ISSN 2278-3091
Volume 9, No.1.1, 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse5491.12020.pdf
https://doi.org/10.30534/ijatcse/2020/5491.112020

The Framework to Analyze the Factors and Aspects of Information Security Program Maturity Grid

Asadullah Shaikh
College of Computer Science, and Information Systems,
Najran University, Najran, Saudi Arabia
asshaikh@nu.edu.sa

ABSTRACT

Information Security becomes the basic need day by day for the individuals and the organizations. In this paper, we present the framework that analyzes the attribute of the Information Security Program Maturity Grid with the help of two reference models. To accomplish this goal, interviews with professional organizations have been conducted to find which attributes, regarding information security maturity is essential to consider. The measurements of the information Security Program Maturity Grid are also discussed.

Key words : Security Aspects, Maturity Grid, Information Security attributes.

1. INTRODUCTION

Maturity levels can be utilized in a business point of view. The maturity value can be utilized for business reasons, for instance, to introduce the association's level of development. The development level can likewise be utilized in business co-activity settings, for instance, to discover the development level of providers and other co-employable associations. Ensure that providers and co-usable associations don't comprise the most fragile connection of the data framework utilized by numerous associations [1]. A target estimation of the development level of the provider or co-operative organizations can be performed to ensure they are not a risk to data security. The degree and cost of this estimation are subject to the standard utilized for deciding the development level.

This paper presents the consequences of an examination in the data security development field, made by understudies of the Software Engineering Security Management Principles. The principal focal point of the paper is to explore a data security development basis, the Information Security Program Maturity Grid. This report presents the foundation, procedure, acknowledgment, results, end, and conversation of this examination [2].

This examination depends on the findings in the article, towards the development of data security development criteria [1] where it is presumed that: "The data security program development matrix can adapt well to advancements. Truth be told, on the most significant level (of development) it necessitates that the association's security individuals to participate in look into ventures, in this manner requiring associations to make advancements."

There are two main security criteria, i.e., SSE CMM, and Murine Carpenter development standard, and in the discussion of those, it is communicated that they "will in general pressure the utilization of existing and functional practices for making sure about associations data frameworks. Thus, these criteria face three issues that should to be moved. "To begin with, it supports neither creative reasoning nor change in worldview/investigates the program. It rather maintains the utilization of existing practices". With this it is concluded that SSE CMM isn't a rule to be utilized in college instructions. It additionally expresses that "the college degree is maybe the best gathering for accomplishing change through training". The first issue referenced that "associations which embrace advancements at their primary serious procedure gain nothing from the adjustment of these development criteria." The second and last issue expressed is that "associations utilizing cutting edge strategies/systems may perform gravely in development estimations since the old criteria don't perceive new techniques/methods".

The Information Security Program Maturity Grid is by all accounts a creative and useful basis for deciding the data security development level. Be that as it may, can this rule adapt to the advancements in associations. The examination will break down the data security development field and research [2].

2. PROBLEM DESCRIPTION

The purpose of this investigation is to investigate the model, the Information Security Program Maturity Grid. This criterion can be used to measure the information security maturity level according to the conceptual analysis of the Information Security Program Maturity Grid.

Hence, this investigation will answer a question.

What value could be seen by the Information Security Program Maturity Grid?
We further divided this investigation into two main objectives:

1. *What is significant for the the organizations to measure with the information security maturity?*
2. *How significant is the estimation of the data security development for the ornization?*

This examination is directed into two sections. A literature study, including the Information Security Program Maturity Grid, is researched, and two different paradigms used to decide the data security development level in associations are concentrated nearer. Right now, ISPMG will be concentrated just as SSE CMM [3] and SPICE [4].

In order to determine what is important to measure with an information security maturity level of an organization, the other part of the study will be conducted as open interviews, this part of the study will answer objective 1 and 2.

4. RESARCH FRAMEWORK

This section provides the introduction to information security which is based on three maturity methods.

A. Information Security

Individuals and organizations are reliant on information. Information technology (IT) have been an issue since the humans started to communicate. Since people began to impart along these lines data security has been an issue, and the refinement of the techniques for ensuring the data has advanced from that point forward. This development of securing data has from that point forward, after the rising advancements of imparting. Because of the utilization of disseminated systems, specialized assurance arrangements have been grown quickly for example firewalls and against anti-virus programs. Be that as it may, from the data framework (IS) perspective, the main restricted arrangement has been created, for example step by step instructions to structure a safe IT System [5].

