Information Security Maturity as an Integral Part of ISMS based Risk Management Tools

Ben Fetler, Carlo Harpes
itrust consulting s.à r.l.
Niederanven, Luxembourg
e-mail: fetler@itrust.lu, harpes@itrust.lu

***Abstract*—Measuring the continuous improvement of Information Security Management Systems (ISMS) is often neglected as most organizations do not know how to extract key-indicators that could be used for this purpose. The underlying work presents a six-level maturity model which can be fully integrated in a risk management tool and helps to define key indicators for measuring the improvement of an ISMS. Furthermore, the proposed model establishes on how far the increase of maturity can help to mitigate information security risks and finally, a cost-benefit equation is presented which can be used to quantitatively justify the increase of maturity of an ISMS and to establish an action plan increasing the maturity.**

Keywords-Information Security Management System; Maximal Efficiency Rate; Return On Security Maturity Investment; Information Security Risk Analysis; Security Maturity.

I. INTRODUCTION

The need to set up an Information Security Management System (ISMS) in organizations that treat critical or sensitive information is growing. Constantly new vulnerabilities, exploits and threats express the necessity to set up a managed system that is perfectly adapted to the fast evolving information and communications technology (ICT) environment.

One major difficulty of an ISMS is on how to measure its efficiency, quality or more generically its maturity. By considering the fact that an ISMS is based on continuous improvement, it is important to measure its maturity evolution. The maturity level of an ISMS can be used as a key indicator by Information Security Managers to monitor its efficiency and improvement. For example, young ISMS with low maturity often show similar deficits, such as non-formalized processes or security instructions, untested security procedures or unverified security statements.

A key element of an ISMS that follows the international standard ISO/IEC 27001 [1] is the periodic assessment of risks that includes identification of vulnerabilities, threats as well as estimation of their probability of occurrence and possible impact. During a risk analysis, the organization establishes an overview of currently implemented security controls and sets up an action plan to counteract non-acceptable risks. The aim of the underlying work is to introduce a maturity model that is part of the risk analysis process with the objective to determine the maturity level of security controls, the effect of missing maturity on risks and cost of increasing maturity. Finally, this model allows to define a risk treatment plan combining actions to increase security and actions to increase maturity.

To prove that the security maturity model can be adapted to its context, the model has been tested for a small to medium-sized enterprise (SME).

The rest of this paper is organized as follows. Section II presents related work considered for developing the security maturity model. Section III describes the security maturity model. Section IV introduces the concept of the return on security maturity investment. Section V closes the paper with the conclusion and outlook on further work.

II. RELATED WORK

Several Maturity Models exist for determining the quality of organizational processes. Two common models (Capability Maturity Model Integration (CMMI) [2] and ISO/IEC 15504 – Software Process Improvement and Capability Determination (SPICE) [3]) have been analyzed to collect valuable information that could be reused for the setup of a Maturity model related to Information Security.

The National Institute of Standards and Technology (NIST) developed an IT Security Maturity Model, including several maturity levels and related tasks [4]. These standardized tasks have been reused and partly adapted to fit to the Security Maturity Model described in this paper.

Furthermore, there have already been first tries of including maturity in risk assessment tools [5-6]. Unfortunately, in those tools, maturity is not handled as an evolution indicator but rather as a substitute for indicating the implementation rate of security controls or as a generic and qualitative indicator with no further details on how maturity is measured.

Finally, the quantitative computations that are made to compute the cost-effectiveness of increasing Security Maturity are based on the mathematical models used by the risk assessment methods ISAMM [7] and TRICK Service [8].

III. SECURITY MATURITY MODEL

The elaborated security maturity model is based on a multi-level approach (Section III.A.) with associated Maximal Efficiency Rates (Section III.B.) having a direct influence on the estimated implementation rates of current security controls. This direct influence of maturity levels on the implementation rate of security controls allows establishing a

 ISBN: 978-1-61208-493-0

link between security maturity and the assessment of the overall information security status of an organization.

