A Cyclical Evaluation Model of Information Security Maturity

ABSTRACT

Purpose - The lack of a security evaluation method might expose organizations to several risky situations. This paper aims at presenting a cyclical evaluation model of information security maturity.

Design/methodology/approach - This model was developed through the definition of a set of steps to be followed in order to obtain periodical evaluation of maturity and continuous improvement of controls.

Findings – This model is based on controls present in ISO/IEC 27002, provides a means to measure the current situation of information security management through the use of a maturity model and provides a subsidy to take appropriate and feasible improvement actions, based on risks. A case study is performed and the results indicate that the method is efficient for evaluating the current state of information security, to support information security management, risks identification and business and internal control processes.

Research limitations/implications - It is possible that modifications to the process may be needed where there is less understanding of security requirements, such as in a less mature organization.

Originality/value - This paper presents a generic model applicable to all kinds of organizations. The main contribution of this paper is the use of a maturity scale allied to the cyclical process of evaluation, providing the generation of immediate indicators for the management of information security.

Key words: Security; Maturity; Risks

Article Classification: Research paper

INTRODUCTION

The critical and methodical evaluation of information security related controls becomes necessary since technologies, business processes and people change constantly, altering the current level of risk and creating new risks to the organization (Jirasek, 2012).

The challenge lies in defining information security goals, reaching them, keeping them and enhancing the controls that support them, to assure competitiveness, profitability, compliance to legal requirements and maintaining a good image of the organization to the society and the financial market. Maturity models can help in facing this challenge.

Maturity models are based on the improvement of processes and the existence of fundamentals to guide and measure the implementation and improvement of processes (Chapin and Akridge, 2005; The Open Group, 2011). Although CobiT (Control Objectives for Information and Related Technology) has a maturity model, it does not define a rigorous and practical maturity evaluation model. Users of the CobiT maturity model need to build their own evaluation model (Breier and Hudec, 2012; Walker et al., 2012). Currently there is a research effort related to the use of models to measure the maturity of Information Security Management Systems (Aceituno, 2007; Chapin and Akridge, 2005; Karokola et al., 2011; Park et al., 2008; The Open Group, 2011; Woodhouse, 2008).

This paper proposes a method for information security management through a periodic evaluation of maturity and continuous improvement of controls. The proposed model is generic and applicable to all kinds of organizations, using the ISO/IEC 27002 security controls (ISO, 2005b) related to the analysis of risk and the evolution of the environment.

The paper is organized in seven sections. Section 2 presents the main related works. Section 3 presents the main technical standards related to information security and risk management. Section 4 describes basic concepts of maturity models. In section 5, a cyclical evaluation model of information security maturity is proposed. Section 6 presents a case study in which the model was applied in an organization to verify its effectiveness. The last section presents the conclusions.

RELATED WORK

The work of Karokola et al. (2011) describes a proposal of information security maturity model (ISMM) for secure e-government services (implementation and service delivery). Basically, the model is based on the findings from the critical analysis of information security maturity models of the literature. Five maturity levels with their respective security control dimensions were defined: level 1 (undefined), level 2 (defined), level 3 (managed), level 4 (controlled) and level 5 (optimized). Maturity level 1 is the lowest and maturity level 5 is the highest. This paper is a theoretical proposal and does not show a case study of application of the proposed model. The paper is limited to defining five levels to evaluate the maturity of an information security management system specifically for secure e-government services, without presenting a method for the measurement of the current situation of security or the monitoring and evolution of security and related processes.

In the study of Dzazali et al. (2009), the researchers attempt to evaluate the information security maturity level of the Malaysian Public Service organizations. This research uses CobiT maturity levels as the base. This study uses data collected from 970 targeted individuals through a self-administrated questionnaire. Findings on the maturity level show that 21% of respondents are at Level 2, 61% are at Level 3, followed by 13 % at Level 4 and 1% at Level 5. It is an exploratory study, of qualitative nature, with the application of questionnaires. The study of Dzazali et al. (2009) presents specific and static propositions, which may preclude the evaluator conducting proper risk analysis as technologies, business processes or external requirements evolve.

The main difference between the cited works (Dzazali et al., 2009; Karokola et al., 2011) and this paper is that in this paper we present a management process for the continuous improvement of security, in the form of a generic model applicable to all kinds of organizations, regardless of size or field, using the 133 information security controls present in the ISO/IEC 27002 standard.

The work of Woodhouse et al. (2008) is similar to this one in the sense that it does not use a methodology based on generic checklists created based on technical controls. However, Woodhouse et al. (2008) does not present a method to effectively measure and find out the level of information security maturity.

Park et al. (2008) presents a way to measure maturity in the management of information technology services and uses the IT Infrastructure Library (ITIL) as a foundation. The paper shows the phases of interviews of persons in charge, measurements of maturity and the results of measurement. The model of Park et al. (2008) presents the limitations of evaluating security under the scope of Service Support and Service Delivery processes, which are essentially linked to Information Technology, it does not allow for an analysis of information security risks generated in business processes not essentially related to IT.