Today, most business associations' data (exclusive information) is stored electronically in databases. Before they stored their data in a paper-based way, and in this way the way toward making sure about data resources contrasted from how it is made sure about today. Before delicate information and data were put away as a printed copy in records and safely secured into cupboards a bolted room. Right now, number of safety efforts were thought about to guarantee that only approved staff approached this data. Since everything was unique and confined previously, just physical security was enough to guarantee the security of organizations' data resources. Therefore, information security became the basic need of the society.

B. Essentials of Information Security

Data security is tied in with controlling access to data for guaranteeing secrecy, uprightness, and accessibility [6-8]. Data security is additionally characterized by the International Standards Organization ISO-17799 [9].

- Confidentiality - guaranteeing that data is open just to approved people
- Integrity - defending the exactness and culmination of data and handling strategies
- Availability - guaranteeing that approved clients approach data and related resources when required

Information security deals with the protection, deletion, fabrication, destruction (whether accidental or intentional) and modification of information assets.

C. The Maturity Standards of Information Security

There exist strategies for estimating data security of an association with the executives arranged development principles. These sorts of benchmarks are the promising developments [10] of the data agenda the board standard branch. The destinations for these models are to propel security building with characterized, develop and quantifiable exercises. Further these measures additionally give associations a device to start and support a nonstop procedure improvement action. For programming creating associations these models give key and strategic heading to surveying, estimating, and anticipating risks, and propose a scope of security controls concentrated on defending data resources. Following such a model, programming advancement associations will be able to guarantee that their product improvement process is lined up with, and bolsters, the business needs of the association. Advantages for the product clients when receiving such a model are for example that they will have the option to decide the capacity of programming providers and evaluate the hazard associated with choosing one provider over another. Security is a genuine client concern. In any case, if the present patterns proceed, it would be a lot of more awful later and may in the long run drive out organizations from the market that don't address these issues now and become qualified later on.

D. Security Insights in Capability Maturity Model (CMM)

The Information Security Program Maturity Grid is a method based on the Capability Maturity Model (CMM) standard [11]. This grid seems to be a simple way to determine the maturity level of an organization. Due to the connection between process development and risk decrease, it appears that the framework could be custom fitted for use by directors in evaluating an undertaking's data security development level.

The first dimension of ISPMG aims to classify the organizations into one of five maturity level which is:

- Uncertainty
- Awakening
- Clarification
- Wisdom
- Generosity

The second component of this framework proposes to assess the development through various estimation classes as shown in table 1. The estimation classifications for assessing an associations data security program development are:

- management comprehension and disposition
- security association status
- incident dealing with
- security financial aspects
- security improvement activities

Table 1: A matrix level in the ISPMG

Security Maturity Stage	**Measurement Categories**				
	Management	Associations	Incidents	Financial	**Improvements**
Stage 5					
Stage 4		X			
Stage 3	X	X	X		**X**
Stage 2	X	X	X	X	**X**
Stage 1	**X**	**X**	**X**	**X**	**X**

E. Software Process Improvement and Capability Determination (SPICE)

Software Process Improvement and Capability Determination (SPICE) [12] is a worldwide activity to help the International Standard ISO/IEC 15504 for (Software) Process Assessment. It is a system produced for crossing over any barrier among American and European evaluation techniques which were not perfect. The American and Europeans have various ways to deal with programming process appraisal and thusly it was expected to blend and incorporate the various methodologies into a compelling universal standard.

In order to identify the maturity of the processes, SPICE provides a scheme to follow in order to come up with a result regarding to the process assessment as shown in figure 1.

The SPICE framework proposes to survey the ability of an association on a scale from 0 to 5. The objective of this assessment is to connect with an improvement procedure, if necessary. With SPICE, each procedure is surveyed exclusively and is assigned out a legitimate degree of development, to have the most exact investigation possible.

