with the business requirements in order not to create disruptions in the current activities of the company.

DOI: 10.2478/picbe-2018-0043

As any company can have several management systems already implemented before ISMS, it is crucial to integrate this management system within the current ones for a successful effectiveness of the organizational processes. The purpose of this integration is to have one single management system that manages all the challenges of the company, including the security ones. The steps of the methodology proposed for implementation of an ISMS considered this aspect. The ISMS must, also, have an internal integration between its components: strategy, people, organization, technology (AlHogail, 2015).

Current state of methodologies for the implementation of Information Security Management Systems

There are some well-known recognized guidelines for the implementation of an ISMS, like ISO/IEC 27003, GASPP/GAISP, SSE-CMM (Siponen & Willison, 2008) that debate various ways to obtain an effective ISMS. There are some methodologies specific for computers security (Grance at al., 2003) and security standards like ISO/IEC 27001, COBIT, German IT-Grundschutz and Common Criteria (Beckers at al., 2014) that can be used as best practices in the implementation of an ISMS (Hohan et al., 2014; Maier at el., 2013).

The most known ISMS implementation methodology is the one proposed by the International Organization for Standardization, in its ISO/IEC 27003 standard. It is based on the Plan-Do-Check-Act cycle of process continual improvement and proposes several steps for the implementation of ISO/IEC 27001 ISMS requirements standard (ISO/IEC 27003, 2010).

While ISO/IEC 27003 considers only three information attributes (confidentiality, integrity and availability) as a minimal requirement for information security, other methodologies propose even six attributes (confidentiality, integrity, availability, accountability, authenticity and reliability) (Hoppe et al., 2002) to be considered for the information security.

The ISMS implementation methods vary from six phases (Hoppe et al., 2002) to even twelve phases (Kadam, 2002). In all cases, ISMS must be a documented system based on security policies (Wood, 2002; Moule, 1995). A documented ISMS assures the framework for the business continuity process and, in the same time, is a base for the training process as well.

Organizational vulnerabilities are related to IT&C equipment but also refer to vulnerabilities related to the human resource (Safa et al., 2016). The security awareness level of the people involved in ISMS is very important (Da Veiga & Martins, 2015a) as they have direct access to company's information using their credentials. Therefore, an information security awareness program is of high importance (Vroom & Von Solms, 2002). Some studies revealed that managers must have an effective role in ISMS for a successful implementation (Kiehne et al., 2017; Soomro et al., 2015). Knowledge sharing among the employees is a key factor that can reduce the number of security incidents (Safa & Von Solms, 2016) as the current and former employees are one root cause of information security breaches (Da Veiga & Martins, 2015b).

Research methodology

The authors studied several implementation methodologies that have been proposed by various authors over the past 25 years. These methodologies are specific to information security management system, applicable in any industry, no matter the size of the company. A sample of twenty small companies, with up to twenty employees each, having an ISMS implemented has been studied also. The authors wanted to study if the chosen sample of companies use some customized ISMS implementation methodologies specific for their industry or if these steps can be the same for any small and medium enterprise.

The assessment method used for the ISMS implementation steps that have been used in these companies, was by performing audits in these companies. The audits lasted between one to five days each and were based on interviews with the staff of the companies, review of ISMS documents (policies, procedures, records), system testing, and direct observation of the activities performed. All the audits were performed in the last 10 years.

Research results

The proposed methodology presents the approach proposed by the authors for the ISMS implementation steps for a small to medium company following the study of the current implementation methodologies and the implementations of ISMS found during the audits performed in these twenty companies.

The organizational chart below represents the typology of the studied sample of companies having an ISMS implemented. The main processes are represented with green color.