MAIN TECHNICAL STANDARDS RELATED TO INFORMATION SECURITY

The main normative references are the standards in the "27000 family" from the International Organization for Standardization (ISO), which are specific for the management of information security (Cowan, 2011).

ISO/IEC 27001:2005 – its goal is "to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS)" (ISO, 2005a).

ISO/IEC 27002:2005 - it is the foundation standard for information security. The goal of this standard is to establish guidelines to establish, implement, maintain and improve information security management, through the definition of controls that may be used to meet requirements identified by risk assessment (ISO, 2005b). The standard is structured in 11 sections of information security controls, divided in 39 main security categories and one introductory section that addresses the assessment and treatment of risks. 133 controls applicable to information security are defined. The standard is not perfect and foresees that organizations may have to use more controls than those presented. Every activity in an organization involves risks that have to be identified, analyzed and assessed to establish if they need treatment. This review is exactly what will determine the need for changes and the prioritization of these changes according to requirements that must be met by the organization.

ISO/IEC 27005 provides guidelines for information security risk assessment (ISO, 2008). Figure 1 presents a schematic view of the information security risk management process according to ISO/IEC 27005.

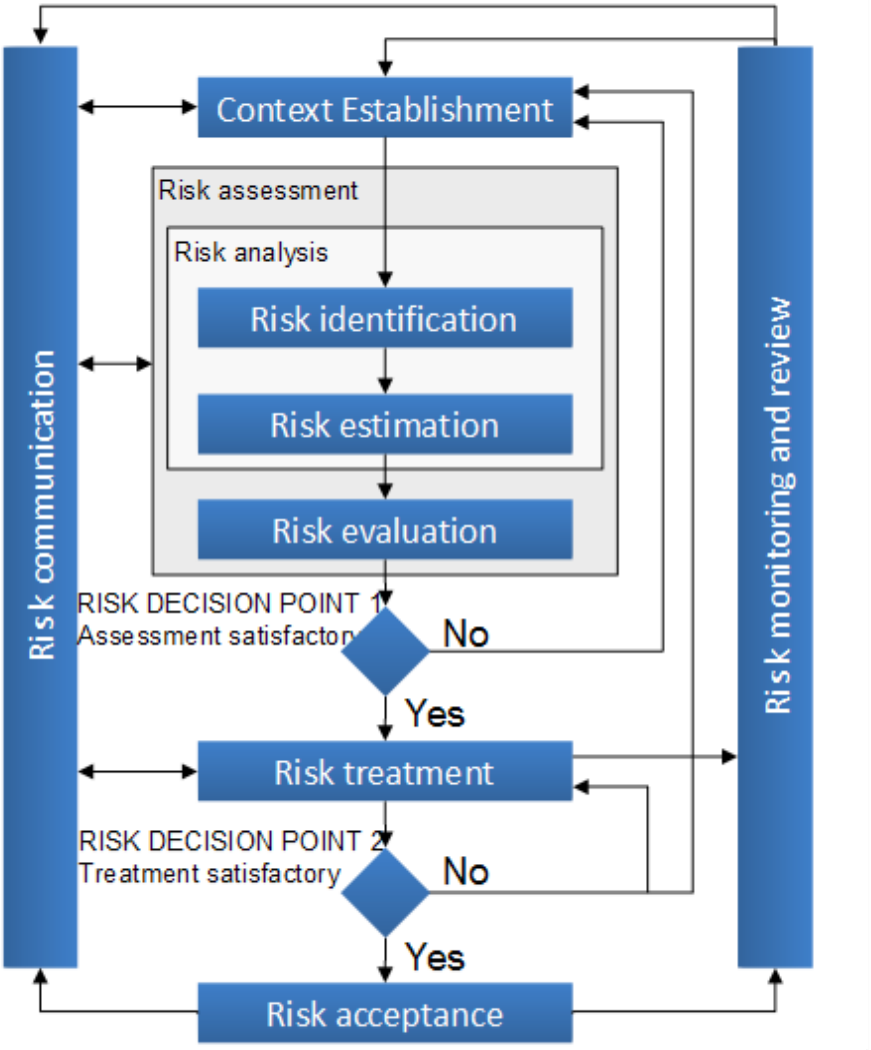

Figure 1. Information security risk management process (adapted from ISO (2008)).

SECURITY MATURITY MODELS

A security maturity model provides a guide for a full security program. It also defines the order in which security elements must be implemented, encourages the use of standards of best practices and provides a means to compare security programs (Chapin and Akridge, 2005; The Open Group, 2011).

After identifying critical processes and controls, the use of a maturity model allows the identification of gaps that represent risk and how to show them to management team. Based on this analysis, action plans can be evaluated and developed for the improvement of processes and controls considered deficient up to the desired development level (ITGI, 2007; Jirasek, 2012).

Some approaches of information security management standards can be classified in the following way: process oriented, such as CobiT and ITIL; control oriented, such as ISO 27001; product oriented such as Common Criteria (ISO 15408); risk management oriented, such as OCTAVE and ISO 27005 and best practices oriented, such as ISO 27002. Aceituno (2007) defines a maturity model for information security management, currently called O-ISM3 and compatible with the ISO 27001 standard.

