

A Reference Information Model to Information Security Service

Antonio Goncalves, INESC-ID Lisboa, Portugal, antonio.goncalves@inesc-id.pt
Anacleto Correia, CINA V Almada, Portugal, cortez.anacleto@marinha.pt
Marielba Zacarias, Universidade Algarve, Algarve, Portugal, mzacaria@ualg.pt

Abstract

Although the existence of an established body of knowledge, risk managers still strive to find a suitable risk information model that should be used in information security process. The purpose of this document is to capture key concepts of information risk management. It includes all information and / or assets associated with the information that are used in the organization or that may have an impact on information security. When it comes to implementation, information security risk management is a challenging process, because risk factors are constantly changing, due to rapidly changing technologies and the attacker's knowledge level. However, the main issue of our approaches is set a baseline to define the requirements for establishing, implementing, maintain and continually improving an information security management system.

Keywords: Information Security; Risk; Framework; Model.

1. INTRODUCTION

This paper details some key concepts related with information security risk assessment through the identification of threats and vulnerabilities that is carried out by risk team. The goal of an information security service based on risk management is to maximize the organization's output, while at the same time decreasing unexpected negative outputs generated by potential risks (Peltier, 2016) (Von Solms & Van Niekerk, 2013).

The outline of this paper is as follows. Section 2 presents some information regarding the concept of information security. section 3 presents an overview of concepts related with risk applied to information security. Section 4 describes the concept of risk management used to draw the proposed method. We conclude with recommendations, based on the problems found, as well as future work, in section 5.

2. INFORMATION SECURITY

Information security introduces an important definition in terms of the properties that information manipulation should have. These include availability, confidentiality, and integrity of information.

Availability refers to the fact that the information used by an organization remain accessible when they are needed. Thereafter, system failure is an organizational security issue (Andress, 2014).

Confidentiality refers mostly to restricting information access to those who are authorized. Organizations strives to control information access, since technology offers developments aimed at making information accessible to the many (Andress, 2014).

Integrity refers to maintaining the values of the information stored and manipulated, such as maintaining the correct meaning. Information integrity is commonly assured by using cryptographic or/and information replication strategies. The cryptographic tools are indeed used to sign single pieces of data, so that any faking information can be detected through signature validations (Andress, 2014).

3. RISK CONCEPT

Every organization is subjected to risks. Risks affect the path that organizations take to achieve their objectives. Risk identification is important, allowing early identification and resolution of an organization high-risk elements, effectively allowing organizations to adjust their operations accordingly so that the focus is kept on building and developing their business. Table 1 presents the main concept of risk from the selected references.

Concept	Description
NIST 800	A measure of the extent to which an entity is threatened by a potential circumstance or event.
OCTAVE	Possibility of suffering harm or loss. Refers to a situation where a person could do something undesirable or a natural occurrence could cause an undesirable outcome.
FAIR	The probable frequency and probable magnitude of future loss.
COBIT	The combination of the probability of an event and its consequence.
ISSRM	The combination of a threat with one or more vulnerabilities leading to a negative impact harming one or more of the assets.

Table 1 – Risk Concept

The notion of risk constantly includes the chance of negative impact (OCTAVE and ISSRM). While all the risk definitions are one way or another similar, the one presented in NIST seems like the most technical one.

4. RISK MANAGEMENT

Risk management is an artefact that includes a set of coordinated activities performed to direct and control the risk of losing availability, confidentiality, and integrity of organizational information. It includes a set of plans, relationships, accountabilities, resources, processes that provide the policy and objectives to manage risk. The risk management policy addresses the aims and strategy of the organization regarding risk management (ISO, 2009) (Guide, 2009).

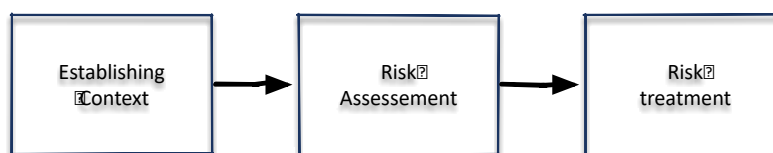


Figure 1 - Risk Management

A risk management framework can be understood as a system whose purpose is to ensure the fulfilment of the goal of risk management. It should also include a risk management process, and the resources and principles used in its implementation, as represented on Figure 1. These features can vary, however, the most important one in practice are grouped into three main stages (Figure 1) which can result in multiple solutions depending on the technical and technological support available to the risk management.

5. CONCLUSION

Risks exist universally and can have costs every day, whether it is recognized by the organization affected by them. One of the main challenges that the organization must address is on the modelling of risk information. Risks modelling involve a highly heterogeneous set of assets, events, methods, stakeholders and responsibilities, requiring adaptable methods and tools to support the exchange and interoperability of risk information, since risk management and risk assessment tend to be done by distinct teams with potential different views on the same risks.

The research describe in this paper is driven by information security in any potential scenario that deals with information. A common way to model and address complex business systems is the use of model. Thus, we intend to bring the concepts and strategies of modelling into this subject. Modelling information risk is a complex task, especially in scenarios where protection of information is not a unique concern of the organization. To cope with information security risks, this there are need to have a cooperation between risk management and information security department, making it possible to align information security concerns with other (potentially related) organizational concerns.

Future work intends to extend risk management and information security models to include the dynamic perspective of information security, and conduct empirical studies for assessing the usability and efficacy of our approach in the risk management and information security domains.

REFERENCES

- Andress, J. (2014). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress.
- CALDER, A. (2013). *ISO27001 / ISO27002* (2nd ed.). IT Governance Publishing. Retrieved from <http://www.jstor.org/stable/j.ctt5hh4qg>
- Cherdantseva, Y., & Hilton, J. (2013). *A Reference Model of Information Assurance & Security*. 2013 International Conference on Availability, Reliability and Security, 546–555. <http://doi.org/10.1109/ARES.2013.72>
- Guide, I. S. O. (2009). 73: 2009. *Risk management—Vocabulary*.
- ISO, I. (2009). 31000: 2009 *Risk management—Principles and guidelines*. International Organization for Standardization, Geneva, Switzerland.
- Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. CRC Press.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102.