A. Security Maturity Levels (SML)

The elaborated security maturity model contains six levels with associated tasks that have to attain a predefined implementation rate before a higher level can be reached.

The tasks are categorized into five different domains: "Policies" (Pol), "Procedures" (Pro), "Implementation" (Imp), "Test" (Tes) and "Integration" (Int). Every task aims to cover a different aspect of security maturity. The tasks and the different maturity levels are based on the standard NISTIR 7358 [4]. However, the tasks have been reorganized to create an interdependency of the tasks, so that it should not be possible to reach a high SML without fulfilling the tasks of the lower SML's.

In the following, the six SML's and their associated tasks will be presented.

Security Maturity Level 0: Incomplete - No specific tasks available for Security Maturity Level 0, which is reached by default. The associated security controls are quite superficially implemented, typically by a small ISMS team which does not show any systematic approach.

Security Maturity Level 1: Performed - Pol 1: Formal, up-to-date documented policies exist and are readily available to employees; Imp 1: Procedures are communicated to individuals who are required to follow them; Pro 1: Formal, up-to-date, documented procedures are provided to implement the security controls identified by the defined policies; Tes 1: Tests are routinely conducted to evaluate the adequacy and effectiveness of all implementations.

Security Maturity Level 2: Managed - Pol 2: Policies establish a continuing cycle of assessing risk and implementation and uses monitoring for program effectiveness; Imp 2: Information security procedures and controls are implemented in a consistent manner everywhere the procedure applies and are reinforced through training; Pro 2: Procedures clarify where the procedure is to be performed, how the procedure is to be performed, when the procedure is to be performed, who is to perform the procedure, and on what the procedure is to be performed; Tes 2: Tests ensure that all policies, procedures, and controls are acting as intended and that they ensure the appropriate information security level.

Security Maturity Level 3: Established - Pol 3: Policies are written to cover all major facilities in scope; Imp 3: Ad hoc approaches that tend to be applied on an individual or a case-by-case basis are discouraged; Pro 3: Procedures clearly define Information security responsibilities and expected behaviors for (1) asset owners and users, (2) information resources management and data processing personnel, (3) management, and (4) Information security administrators; Tes 3: Effective corrective actions are taken to address identified weaknesses, including those identified as a result of potential or actual information security incidents or through information security alerts issued by national Computer Security Incident Response Teams (CSIRT) or Computer Emergency Response Teams (CERT).

Security Maturity Level 4: Predictable - Pol 4: Policies are approved by key affected parties; Pro 4: Procedures contain appropriate individuals to be contacted for further information, guidance, and compliance; Tes 4: Self-assessments, a type of test that can be performed by company staff, by contractors, or others engaged by company management, are routinely conducted to evaluate the adequacy and effectiveness of all implementations; Tes 5: Independent audits are an important check on company performance, but are not to be viewed as a substitute for evaluations initiated by company management; Tes 6: Information gleaned from records of potential and actual Information security incidents and from security alerts, such as those issued by software vendors are considered as test results. Such information can identify specific vulnerabilities and provide insights into the latest threats and resulting risk.

Security Maturity Level 5: Optimized - Int 1: Policies, procedures, implementations, and tests are continually reviewed and improvements are made; Pol 5: Policies delineate the information security management structure, clearly assign Information security responsibilities, and lay the foundation necessary to reliably measure progress and compliance; Pol 6: Policies identify specific penalties and disciplinary actions to be used if the policy is not followed; Pro 5: Procedures document the implementation of and the rigor in which the control is applied; Tes 7: Evaluation requirements, including requirements regarding the type and frequency of testing, are documented, approved, and effectively implemented; Tes 8: The frequency and rigor with which individual controls are tested depend on the risks that will be posed if the controls are not operating effectively.

B. Security Maturity Parameters

The following section presents the key parameters of the developed security maturity model. All parameters are customizable and can be fine-tuned according to the specificities of the organization in focus.

1) Implementation Scale for Security Maturity Tasks.