The two most important maturity models considered in this work are CobiT and O-ISM3. The COBIT maturity model is widely used for IT governance. The O-ISM3 model is specific to management of information security. In Karokola et al. (2011), other maturity models are described, but these were not considered, since they do not present measuring aspects.

CobiT Maturity Model

CobiT presents a set of indicators obtained by the consensus of experts, which are more focused on the controls of activities than in their execution. These controls assist in optimizing the IT investment, ensure service delivery and provide a measure to pass judgment and allow comparison.

The information security management model presented in this paper has its measurement basis supported by the maturity scale of CobiT (Figure 2).

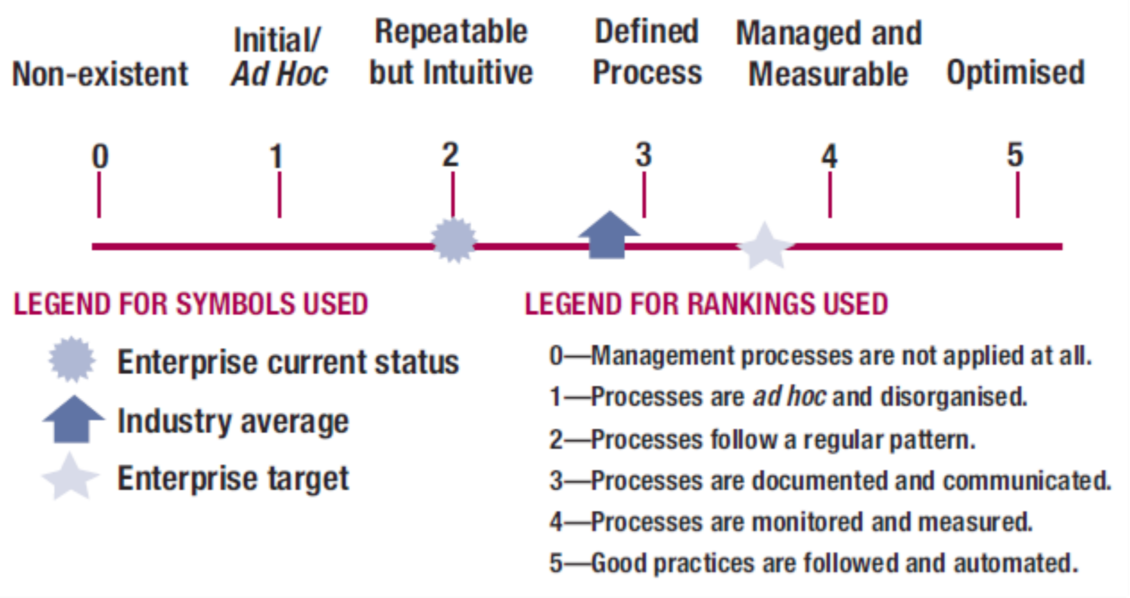
Non-existent
Initial/ Ad Hoc
Repeatable but Intuitive
Defined Process
Managed and Measurable
Optimised
0
1
2
3
4
5
LEGEND FOR SYMBOLS USED
Enterprise current status
Industry average
Enterprise target
LEGEND FOR RANKINGS USED
0—Management processes are not applied at all.
1—Processes are ad hoc and disorganised.
2—Processes follow a regular pattern.
3—Processes are documented and communicated.
4—Processes are monitored and measured.
5—Good practices are followed and automated.

Figure 2. Graphic representation of the maturity model used in CobiT (adapted from ITGI (2007)).

The maturity scale used in this paper is presented in Table 1.

Level	**Characteristics**
0 Non-existent	Complete lack of any recognizable processes. The enterprise has not even recognized that there is an issue to be addressed
1 Initial/Ad-hoc	There is evidence that the enterprise has recognized that the issues exist and need to be addressed. There are, however, no standardized processes; instead, there are *ad hoc* approaches. The overall approach to management is disorganized.

Level	Characteristics
2 Repeatable but Intuitive	Processes have been developed until the point where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.
3 Defined Process	Procedures have been standardized and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalization of existing practices.
4 Managed and Measurable	Management monitors and measures compliance with procedures and takes actions where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.
5 Optimized	Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow.

Table 1. Scale used for maturity levels (adapted from ITGI (2007))

Users of CobiT need to build their own evaluation model, according to the granularity of the processes, since the maturity model does not define a practical evaluation model (Breier and Hudec, 2012; Walker et al., 2012).

O-ISM3 Maturity Model

The O-ISM3 (The Open Group Information Security Management Maturity Model) is an information security management maturity model with five levels: undefined, defined, managed, controlled and optimized (The Open Group, 2011). The model development is grounded on CMMI, ITIL, ISO 9000, and ISO 17799/27001. However, ISM3 does not measure risk or security directly (Karokola et al., 2011).