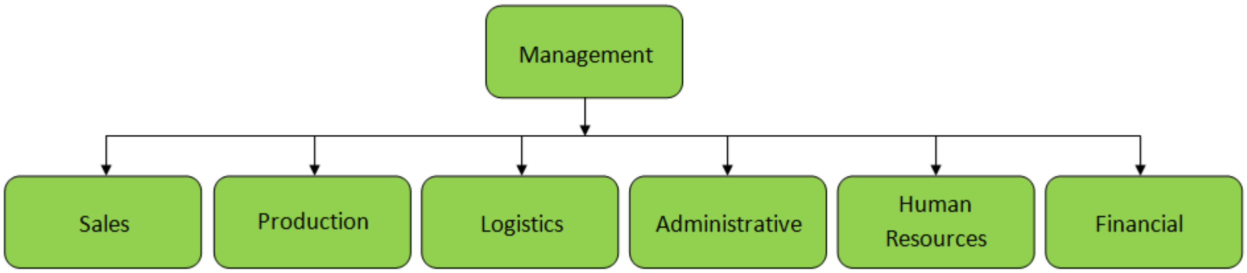

Figure 1. Organizational chart considered for the proposed ISMS methodology

Source: Contribution of the authors.

The authors assumed the top management targets to implement ISMS in the company so a business case to make it aware of the information security importance for the company's processes is not needed in this case. In all the other cases, the information security awareness of the top management should be the first one.

The authors propose this ISMS methodology that can be applied to any small and medium enterprise (SME) from any industry. The steps of this methodology are chronological and based on a simple organizational chart as it is in the figure no. 1. These steps are:

Step 1: Define the ISMS managing structure

Top management must appoint an employee to take the responsibility of managing the implementation process. A first line manager should be chosen to manage this process. Selection of this responsible must be done by considering the following factors:

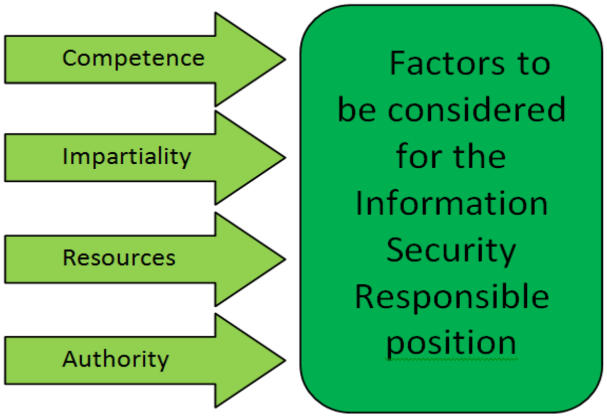
Competence
Impartiality
Resources
Authority
Factors to be considered for the Information Security Responsible position

Figure 2. Factors to be considered for the Information Security Responsible position

Source: Contribution of the authors.

- *Competence*. The responsible must know information security concepts and the specific business processes and risks. Having an IT and security background is a very important aspect. The competence of this person should cover also the requirements of other management systems, if the company has implemented more management systems. As an example, if a quality management system is implemented in the company the knowledge of the ISMS responsible should refer to the defining, measurement and control of the quality of processes, products and/or services of the company. Integration between ISMS and other management systems is not mandatory to exist within the company but if exists, it has many benefits for the management system (e.g.: less procedures and records to be managed, increased control of the internal processes, less resources allocated for this control).
- *Impartiality*. It is assumed that multiple responsibilities are allocated to the same ISMS responsible if this person is one of the employees. This happens in the small and medium companies usually as they do not have enough internal resources. In this case, the auditing of the processes managed by this ISMS responsible person must be performed by a different competent person in order to preserve the impartiality. The lack of segregation of duties can affect the quality of the internal audit directly. If the ISMS responsible audits processes that are performed by himself/herself daily, it is possible not to discover all the existing deficiencies. That is why a second opinion is recommended to be given by another competent person. One of the available solutions to avoid the lack of impartiality is to train at least one more internal ISMS auditor beside the appointed ISMS responsible.
- *Resources given for the implementation*. As the security costs, the ISMS responsible must have a budget allocated to implement the security measures. The resources are related to financial figures from the budget but also to the time and human resources allocated for ISMS activities by the company. In very rare cases the responsible is a new employee hired with the sole responsibility to manage the ISMS. In some cases, an external consultant can help in the implementation process, in others the whole implementation is performed with internal resources.
- *Authority*. The ISMS responsible must coordinate all the implementation process and must steer the organization towards its security objectives. To do that, this person must have enough authority in the company to ask for implementation and then manage the required changes.