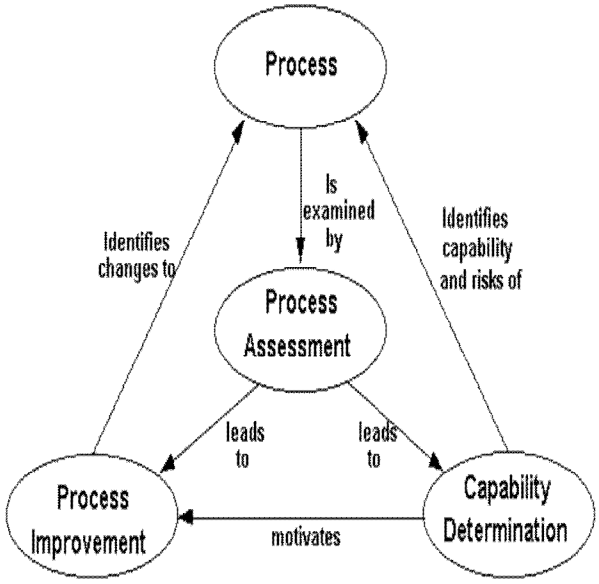

Figure 1 : The sections for identifying the capability of a process.

5. OPEN INTERVIEWS AND LITERATURE ANALYSIS

We selected two method of investigation, i.e., open interviews and literature analysis. The aim of the qualitative interview to distinguish properties and qualities of the subject under analysis. Accordingly, the determination of respondents will have an immediate effect on the consequence of the meeting. To research the correct subject, it is significant that the correct respondents are picked. The main question that was asked in the interview was "According to you, what are the important attributes to be included in the value of information security?"

A literature analysis is a systematic examination of a problem and should not be mixed up with a review of existing work. The different sources of information have different weights within the academic world. This is depending on the acceptance of the publisher within the scientific field, the process of review, the earlier knowledge within the field.

Scientific journals and conference proceedings could also be a good source of information. Journals and conference proceedings have the advantage of presenting the latest findings within the field, but they also have the disadvantage of being less accepted and may have less scientific importance. To assure the quality and acceptance of the journals and proceedings the supervisor and professors within the field should be consulted.

The expected result from the interviews is a list presenting the common attributes of information security and some specific attributes for information security maturity. The list will also present what value these attributes may have for the organizations and in what situations it may be valuable to communicate an information security maturity level.

The information security maturity levels of the participating organization are expected to be rather low.

The literature study is expected to result in a deeper understanding of the information security field and in an overview of current approaches to determine the information security maturity level of organizations. The literature study is also expected to present the purpose of the Information Security Program Maturity Grid (ISPMG), and what attributes that are of importance according to the method.

The match of the result from the open interviews and the literature study is expected to result in a list of common attributes and a list of missing attributes of the ISPMG.

6. RESULTS

Open meetings were directed with four organizations. Two of these associations were enormous global programming development organizations with a few thousand employees. The other two associations were smaller, with only a couple of representatives and with the principle center around creating security answers for different organizations.

The main question during these interviews was objective 1 and 2 stated in section 2 of this paper. The result of the meetings was a few properties. These properties were breaking down and accumulated in table 2. The characteristics right now the aftereffect everything being equal. All traits referenced during the four meetings have been incorporated and assembled right now. A few of the qualities were referenced by all organizations and have in this manner been intensified into characteristics speaking to the appropriate responses from even more than one respondent. The value segment is a description of how significant this property is considered by the respondents. The value is introduced as a clarification of how this characteristic impacts the association on the off chance that it isn't satisfied or what this trait can contribute with if it is actualized accurately. The circumstances section speaks to the circumstances when the characters can be important. The estimation of the trait is portrayed as far as inner and outer qualities. This segment presents if the qualities can be important inside, remotely or both inside and remotely. Inner is expressed if the property includes an incentive inside the possess association for instance to convey the static estimations of security. Outer is expressed if the character has an incentive outside the association, for instance for notice towards clients or helpful accomplices.

Table 2: The attributes for interview results

Characteristic	Value	Situations
Framework that defines the information security processes.	Return on security investments, the long term working plan.	**Internal** To communicate the static values of security.
External awareness (The awareness of trends and threats in the context and environment of the organization)	Crucial for risk management and strategic decisions.	**Internal** To make strategic decisions and to determine the priority of threats.
Internal awareness (Information security maturity should be concluded from the awareness of the personnel)	Crucial for having any kind of security within the organization.	**Internal** (Externally) To be aware of defects within the organization. To ensure the realizations of the processes. To determine the level of education needed among the personnel.
Catastrophe plan (Continuity plan, to be prepared)	Continues operation when exposed to an incident or catastrophe.	**Internal and externally** Business case. To minimize the economical effect of an incident.
Information Security Architecture	To assure that the right information is given to the right source. To assure that the security rules are up to date. (Practical function)	**Internal** To identify the level of tool support for information security.
Integrating information security in management systems	The level of strategic importance is affecting the security of the organization. Acceptance in the management is the factor that drives the security work.	**Internal** To ensure the acceptance of security within the organization. (Management level)
Risk management	Crucial for having the right level of security, in other words to have the right level of security.	**Internal** To ensure and identify assets.
Confidentiality	The foundation of information security.	**Internal and externally** Business case