THE MODEL OF EVALUATION BY MATURITY LEVELS

The model presented in this paper aims to evaluate information security in a way consistent with organizational goals. The main characteristics of the model are:

1. Being structured in the form of a management process that allows continuous evaluation and improvement, through the use of the ISO/IEC 27001 standard;
2. Being based on controls that are appropriate for information security, through the use of the ISO/IEC 27002 standard;
3. Providing a means to measure the current situation of information security management and its evolution over time, through the use of a maturity model; and
4. Providing support for appropriate and feasible improvement actions, based on risks, supported by the use of the ISO/IEC 27005 standard.

Evaluation and continuous improvement

Since risks are dynamic, information security requirements are constantly changing. The use of PDCA (Plan-Do-Check-Act) model adopted by ISO/IEC 27001 encourages the ISMS administrative users to highlight the importance of continuous improvement based on objective measures.

Information security controls

The evaluation model in this paper uses the structure of controls from the ISO/IEC 27002 standard. The standard defines 133 controls that can be evaluated.

Measurement and monitoring

The information security management system presented in this article has its base measurement supported on the COBIT maturity scale (Figure 2 and Table 1).

Stages of the cycle of evaluation and continuous improvement

This paper contributes in proposing stages of the cycle of maturity assessment and improvement of information security (Figure 3), since CobiT does not define a practical model for assessing the maturity and users need to build their own evaluation model (Breier and Hudec, 2012; Walker et al., 2012).

One metric, or indicator, by itself is not the answer to manage IS (Information Security) issues in an organization. Besides measuring, there must be action on the problems found and monitoring on the evolution over time. Figure 3 presents the eight stages that comprise the proposed cycle of evaluation of information security maturity.

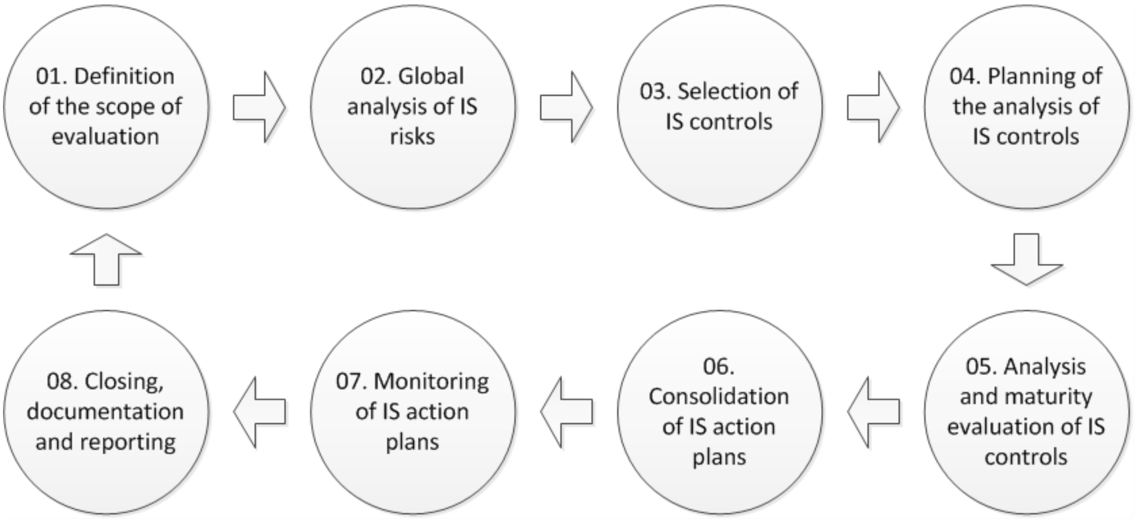
01. Definition of the scope of evaluation
02. Global analysis of IS risks
03. Selection of IS controls
04. Planning of the analysis of IS controls
05. Analysis and maturity evaluation of IS controls
06. Consolidation of IS action plans
07. Monitoring of IS action plans
08. Closing, documentation and reporting

Figure 3. Proposal of stages of the cycle of evaluation and improvement of information security (IS)

Each of these stages is described in more detail below.

1. *Definition of the scope of evaluation*

An organization may have, simultaneously, administrative, industrial or service providing activities, or may be geographically distributed, and consider convenient to divide the evaluation of security maturity in parts.

The definition of scope consists in identifying areas, technologies and processes of the organization that will be included in the evaluation (ISO, 2005a).

2. *Global analysis of risks related to information security*

This model uses the qualitative method (Harris, 2012; ISO, 2008) for risk analysis, through the use of a scale with qualifying attributes that describe the magnitude of potential consequences (impact) and the probability that these consequences may occur (as presented in Figure 4). The method of information gathering uses interviews with at least two people: one with experience in risk analysis and the other with the domain knowledge. Participants of the interview define risks and for each risk the probability and impact are identified, in order to realize the risk analysis. This approach was considered sufficient for the identification of risks and to support the choice of controls to be evaluated.

3. *Selection of information security controls*

In this stage information security controls present in ISO/IEC 27002 are chosen when considered applicable for covering the risks identified in the information security risk analysis stage. From the risk analysis, the goal maturity level (or envisaged level) is defined for each security control in order to keep risk at an acceptable level.