In some particular cases, the lack of authority can be linked with the lack of objectivity. This linkage can appear when the ISMS responsible checks the ISMS performance of the processes managed by his/her superiors. The objectivity of the ISMS audit process might be affected due to the lack of authority of the ISMS responsible upon the auditee.

Step 2: Define the information security scope

Top management must define the scope as he/she allocates the resources and knows best the purpose of the ISMS. In some cases, the ISMS Responsible can propose a scope but the final approval comes always from the top management. The scope must contain the business processes that will be covered by the ISMS and the physical locations where the company operates. These physical locations can be owned or not by the company. Clarification of the scope means the limits of the ISMS are clearly defined. The scope must refer to the IT infrastructure limits as well. The company must identify the locations of its critical data not matter of they are physical or virtual locations. The dependence of external providers must be also considered in the scope definition process, mainly if the company outsourced parts or its entire IT infrastructure maintenance and administration to a third party.

Step 3: Define the information security purpose

Each ISMS implementation must have some specific information security objectives. These objectives must be formulated in direct reference with the specific business approach and ISMS scope (e.g.: protecting the information security of the data that are stored on the clients' information systems for which the company is having maintenance contracts). The objectives must be clear, communicated to all the stakeholders and must have persons to be appointed as responsible to achieve the targets. Resources must be allocated as well, for each objective.

Each objective must address a specific security need. These needs should be defined by the top management of the company. The management can use as input data for the start of the objectives' establishment process, the following:

- the need to solve some known security issues;
- the desire to fulfill some external requirements from providers or clients;
- the need to fulfill some legal and regulatory requirements.

The ISMS responsible can design a strategy, consisting in some specific actions that should address all together a specific objective. Once the specific action plan is put into practice, the objective must be reached.

Step 4: Identify other business requirements and objectives

This step is mandatory in order to integrate this ISMS with other possible management systems in order to avoid creation of duplicate documents, useless processes and bureaucracy.

For example, the Sales department has the objective to reach a certain turnover, as part of the quality management system, so in order to fulfill this task, the sales employees must have fast access to needed information in order to respond to their clients promptly. In many cases the access control and security concepts are ignored in the setup of this objective of the Sales departments. If the ISMS is implemented, the accessibility of information in the Sales department shall be affected due to new internal security rules that mitigate some identified security risks in the Sales department. A main security risk, specific to the Sales departments, is the theft of the clients' database by the former sales employees and its use at the new workplace. Some specific security controls like segregation of duties, setting of password policies and access control to the clients' database can assure the security framework inside the Sales department if each Sales employee has limited access to only a part of the clients' database, and not to the whole database, as it was before the implementation of ISMS.

Another purpose of this step is to check business requirements in terms of processes' efficiency and legal, contractual compliance. In the example above, by securing the clients' database, the company fulfils the legal and contractual requirements as well as regards the confidentiality agreements with its clients and the personal data protection legislation.

Step 5: Identify sensitive information to be protected

A small group formed by the company's main business processes managers must analyze and identify which information and physical assets are critical to protect from business, legal and contractual perspectives. An inventory of these information and physical assets should be documented in order to be clear for all stakeholders what information must be protected. The responsible for the asset inventory should consider the products, services, processes and the assets which are inside the ISMS scope only.

A gap analysis is needed to identify current security status for each company's asset. This analysis is recommended to be done at the beginning of ISMS implementation and should identify the needed security measures with the purpose to fill the gaps between the current state of security and the ISMS requirements and expectations.