This section defines a scale for measuring the implementation rate of the different security maturity tasks. The implementation scale includes five different levels as presented in Table 1 below.

TABLE I. IMPLEMENTATION SCALE OF SECURITY MATURITY TASKS

Level	Explanation	
Not achieved	There exist no proofs that the Security Maturity tasks of the corresponding Security Maturity Level are implemented.	
	Acronym: N	Range: 0%
Rudimentary achieved	There are none or only few proofs available that the Security Maturity tasks of the corresponding Security Maturity Level are rudimentary implemented.	
	Acronym: R	Range:]0%, 20%]
Partially achieved	There are none or only few proofs available that the Security Maturity tasks of the corresponding Security Maturity Level are partly implemented.	
	Acronym: P	Range:]20%, 50%]
Largely achieved	There are proofs available which show that the Security Maturity tasks of the corresponding Security Maturity Level are essentially fulfilled.	
	Acronym: L	Range:]50%, 80%]
Fully achieved	There are proofs available that the Security Maturity tasks of the corresponding Security Maturity Level are fully implemented.	
	Acronym: F	Range:]80%, 100%]

2) Task Overview per Security Maturity Level

Each SML has related tasks which have to attain a predefined implementation rate in order to pretend that the SML is reached. The following list exemplary shows the 6 SML's and the related tasks with their required implementation rates:

SML 0: Reached by default – no tasks have to be fulfilled.
SML 1: Pol1, Pro 1, Imp 1, and Tes 1 have to be largely achieved
SML 2: In addition to SML 1, Pol 2, Pro 2, Imp 2, and Tes 2 have to be largely achieved
SML 3: In addition to SML 2, Pol 3, Pro 3, Imp 3, and Tes 3 have to be largely achieved
SML 4: In addition to SML 3, Pol 4, Pro 4, Tes 4, Tes 5, and Tes 6 have to be largely achieved
SML 5: All tasks have to be fully achieved

3) Maximal Efficiency Rate

By looking at the previous sections, it is possible to conclude that the higher the reached SML the higher the efficiency of the security treatment in the organization. Hence, a fully implemented security control cannot be fully efficient if the associated SML is not the highest possible.

In order to include these reflections in a risk assessment approach, we introduce the notion of Maximal Efficiency Rates (MaxEffRate) associated with the different SML's (see Table II below).

With the help of collected data during the case study with the SME, the different Maximal Efficiency Rates of Security Maturity Levels can be fine-tuned.

TABLE II. SECURITY MATURITY LEVELS WITH ASSOCIATED MAXIMAL EFFICIENCY RATE

SML	Qualification	MaxEffRate (linear)	MaxEffRate (tailored to our use-case)
0	Incomplete	10%	20%
1	Performed	20%	40%
2	Managed	40%	50%
3	Established	60%	70%
4	Predictable	80%	90%
5	Optimized	100%	100%

The now determined MaxEffRate per SML can be used to calculate the implementation rate of a security control taking into account the SML. For example, this allows to model the fact that a security control can be fully implemented but only have a small efficiency, if the associated SML is low.

The following formula is used to calculate an improved implementation rate of a security control taking security maturity into account, called the Maturity-based Effectiveness Rate (MER):

$$MER = IR * MaxEffRate_{SMLi} \quad (1)$$

where

- MER= (Maturity-based Effectiveness Rate) be the improved implementation rate of the security control in focus taking Security Maturity into account;
- IR=the current implementation rate of the security control;
- $MaxEffRate_{SMLi}$ be the maximal efficiency rate of the current Security Maturity Level (SML_i).

Example: For the considered SME, we determined that a security control called "Implement an antivirus solution for every system in use" has been applied to 50%. The SML of the antivirus control is 3 because all requirements of SML 3 have been fulfilled (e.g., validated policy in place, requiring the implementation of antivirus solutions) but some tasks of SML 4 are still not satisfied (e.g., no audit was done to verify the well-functioning of the antivirus solution). Thus we have for the antivirus control an implementation rate (IR) of 50%, and a MaxEffRate of 70% which gives a MER of 50%*70%=35% for the antivirus security control.