Although the model uses the control structure of ISO/IEC 27002 as a basis for evaluation, organizations must be capable of identifying other controls, considering, for instance, corporate risk analysis or best practices adopted in the field in which the organization operates.

4. *Planning of the analysis of information security controls*

In this stage planning for the analysis and evaluation of controls considered applicable and their respective control activities will be performed. The purpose of this stage is to identify and commit the parties involved, identify stakeholders, define a schedule for evaluation activities in the cycle and create a communication plan for the results obtained.

5. *Analysis and maturity evaluation of information security controls*

Processes and activities carry out security controls. Thus, we can measure the maturity of the processes by measuring the maturity of the related individual controls. A single security control can also be present in distinct processes of an organization.

In this stage the maturity level of each control will be compared to the risk analysis and, if necessary, actions must be proposed for the correction or improvement of related activities. This stage is divided in the following five steps (represented in Figure 4):

a) Identification of related processes and activities: the information security controls are accomplished in the activities of business, operational (task execution) or control (verification or approval of the executed task) processes. This step consists of identifying and relating to the selected security controls, every process, procedure and activity that contribute to its accomplishment;

b) Analysis of the maturity level of the control: based on the processes and activities that support the evaluated control, ascertain the maturity level of the control according to the maturity scale used by the model. Each control can be present in distinct processes/activities and in each process/activity the same control can have a different level of the goal maturity level and of the evaluated maturity level.

c) Evaluation of the maturity level of the control: in this step it will be evaluated if the maturity of the control, ascertained by the set of activities that support it, is consistent with the maturity necessary to treat business related risks (defined as the goal maturity level);

d) Definition of necessary improvements: based on possible deficiencies found in the accomplishment of controls, in this step the actions and improvements in activities related to the security control, or even the creation of new control activities to keep the risk at an acceptable level, will be documented;

e) Communication of results to those responsible for the control: in this step the results of the analysis of the security control are communicated to those responsible, so that they are aware and can assess the necessary actions and possible emergency interventions.

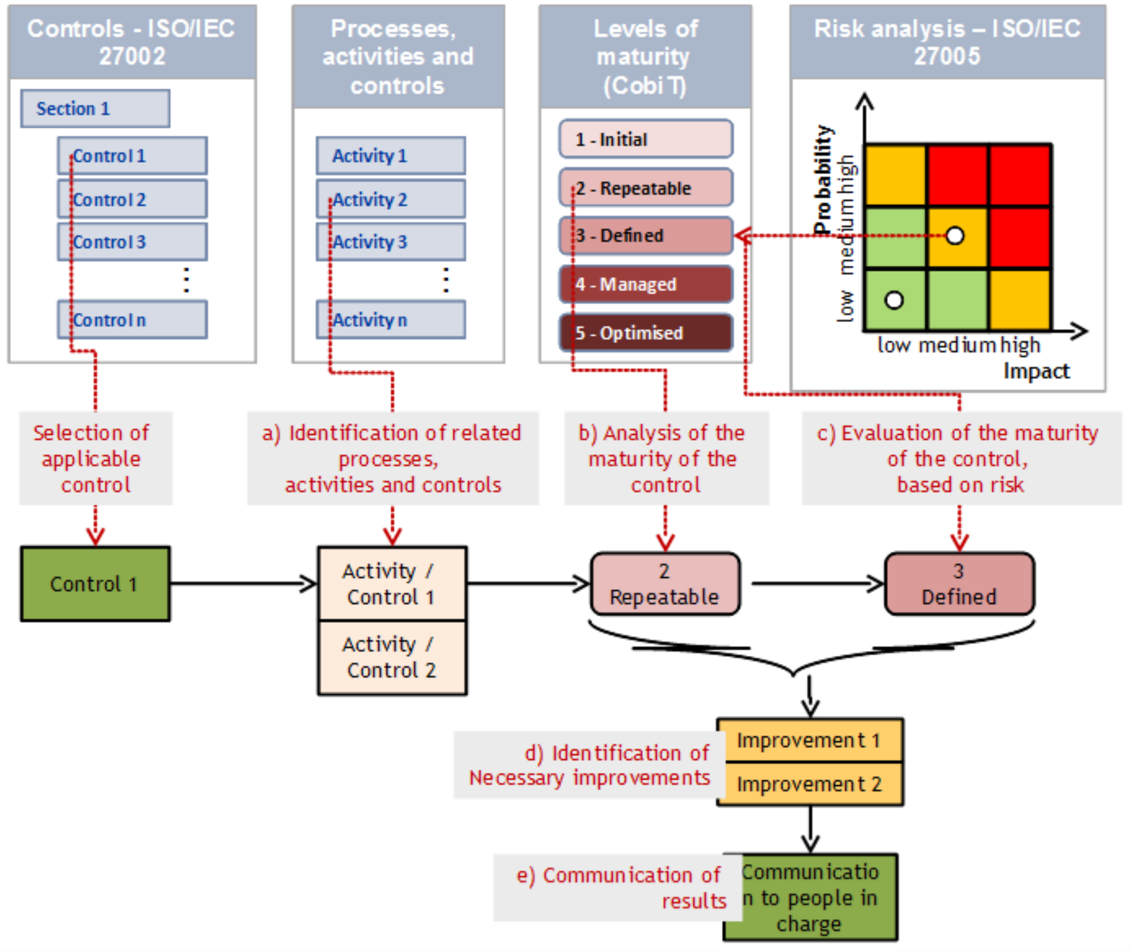
Controls - ISO/IEC 27002
Section 1
Control 1
Control 2
Control 3
Control n
Processes, activities and controls
Activity 1
Activity 2
Activity 3
Activity n
Levels of maturity (CobiT)
1 - Initial
2 - Repeatable
3 - Defined
4 - Managed
5 - Optimised
Risk analysis – ISO/IEC 27005
Probability
low medium high
low medium high
Impact
Selection of applicable control
a) Identification of related processes, activities and controls
b) Analysis of the maturity of the control
c) Evaluation of the maturity of the control, based on risk
Control 1
Activity / Control 1
Activity / Control 2
2 Repeatable
3 Defined
d) Identification of Necessary improvements
Improvement 1
Improvement 2
e) Communication of results
Communication to people in charge