Step 6: Identify the risks and protection measures

Information security risks must be identified for each element from the inventory. Technical and organizational protective measures must be defined for each element in the inventory, for each identified risk. The risks can be seen as a security threat that might exploit one or more vulnerabilities of a certain asset.

Sources of the threats might vary from people with bad intentions, natural disasters to cyber-attacks or physical attacks. In the same time, the possible vulnerabilities can vary from the lack of training of the people working with the sensitive data, wrong or lack of configurations of the IT equipment to usage of weak passwords.

One risk can be represented by the lack of an information security awareness process among the employees that can allow an attacker to affect the company's sensitive information. Lack of an in-depth security mechanism can be exploited also by an attacker (for example, an employee or a hacker). The legal risks or compliance ones shall be identified as well in the risk analysis (e.g.: usage of software without having a license is against the legislation requirements).

Each risk, from the risk analysis, must have associated one or more mitigation measures. This set of measures have the purpose to increase the security level in that specific area of the company.

Step 7: Implement the protection measures

Implementation of the above identified measures must be done starting from the most critical risks that have been identified (e.g.: lack of strong passwords for accessing critical assets, lack of a business continuity plan, lack of performing back-up before interventions in the clients' computers for solving a malfunction) and implement security measures to mitigate this risk. In it highly recommended these security measures to be implemented in order not to affect the processes efficiency overall. A cost-benefit analysis can be done to identify the best security measures that are mitigating a certain risk. Exhaustive security measures would increase the costs of the ISMS implementation and exceed the initial budget established by the company for its ISMS. So, a proportionate number and type of security controls is recommended to be implemented in order to fit the budget and mitigate the real security risks.

Some security measures can refer to the need of developing procedures for some critical processes. Others can refer to the training of staff, access control, enforcement of a password policy and application of cryptography. In any case, two main processes must be developed in this implementation stage: managing of security incidents and business continuity. The security incidents process must start from the training of employees with the need of reporting of any suspicious action they detect, especially of the infringement of the established security rules. ISMS responsible or other designated responsible could centralize all the reported incidents, review them and provide a resolution with a set of actions to be implemented in order to close the incident. A database or record with all the actions performed for closing an incident should be developed and maintained to mitigate the risk and impact of a further appearance of the same incident.

The business continuity process should consist in developing of some scenarios with actions to be done for the most significant security risks (e.g.: detailed action plan for recovering after a cyber-attack, training of staff with the needed behavior in case of an earthquake). This action plan must lead to the recovery of critical processes first and then of all the other related ones. Any developed scenario must be tested to check if the proposed actions are suitable and lead to a fast and full recovery of the process and data. Awareness and training programs for staff are key factors for the success of a business continuity plan.

Step 8: Check the ISMS

In this step, the company tests the effectiveness of the security measures that have been implemented. This step can include: internal audits, external/internal vulnerability scans, penetration tests, feedback from interested parties, incident management reviews. The results of these verifications must be retained for internal and external evidence.

The check of the ISMS can be done by using a checklist containing the requirements or by processes. The difference between the two approaches is that the audit based on a checklist doesn't follow the process so specific security issues can be skipped easily. On the other hand, the audit on process can skip some ISMS requirements. Therefore, the best option for performing the audit of the ISMS is to combine the audit on process with the checklist. A matrix of specific requirements to be checked for each process will result by using this combination. This approach should assure the company that the auditor will check the right requirements of ISMS for the specific processes and all the ISMS processes and requirements will be audited.