Characteristic	Value	Situations
Integrity	The foundation of information security.	To determine security classification.
Availability	The foundation of information security. Lost of income if the information is unavailable.	
Validation (Traceability in a legal manner)	The foundation of information security.	**Internal and External** Legal aspects. Lifecycle of the information.
The security work is conducted by the organization it self.	Crucial for the realization of information security within the organization.	**Internal** To understand the underlying motivation for the security work.
None technical focus for the security work	High importance, the technical parts should be a result from the decisions on a higher level of organizational abstraction.	To determine the focus of the security work.
Knowledge about the abstraction level of the problem.	Lift problems to the right abstraction level.	**Internal and external** Direct the effort for the right level of abstraction.
Effort for security should be proportional towards decided maturity level of security. (Increased effort on higher levels)	Optimize the value of the security effort.	To analyze how well resources are being used.
Physical security	Categorization of security	**Internal (External)** To categorize the security work. To increase the business case for the organization.
Logical security	Categorization of security	
System security	Categorization of security	
Continues evaluation.	Continues evaluation of processes, new risks and organizational defects, this is important for the validity of the security.	To cope with new threats. To make risk assessments and to evaluate the strategically decisions.

6. CONCLUSION

In this paper, the key attribute of the Information Security Program Maturity Grid has been assessed and compared with the key attributes of the two reference models. Furthermore, interviews with professional organizations have been conducted to find which attributes, regarding information security maturity, they consider as an essential. It has been analyzed if the Information Security Program Maturity Grid does measure these attributes. The conclusion of this investigation is that the Information Security Program Maturity Grid is suitable for internal assessment of the information security maturity for organizations.

REFERENCES

[1] Siponen, M “Towards Maturity of Information Security Criteria: Six Lessons Learned from Software maturity Criteria” in Information management & Computer Security, Vol 10, No 5, pp 210-224. https://doi.org/10.1108/09685220210446560

[2] Stacey, T.R. “Information Security Program Maturity Program” in Information Systems Security, Vol 5, No 2, pp. 22-34.

[3] SSE-CMM official site, http://www.sse-cmm.org. Last Accessed on 2020-02-23

[4] Mitasiunas, Antanas, Leonids Novickis, and Rimas Kalpokas. "Security Process Capability Model Based on ISO/IEC 15504 Conformant Enterprise SPICE." Applied Computer Systems 15.1 (2014): 36-41.

[5] Hassanien, Aboul Ella, and Mohamed Elhoseny. Cybersecurity and Secure Information Systems. Springer International Publishing, 2019.

[6] Masala, Giovanni L., Pietro Ruiu, and Enrico Grosso. "Biometric authentication and data security in cloud computing." Computer and Network Security Essentials. Springer, Cham, 2018. 337-353.

[7] Graham, James, Ryan Olson, and Rick Howard, eds. Cyber security essentials. CRC Press, 2016. https://doi.org/10.1201/b10485

[8] Francia, Guillermo, et al. Computer and network security essentials. Springer, 2017.

[9] Nisaa, Nurul Fariidhotun, and M. Kom. "Technology Safety Audit in Computer Laboratories Using ISO/IEC 17799: 2005 (Case Study: FTK UIN SUNAN AMPEL SURABAYA)." (2019).

[10] Dzazali, Suhazimah, and Ali Hussein Zolait. "Assessment of information security maturity." Journal of Systems and Information Technology (2012).

[11] Paulk, Mark. "Capability maturity model for software." Encyclopedia of Software Engineering (2002). https://doi.org/10.1002/0471028959.sof589

[12] O'Connor, Rory, et al., eds. Software Process Improvement and Capability Determination: 11th International Conference, SPICE 2011, Dublin, Ireland, May 30–June 1, 2011. Proceedings. Vol. 155. Springer, 2011.