Figure 4. Proposal of steps in the maturity evaluation of information security controls

6. *Consolidation of information security action plans*

It is reasonable to expect that many control objectives may have common action plans. In this stage all the proposed improvements will be consolidated and organized according to the processes and business activities to which they are related. This stage is divided in four steps:

a) Review and organization of identified improvements: this step aims to create an integrated view of all the improvement actions necessary to reduce the implementation effort, since similar changes may be identified and proposed in different controls;

b) Definition of responsibilities for execution: the goal of this step is to appoint, for each proposed action plan, a person responsible for its execution and monitoring;

c) Approval of action plans: in this step, the prioritization, the approval and the planning of action plans are performed;

d) Communication of action plans: in this step the action plans are communicated to those responsible, to make them aware of the work to be done.

The organization must "update security plans to take into account the findings of monitoring and reviewing activities" (ISO, 2005a).

7. *Monitoring of information security action plans*

In this stage a monitoring of the execution of action plans will be performed, to verify the meeting of deadlines and evaluate possible problems in execution.

8. *Closing, documentation and reporting*

In this stage the actions performed during the evaluation cycle are registered and the operational and management reports are issued. Also, the evolution of the maturity level of the controls is documented.

The closing documentation must be complete enough to demonstrate the evolution of information security, raise the awareness of management to the main remaining attention points and risks, justify the need for resources to enhance the level of security and base the critical analysis of improvement of the ISMS.

CASE STUDY OF THE EVALUATION OF INFORMATION SECURITY MATURITY

A case study was performed for the application of the model of evaluation of information security maturity level. The organization that participated in the study is real, but will be named CompanyX.

The chosen scope of evaluation was the set of administrative processes and activities of the organization. The organization had already performed, previously, information security evaluations with a method similar to the described in this paper, which facilitated the tasks of evaluation and reduced the time of analysis.

At the beginning of the study, the evaluated organization did not have a formal evaluation of risks specifically related to information security. It was considered that a complete analysis of information security controls would be adequate for calculating the current maturity level and identification of unknown risks.

Initially, because of the great extension of business processes of the organization, it was decided to consider applicable most of the information security controls proposed in ISO/IEC 27002. Control 10.9.1 – Electronic Commerce – was the only control excluded from the scope of analysis, because the organization does not practice this kind of activity.

The evaluation of controls was performed by the person in charge of information security, with the possibility of consulting experts in each area. The analyses and assessments were recorded in a spreadsheet. For each of the security controls of ISO/IEC 27002, the evaluation spreadsheet had fields that were filled with the following data: the current level of maturity, the goal maturity level, the name of the evaluator(s), the date of the last evaluation, the processes and the related activities to each control and the suggested plans of action.

As an example, we selected the control 11.2.4 – Review of user access rights, control objective 11.2 – User access management. According to ISO/IEC 27002, "management should review users' access rights at regular intervals using a formal process", to maintain an effective control over accesses. Activities performed in the five stages of evaluation were:

1. Identification of related processes and activities: the organization had a semiannual process for reviewing access rights to the computing environment. The whole review process was formalized in a process and the Information Security Policy. People in charge of the review had been trained and support material was available. The process coordinator was the person responsible for information security. However, the request for the review and the review conclusion were conducted via e-mail, with little control over the execution of the process;
2. Analysis of the maturity level of the control: according to the maturity scale used in this work, the existence of a formally defined and approved process, with identified responsibilities and training of people involved characterizes the maturity level 3 – Defined;
3. Evaluation of the maturity level of the control: because the organization was subject to control requirements in its IT processes, it needed to show a control over the access rights review process was in place. As a consequence the organization considered necessary to improve the access rights review process to achieve level 4 - Managed;
4. Definition of necessary improvements: to reach maturity level 4 (managed) the following actions were suggested:
   - I. Develop a system to register every user access rights review cycle;
   - II. Modify the review process so that there was a documented evidence over the reviews and the actions taken if some system, module or environment does not have its review process finished in the specified time;
   - III. Formally communicate the person responsible that does not have its review process finished in the specified time; and
   - IV. Formally communicate the IT and internal audit managers about the monitoring of the process and the completion of the review cycle.
5. Communication of results to those responsible for the control: the proposed actions were documented and forwarded to the IT manager and internal audit.