This example demonstrates that if the maturity of the ISMS in focus has not reached the highest level, the implemented security controls cannot be fully efficient. This conclusion is not astonishing as we can pretend that if for example policies, procedures, implementations, and tests are not continually reviewed and no improvements are made (see Task Int 1 of SML5), the underlying security controls cannot be fully efficient.

Figure 1 illustrates the impact of Security Maturity on the implementation rate of a security control where Security Maturity is taken into account. The figure shows the SME-tailored model.

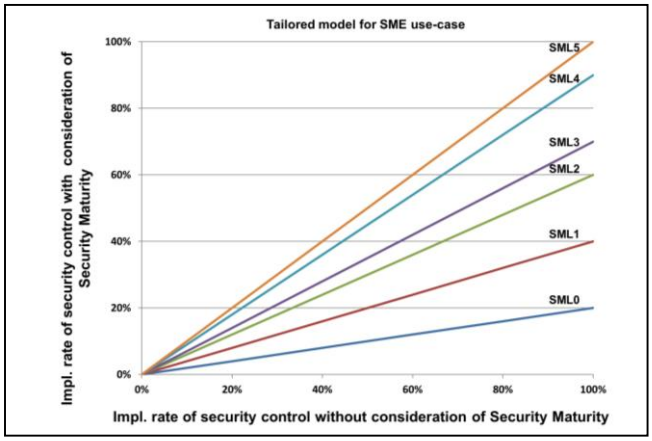

Figure 1. Impact of Security Maturity on implementation rate of security controls (MaxEffRate tailored to SME use-case)

IV. RETURN ON SECURITY MATURITY INVESTMENT (ROSMI)

The introduced maturity model offers the possibility to compute the Return On Security Maturity Investment (ROSMI) which can be used to justify the costs resulting from the resources to invest for implementing the tasks to increase the security maturity (resources are needed to fulfill the different tasks presented in Section III.A.).

The ROSMI is based on the Return on Investment (ROI) and Return On Security Investment (ROSI) concepts [7], [9-10], which consist of investing a certain amount of money with the aim to reduce the risk and such in return save more money than initially invested. This risk reduction is expressed as the difference of the Annual Loss Expectancy (ALE) before, and the ALE after implementing security controls.

The ROSMI, when raising the current SML to the SML above ($ROSMI_{SML_{i\rightarrow i+1}}$), is expressed as the difference between

the ALE reductions generated by the raise of the current SML ($\Delta ALE_{SML_{i\rightarrow i+1}}$) and the costs incurring by the increase of the SML ($Costs_{SML_{i\rightarrow i+1}}$):

$$ROSMI_{SML_{i\rightarrow i+1}} = \Delta ALE_{SML_{i\rightarrow i+1}} - Costs_{SML_{i\rightarrow i+1}} \quad where\ 0 \leq i \leq 4 \qquad (2)$$

The ALE Reduction (ΔALE) emerging from the raise of the current SML ($\Delta ALE_{SML_{i\rightarrow i+1}}$) is based on the quantitative risk assessment method, ISAMM [7] and TRICK Service [8].

The first step consists in computing the ALE reduction of every security control based on the increase of the current SML ($\Delta ALE_{M,SML_{i\rightarrow i+1}}$):

$$\Delta ALE_{M,SML_{i\rightarrow i+1}} = ALE_{e_M,SML_i} * RRF_M * e_M * \frac{(maxEffRate_{SML_{i+1}} - maxEffRate_{SMLi})}{1 - RRF_M * maxEffRate_{SML_i} * e_M} \quad where\ 0 \leq i \leq 4 \qquad (3)$$

The risk reduction factor of a security control M (RRF_M) is introduced in the TRICK Service methodology [8] and represents a factor which indicates the impact of a security control on the risk exposure of an asset.