Several vulnerable processes have been identified during this study following the performance of the audits in the sampled companies:

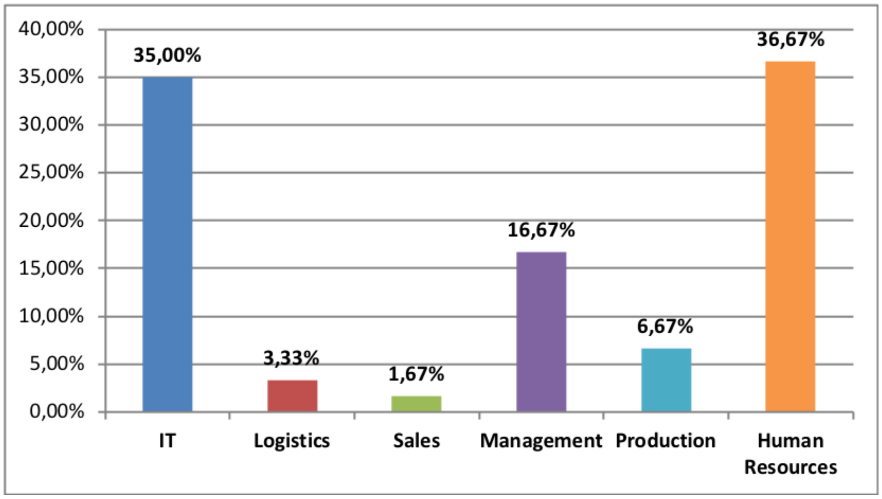

Figure 3. % of nonconformities found for each audited process

Source: Contribution of the authors.

The above nonconformities percentages per process were calculated by adding all the nonconformities found in these specific processes, following the information security audits in all the sampled companies, and dividing them to the total number of all nonconformities found for all processes. The result found after this calculation was the percent on the vertical axis from Figure 3.

Most deficiencies found during the audits in the Human Resources processes were due to the improper training and awareness of the staff involved in Information Security Management System. Many employees failed to respect the new security rules due to the lack of training time and poor selection of the proper individuals to execute certain security tasks.

Step 9: Improve the ISMS

Any deficiency found during the verification phase must be resolved in order to correct and improve the ISMS. Both the verification and improving step must be performed periodically and any time when a significant issue, that might affect the information security, occurs in the activity of the company. Improvements of ISMS should be applied at all levels: information systems, physical, organizational, documental and human resources.

Top management should be informed every time when severe security risks have been identified in order to allow the ISMS responsible to act for improving the company' security by providing him/her the required resources. All the identified improvements must be applied to correct the security deficiencies in such way, they do not create a negative impact on the other business processes.

Conclusion

The security of the companies is obtained by adopting measures for protecting IT&C systems, people, processes and physical assets.

A high number of ISMS deficiencies have been found in the sampled companies from the study, after the first iteration of their chosen ISMS implementation methodology. Most of the deficiencies were found in the human resource process due to the lack of commitment of the employees, and in the IT process due to the short implementation time (almost all studied companies have implemented ISMS in 2-3 months). It has been obviously seen that the minimum time for implementation should be at least 6 months. The authors consider this amount of time to be sufficient for an in-depth implementation of ISMS in a small and medium company. This extended time will assure also a consistent ISMS training and awareness process among the employees. In some cases, the steps from the ISMS methodologies adopted by the audited companies were not consistent as the traceability between these steps and implemented actions was missing. In many cases, the security measures were found to be implemented without knowing which the specific security risks for that process or area are. For this reason, over 15% of the nonconformities from figure no. 3 are for the management process.

All studied ISMS implementation methodologies proposed by various authors have a top down approach and militate for the integration of the security concept into the business processes. This top down approach was found in 100% of the studied companies and proved to be the best choice.

Integration of ISMS with other business requirements is a must in order to increase the efficiency of the processes as well, not only to block the access to sensitive information. Communication between the implementation team and the rest of the employees is a must in order smooth the process of achieving the other business targets and assure a proper awareness and commitment of the whole organization.

For small organizations, one person to manage the planning, implementation, verification and improving the ISMS should be enough. Appointing more employees to be part of an information security commission can be a very good decision for all sizes of companies, even though, in practice, this is mostly applicable to medium-large companies. In some cases, the ISMS responsible must be freed of other tasks in order to have enough time to manage the ISMS properly.