After the completion of the evaluation of the maturity level of every selected control, the proposed actions originated action plans. The action plans that did not need financial resources were selected to be executed first. The action plans that needed financial resources or demanded greater changes in the processes were selected to be monitored by the organization. At each new evaluation cycle the applicable controls will be reevaluated and the action plans revised.

Table 2 presents the results of the average maturity levels obtained from the evaluation spreadsheet filled with data from the current maturity level for each evaluated section of the ISO/IEC 27002.

Section	**Description – ISO/IEC 27002**	**Average maturity**
5	Security Policy	3.17
6	Organizing information security	2.78

Section	Description – ISO/IEC 27002	Average maturity
7	Asset management	2.55
8	Human resources security	2.35
9	Physical and environmental security	3.24
10	Communications and operations management	2.61
11	Access control	2.59
12	Information systems acquisition, development and maintenance	2.80
13	Information security incident management	1.55
14	Business continuity management	2.02
15	Compliance	2.24

Table 2. Average maturity levels ascertained

Figure 5 presents the visualization of calculated average maturity levels.

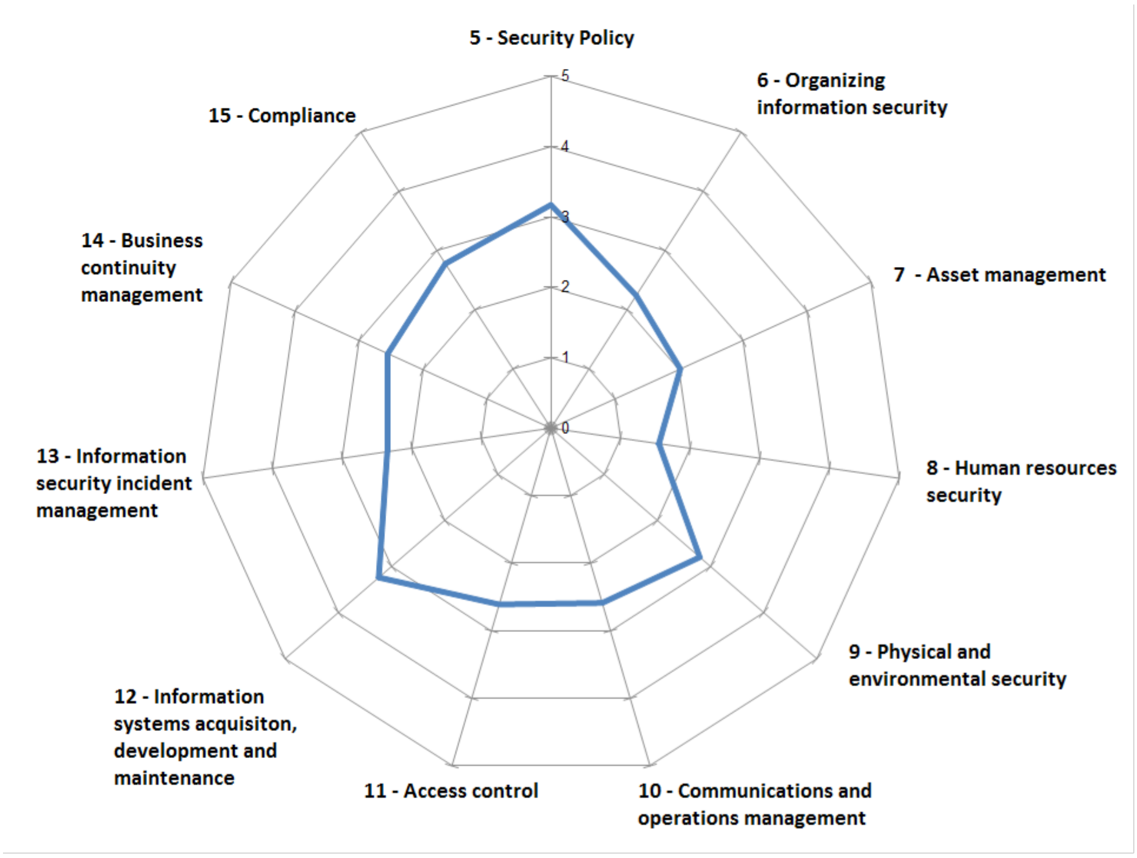

Figure 5. Visualization of average maturity levels ascertained in the case study

Through the analysis of the results obtained, the organization is considered to have an average maturity level of 2.54. It indicates that, on average, their information security related processes are being structured to be formally defined. The organization considers that most of their processes have a maturity level adequate to its reality, and the main controls related to compliance to external requirements are classified in levels 3 or 4. Several action plans created aimed at small improvements in processes, not necessarily related to a maturity level improvement.

