Volume 1 No. 2, June 2011
International Journal of Information and Communication Technology Research

http://www.esjournals.org

Maturity Models in Information Security

Boris Stevanović
Faculty of Information Technologies, Tadeusa Koscuska 63, Belgrade, Serbia
boris.stevanovic@fit.edu.rs

ABSTRACT

This paper explains appliance of maturity models in information security. Two information security standards which are using maturity models are explained and compared.

Keywords: *Maturity Model, ISM3, SSE-CMM, Information security*

1. INTRODUCTION TO MATURITY MODELS

The idea of information security standards that have models with measurable effects on the business becomes more present in practice and more respected by experts. Maturity model (MM) can be described as structured set of elements that describe certain aspects of improvement (maturity) in the organization. Each maturity model can represent:

- First step of project
- Measuring benefits of some previous experience or project
- Factor that puts different goals together
- Framework for priority determination
- Explanation of the improvement that effects are bringing to organization [1]

This tells us that MM can be used as benchmark comparison tool, but also as a help to understand the effects that are expected from the organization.

The experts from *Carnegie Mellon University* have recognized the good idea that Maturity Models brings, and developed *Capability Maturity Model* (CMM) that is used as a tool for measuring performances of the development process of software engineers and the software they develop. As the expected output of every information security standard is the admissible level of information security materialized through ISMS some organizations have managed to adjust CMM for measuring the effects of ISMS from the business aspect of the organization, and gives the management benchmark tool for the evaluation of the benefits that standards are bringing to organization.

The procedure of getting a good MM for the specific case is not simple. Generally, the idea of implementation of these models was generated by empiric observation of the software methodologies, like OWASP, CLASP, *Microsoft Security Development Lifecycle and* others. In the same way, the generation of the models cannot be uniquely determinate, because every organization has different combination of the goals, processes and wanted effects [2].

The level of improvement that some effect gives to the business depends on organizational processes and their specific goals and also on dedication of the resources to the general business goal. Each of these processes must implement certain activities that support the general goal, and verify them in order to measure the effect of the specific activity. Specific goals bring specific activities with the characteristics that are related to the activities for general goals.

An example of metamodel for better understanding of the maturity model concept is given in the figure below

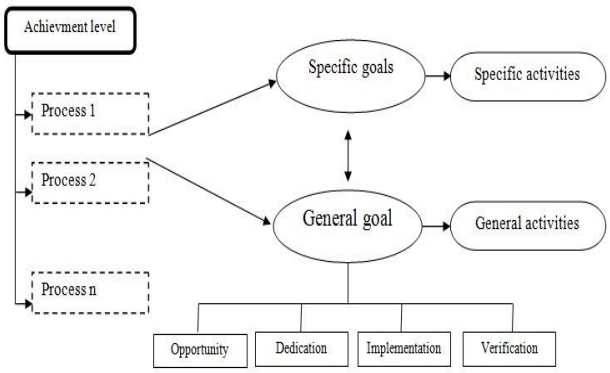

Figure 1 Example of MM metamodel

The idea of adding MM to some of the information security standards emerged from the fact that the information security is the result of many activities. Improvement of information security brings many changes to the organization, and that is something that doesn't happen and that isn't accepted overnight. Those who are introducing some of the Maturity Models to the process of building ISMS should take care of the specific circumstances of the situation and of the fact that a certain already existing solution from the practice can be applied everywhere.

Most of the emerging frameworks, that give the guidelines for building MM for security standards, stress the importance of:

- Legal regulations
- Identification of the resources and risk
- Development methodology
- Post implementation [2]

Activities that are related to legal regulations must: prepare, organize, manage and measure the influence of ISMS on the legal business of the organization. The controls that measure the adjustment of ISMS with legal regulations and prepare the changes of existing internal politics that should be adjusted to new security mechanisms appear here. In this phase, attention is also paid to staff training.

Understanding the risk has the inquiry function of gathering the corporate knowledge and information that ISMS is affecting. The resources that are used by three categories: attack models, security system design and the standards, are being collected. In the third step it comes to the already mentioned empiric part. Using some of the recognized methodologies for software development and security system building, it passes to designing system architecture, implementation and testing of the ISMS. In this phase, the tools for security testing and Quality assurance tests are used.

Most software development methodologies, and also the security MMs development methodology contains post implementation of some form. Constant testing, pen tests, testing of equipment and software environment, experimenting with the system configuration, are just some of the aspects attention must be paid on in order to maintain admissible level of security. If model results fall below the expectations, management comes to the phase of post implementation in which the performances of the system are getting improved, and thus the achieved level of security is maintained or even over passed. These guidelines in standards are being observed as the levels of standard achievement that determine the complexity and the price of standard or ISMS implementation.

2. ISM3

Information Security Management

Maturity Model or ISM^3 (more often – ISM3) represents one of the standards from the information security area, whose main goal, apart from achieving the admissible level of security, is achieving business results. Although it is represented, by it`s authors, as a progress in the perception of information security, some similarities in the applicability of the solutions with all previously explained standards can be noticed. The idea of achieving business results, in spite of the information security issues, appears also with COBIT. It should be underlined that the other standards don`t mention explicitly the way of maintaining efficient business, but they do imply that the business continues in spite of the security issues. Maturity Model, which is integrated into this standard, gives management the tool for measuring business results and that is why ISM3 is characteristic compared to all the other standards. Last revision is from 2009.