The second step consists in summing all ΔALE of the security controls to get the general ALE reduction resulting from the raise of the current SML:

$$\Delta ALE_{SML_{i\rightarrow i+1}} = \sum_M \Delta ALE_{M,SML_{i\rightarrow i+1}} \quad where\ 0 \leq i \leq 4 \qquad (4)$$

The resulting ALE reduction gives a clear indication of the influence that the increase of maturity has on risks that a company is facing to and can be used for the ROSMI computation.

V. USE CASE

The underlying maturity model has been applied in the context of a risk analysis for an SME offering trusted third party services. During the risk assessment, the current implementation levels of ISO/IEC 27002 security controls have been estimated and the current SML of each ISO/IEC 27002 chapter has been computed by determination of the implementation rate of the SML related tasks. Based on the now identified SML per ISO/IEC 27002 chapter, it was possible to compare the current implementation rate with the MER. Some chapters showed a high implementation rate but low maturity and revealed the need of incrementing the SML of the different ISO/IEC 27002 chapters to get more efficient security controls having a better mitigation effect on the current risk level of the SME.

The next step consisted in getting an idea about what security maturity tasks to implement first for getting the best effect on the MER of the security controls. For doing so, the workload for implementing the security maturity tasks has been estimated. These information were used as input to compute a prioritized action plan by using the ROSMI formula, showing which tasks to implement first to get the best effect on the effectiveness of the ISO/IEC 27002 security controls.

VI. CONCLUSION AND FURTHER WORK

This work demonstrated that the maturity of an implemented ISMS can be used as a key-indicator with which it is possible to assess the effectiveness of security controls.

Increasing the maturity of an ISMS can by itself be seen as a security control that is used to improve the current security level of an organization.

Furthermore, the presented maturity model enables to illustrate the evolution of information security in an organization and can be used as a basis for taking decisions, related to the continuous improvement of an ISMS.

Finally, the elaborated concept that is already part of the risk assessment tool TRICK Service, now has to be applied for further organizations in order to setup an knowledge base with which it will be possible to adapt the MaxEffRates (see Section III.B.2) to the different types of organizations and proof the feasibility of the tasks related to the different SML's. It is planned to prove the concept for critical infrastructures in the context of further research projects.

ACKNOWLEDGMENT

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 318003 (TREsPASS). This publication reflects only the author's views and the Union is not liable for any use that may be made of the information contained herein.

REFERENCES

[1] ISO/IEC 27001:2013 Security techniques — Information security management systems — Requirements

[2] Software Engineering Institute, CMMI® for Development, Version 1.3, "Improving processes for developing better products and services", Carnegie Mellon University, 2010.

[3] ISO/IEC 15504-5:2012 Process assessment – Part 5 : An exemplar software life cycle process assessment model

[4] P. Bowen and R. Kissel, National Institute of Standards and Technology. Program Review for Information Security Management Assistance (PRISMA). NISTIR 7358, Gaithersburg, 2007.

[5] SerNet GmbH. verinice. Retrieved March 28, 2016 from http://www.verinice.org

[6] Microsoft Corporation. Microsoft Security Assessment Tool 4.0. Retrieved March 28, 2016 from http://www.microsoft.com

[7] C. Harpes, A. Adelsbach, S. Zatti, and N. Peccia, "Quantitative Risk Assessment with ISAMM on ESA's Operations Data System," In: The 4th ESA International Work-shop on Tracking, Telemetry and Command Systems for Space Applications, 2007.

[8] European Network and Information Security Agency, Inventory of Risk Management / Risk Assessment Tools - TRICK Service. Retrieved April 8, 2016 from, http://www.enisa.europa.eu

[9] European Network and Information Security Agency, "Introduction to Return on Security Investment - Helping CERTs assessing the cost of (lack of) security,". Retreived April 8, 2016 from: http://www.enisa.europa.eu

[10] W. Sonnenreich, J. Albanese, and B. Stout, "Return On Security Investment (ROSI): A Practical Quantitative Model," Journal of Research and Practice in Information Technology, 2006, vol. 38, pp. 45-56

 ISBN: 978-1-61208-493-0