According to the perception of the organization, the method of evaluation of controls of the ISO/IEC 27002 standard by means of maturity levels provided some benefits, according to a report by the IT manager: “This method will not be used only as a form of isolated evaluation, but as an instrument of management for the security of our information. Besides providing a picture of the current scenario of our controls, the method provides the creation of documentation for the evaluation and direction of efforts for the improvement of security. Many improvement actions were identified with the individual evaluation of each control item, and the maturity model aids in its prioritization”.

CONCLUSION

The detailing of a method for the management of information security through periodical evaluation of maturity and continuous improvement of controls was shown. The use of the maturity scale allied to the cyclical process of evaluation provided the generation of instantaneous and temporal indicators for the management of information security.

The similarity between this paper and the related works presented is in the use of the ISO/IEC 27002 standard and a maturity model. The main difference lies in the fact that the proposed models present propositions that are specific, static, which may preclude the evaluator the proper analysis of risks inherent to the business as there is an evolution of the environment. Another significant difference is that this paper seeks to define a generic evaluation model, applicable to all kinds of organization, through the use of all the control objectives of the ISO/IEC 27002 standard.

The use of models with propositions that are static and specific to a given sector may be considered useful for beginner or inexperienced evaluators, since it may contain examples of what could be done to improve their security processes; still, they limit the evaluation to the proposed issues to the vision of the creator and to the time when they were created. The use of a generic model can be inadequate for beginner evaluators, who must first understand and interpret the standards; however, they provide to an experienced evaluator room for adjustments and expansions to the scope of evaluation according to changes in the levels of risk over time, being more consistent with the cycle of continuous improvement.

The perception of the organization that participated in the case study indicates that the evaluation method presented may be effective to evaluate the current state of information security of the organization, to aid in management processes, risk identification and to support the improvement on internal processes and controls.

A future work that can be suggested is to apply this technique to a less mature organization than the one cited in the current case study. It is possible that modifications to the process may be needed where there is less understanding of information security requirements.

Some other future works can also be developed: (a) Design a tool to automate the linking of results of risk evaluations to minimal maturity levels that must be achieved; (b) Calculate the average of the goal maturity level of each control - the goal of the organization would ultimately be to move from the current (evaluated) to the envisaged (goal) maturity level; and (c) Insert in the evaluation cycle a stage for independent auditing of the results, for organizations that have chosen a self-assessment approach.

REFERENCES

Aceituno, V. (2007), "ISM3 - Information Security Management Maturity Model – v. 2.1." , available at: http://www.ism3.com/ (acessed 18/June/2013)

Breier, J. and Hudec, L. (2012), "New approach in information system security evaluation" in *Proceedings of the IEEE First AESS European Conference on Satellite Telecommunications in Rome, Italy, 2012*, pp. 1-6.

Chapin, D. A. and Akridge, S. (2005), "How can security be measured", *Information Systems Control Journal*, Vol. 2, pp. 43-47.

Cowan, D. (2011), "External pressure for internal information security controls", *Computer Fraud & Security,* Vol. 2011 No. 11, pp. 8-11.

Dzazali, S., Sulaiman, A. and Zolait, A, H. (2009), "Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations", *Government Information Quarterly,* Vol. 26 No. 4, pp. 584-593.

Harris, S. (2012), *CISSP All-in-One Exam Guide*, 6th Edition, McGraw-Hill Professional Publishing, New York, NW.

ISO (2005a), *ISO/IEC 27001:2005: Information Technology – Security Techniques – Information Security Management Systems – Requirements,* ISO.

ISO (2005b), . *ISO/IEC 27002:2005: Information technology - Security techniques – Code of practice for information security management,* ISO.

ISO (2008). *ISO/IEC 27005:2008: Information technology - Security techniques - Information security risk management,* ISO.

ITGI (2007), *CobiT 4.1 - Control Objectives for Information and related Technology – Framework*, ITGI, Rolling Meadows, IL.

Jirasek, V. (2012), "Practical application of information security models", *Information Security Technical Report,* Vol. 17 No.1–2, pp. 1-8.

Karokola, G., Kowalski, S. and Yngström, L. (2011), "Towards an Information Security Maturity Model for Secure e-Government Services: A Stakeholders View" in *Proceedings of the Fifth International Symposium on Human Aspects of Information Security & Assurance in London, UK*, pp. 58-73.

Park, J., Kim, S., Choi, B., Jun, M. (2008), "The Study on the Maturity Measurement Method of Security Management for ITSM" in *Proceedings of the ICHIT'08 in Daejeon, Korea*, pp. 826-830.

The Open Group (2011), *Open Information Security Management Maturity Model* (O-ISM3), Van Haren Publishing.

Walker, A., McBride, T., Basson, G., Oakley, R. (2012), "ISO/IEC 15504 measurement applied to COBIT process maturity". *Benchmarking: An International Journal*, Vol. 19 No. 2, pp. 159-176.

Woodhouse, S. (2008), "An ISMS (Im)-Maturity Capability Model" in *Proceedings of the 2008 IEEE 8th International Conference on Computer and Information Technology Workshops in Sydney, Australia*, pp. 242-247.