It is recommended the ISMS scope to cover all business processes and all locations of the company for an increased effectiveness of the security environment.

Bibliography

AlHogail, A. (2015). Design and validation of information security culture framework., Computers in Human Behavior, 49, 567- 575.

Beckers K., Côté I., Fenz S., Hatebur D., Heisel M. (2014) A Structured Comparison of Security Standards. In: Heisel M., Joosen W., Lopez J., Martinelli F. (eds) Engineering Secure Future Internet Services and Systems. Lecture Notes in Computer Science, 8431, Springer, Cham.

Da Veiga, A., Martins, N. (2015a). Improving the information security culture through monitoring and implementation actions illustrated through a case study. Computers & Security, 49, 162-176.

Da Veiga, A., Martins, N. (2015b). Information security culture and information protection culture: A validated assessment instrument. Computer Law & Security Report, 31, 243-256.

Grance, T., Hash, J., Stevens, M., O'Neal, K., Bartol, N. (2003). SP 800-35 - Guide to Information Technology Security Services. Special Publication 800-35. National Institute of Standards and Technology – Technology Administration, U.S. Department of Commerce.

Hohan, A.I., Olaru, M., Pirnea, I.C. (2016). Assessment and continuous improvement of information security based on TQM and business excellence principles, Procedia Economics and Finance, 00, 352-359.

Hoppe, O.A., Van Niekerk, J., Von Solms, R. (2002). The effective implementation of information security in organizations. IFIP/SEC2002 Security in the Information Society Visions and Perspectives International Conference, 17th Edition, May 7-9, Cairo, Egypt.

ISO/IEC 27001:2013. (2013). Information technology -- Security techniques -- Information security management systems – Requirements. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en [16.02.2018].

ISO/IEC 27002:2013. (2013). Information technology -- Security techniques -- Code of practice for information security controls. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en [16.02.2019].

ISO/IEC 27003:2010. (2010). Information technology - Security techniques - Information security management system implementation guidance. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27003:ed-2:v1:en [16.02.2018].

Kadam, A. (2002). Implementation Methodology for Information Security Management System (to comply with BS 7799 Requirements). GSEC Practical Requirements (v.1.4b), SANS Institute, 2003.

Kiehne, J., Ceaușu, I., Arp, A.-K., Schüler, T. (2017). Middle management's role in strategy implementation projects, Proceedings of the International Conference ICBE 11th Edition, March 2017, Bucharest, Romania.

Maier, D., Olaru, M., Hohan, A., Maier, A. (2013). Development of an Organization by adopting the Integrated Management System, Proceedings of the 9th European Conference on Management Leadership and Governance, Nov 14-15, Klagenfurt, Austria.

Moule, B., Giavara, L. (1995). Policies, procedures and standards: an approach for implementation. Information Management & Computer Security, 3 (3), 7-16.

Safa, N.S., Von Solms, R., Furnell, S. (2016). Information security policy compliance model in organizations. Computers & Security, 56, 1-13.

Safa, N.S., Von Solms, R. (2016). An information security knowledge sharing model in organizations. Computers in Human Behavior, 57, 442-451.

Siponen, M., Willison, R. (2009). Information security management standards: Problems and solutions. Information & Management, 46 (5), 267 – 270.

Soomro, Z.A., Shah, M. H., Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36, 215-225.

Vroom C., von Solms R. (2002) A Practical Approach to Information Security Awareness in the Organization. In: Ghonaimy M.A., El-Hadidi M.T., Aslan H.K. (eds.) Security in the Information Society. IFIP Advances in Information and Communication Technology, 86, Springer, Boston, MA.

Wood, C. C. (2002). Information Security Policies Made Easy: A Comprehensive Set of Information Security Policies: Version 9.0. PentaSafe Security Technologies.