ISM3 is process oriented approach, like ITIL. According to this standard, management activities must follow different categories of the process:

- **Risk assessment** – discovering the threats, attacks, vulnerabilities, in order to have the whole picture of the system security and to determine protection priorities, in every moment
- **Surveillance** – Comparison of the current condition of the ISMS with the projected, documented system must be done in every moment
- **Adjustment** – surveillance is of the internal character, but the comparison must be carried out in relation to some externally defined systems
- **Testing** – Constant testing of whether the system inputs give satisfying outputs
- **Improvement** – It is complementary with the testing;
- Following the outputs and looking for the possibilities for their improvement
- **Optimization** – An effort to lower input resources, with the same quality and quantity of the outputs [3]

Measurability is something new that ISM3 brings to information security standards. With MM being the integral part of the standard, it is necessary to give management the tool for identifying which benefits ISMS gives to the organization, which processes can be improved and in what extent. While building metrics, the authors of the standard didn't consider the outputs to be directly related to the achievement of business goals. They have given up this approach because of the specificity of the problem, which may be considered to be an unnecessary investment or a mere cost. ISM3 is focused on measurement of these processes that are under direct control of ISMS. They are:

- Number of outputs in a specific period of time
- Proportion of the system provided by the processes
- Number of system changes
- Availability of the system and interruption frequency

Finding the border value, in relation to which the result requires special treatment, is an often problem. As a solution, authors have chosen control charts, the method that shows whether the outputs of business processes are statistically predictable. An ISM is a standard that considers itself to be "business friendly", being reliable,

accessible, scalable, compatible and open. It allows the possibility of adjustment to the existing ISMS solution and it increases the level of security by its MM. Authors recommend the "top-down" approach in using it, which considers business goals to be the most important, and they want to achieve admissible level of information security by designing ISMS following the guidelines for this standard.

3. SSE-CMM

System Security Engineering Capability Maturity Model – SSE-CMM is a standard of similar characteristics like ISM3, but of the smaller extent and with simpler MM. SSE-CMM describes the basic characteristics that an organization must provide in order to achieve the admissible level of information security. Like ISM3, SSE-CMM is also process oriented, but it`s character is strictly technical and it doesn`t treat business result as a main goal of MM. This standard is intended to be used as a basis for designing ISMS that can be used as:

- Basis of security architecture
- Standard mechanism that the consumers can use to measure and asses security level
- The tool for further development of security mechanisms [4]

The authors of the standard claim that the benefits of using their methodology are achieved through: continuity, repetitiveness, efficiency and acceptability of the processes that are carried out in the organization, and are protected by security mechanisms.

As with ISM3, it has the process metrics which measures, quantifies the results that MM achieves. Unlike ISM3, SSE-CMM introduces the concept of security metrics. For every process that is important from the security aspect, SSE-CMM identifies entities that are being followed and that are measurable. Security attributes that follow it and that represent the basis for measurements are added to every entity. Units of measurement can be the simplest physical units (frequency, number of iterations, etc.), but also the more complex, statistical ones, and others.

These measurements are very important for the management that is often faced with the great number of complex questions from this area and thus the simplicity of the metrics can help them to find the answers and bring the decisions about information security.

4. ISM3 AND SSE-CMM COMPARISON

Similar as for comparing standards that do not have MM for comparing ISM3 and SSE-CMM it is important to identify the criteria of comparison. Mitigating circumstance is that both standards are specialized and they look at the problem of information security from similar perspective.

Table 1 Comparison of ISM3 and SSE-CMM

Criterion	ISM3	SSE-CMM
Number of achievement levels	5	5
Paradigm	Process oriented	Process oriented
Goal	Admissible level of security with maximal business result	Secure and quality ISMS with least expenses
Input	Yes	Yes
Output	Yes	Yes
Metrics	Yes	Yes
Compliance	Yes with ISO 27001	Partly with ISO 27001; Integrated in ISO 21827:2008
Approach	Top-down	Bottom-up
Extent	Strictly	Technological, behavioral
Improvement	Continuously through metrics	Cyclically through outputs
License	Commercial	Free
Last update	April 2009	Jun, 2008

It is important to emphasize that there are two essential differences between the two standards that can be seen in the table 1. Those are: approach to standard implementation and the price of introduction. While ISM3 is oriented on business result achievement, which is on the top of the priority list, SSE-CMM is focused primarily on information security, and the effect on business is measured during the implementation.

ISM3 is, thus, focused on the Top-down approach, from the most important goal of the organization, to lower ones, including information security. SSE-CMM uses Bottom-up approach, in which it goes from information security, as the basis, and other goals of the organization depend, in great extent, from it [5].

The other big difference is in the price of implementation. Although the number of achievement levels is in direct correlation with the price of introduction that is not critical factor in the comparison of these two, because the number is the same. Also, the common process orientation does not represent the key price difference. ISM3 is a commercial standard, which cannot be downloaded for free from the Internet, unlike SSE-CMM, and it is also adjusted with ISO 27002:2005, standard expensive to introduce, so the price of its introduction is much bigger than the introduction price of SSE-CMM. It should be taken into account that SSE-CMM is older and needs revision more than ISM3, so it is doubtful if introduction of older standard can help management to choose it despite its free license.

REFERENCES

[1] Morton A., Performance Metrics for All, Inernet Computing, vol 3., no 4., pp 82-86, 2009

[2] Schneidewind N, "Metrics for Mitigating Cybersecurity Threats to Networks," IEEE Internet Computing, vol. 14, no. 1, pp. 64-71, Jan./Feb 2010

[3] ISF, ISM3 Compared to ISO27001, ISM3 Consortium, 2009

[4] System Security Engineering, SSE-CMM 3.0, System Security Engineering, 2003

[5] Viega A., Eloff J.H.P., A framework and assessment instrument for information security culture,Computers & Security, Volume 29, Issue 2, March 2010, Pages 196-207