Information and Communications Security - Environmental Analysis of a Public Institution: methodological framework for the implementation of security controls applied to information assets

Domingos Savio Evandro da Silva
is a civil servant of the National Civil Aviation Agency (ANAC) as a Regulation Specialist.

Melina Zaban
is a civil servant of the National Civil Aviation Agency (ANAC) as a Civil Aviation Regulation Specialist.

ABSTRACT

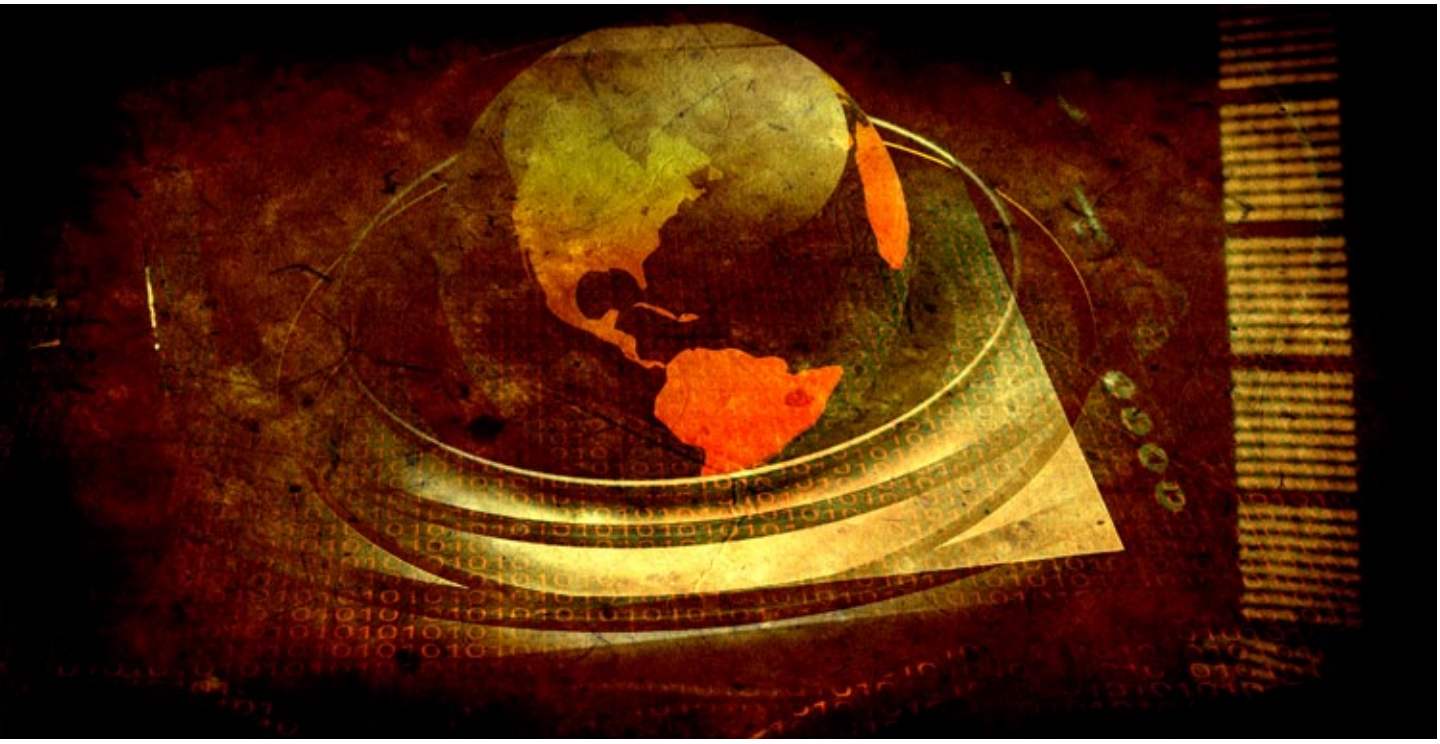
In today's society, where information takes a strategic role in the formulating of organizational policies to obtaining favorable economic results, the efficient use of information resources has been a constant. This article aims to analyze, in a public institution, some information assets that need to be protected against threats as well as checking the current structure of physical security of this institution in which these assets are included, exemplifying some physical risks and associated controls that can be treated by contingency plans.

Keywords: Information Security; Information Management; Risk; Contingency.

1. INTRODUCTION

Information security requires the organization to implement and maintain an adequate structure of physical controls in order to ensure the information assets are protected from threats that may damage or disable them causing possible risk of immensurable loss.

This article aims at analyzing the current structure of the physical and environmental security of a certain public institution and verify, through means of observation, some of the information assets that need



to be secure and protected against possible threats. It also presents some risk examples with a brief analysis of its effects on the institution and of associated physical controls.

2. ORGANIZATIONAL STRUCTURE

The analyzed institution refers to a typical federal public body, which comprises public agents, public servants, outsourced employees and positions of trust.

On its organic structure, in addition to the sectors responsible for the administrative, financial and assets management that are essential for the proper functioning, there are also several units responsible for the general customer services, which represent the primary activities for the compliance with regulatory purposes of that body.

Subsidized financial resources are used for the performance of organizational activities, and a specialized control core must manage them, once the execution of expenses must be previously approved and the results must be measured and monitored, generating information that will be used in the decision making process.

The amount of people walking through the facilities of the institution is great, either for the amount of services delivered to an specific public or for the means of access to the facilities shared with other agencies, which increases the need of keeping a system of information management and information and communication security at adequate levels.

3. ASSOCIATED RISKS

Based on the observation of the information assets that comprise the institution´s assets collection it is possible to list some of the most relevant in order to exemplify the specific threats involved and how to proceed to risks analysis and evaluation level, as presented on table 1.

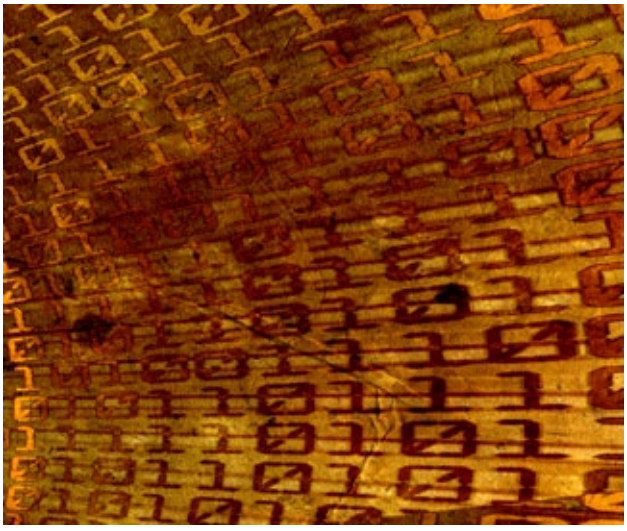


Table 1:
Risks assessment

Id.	Asset	Specific Threat	Vulnerability	Risk - R	Probability	Impact	Risk Level
A1	Archive activities area	Unauthorized access	Absence of an access control system	R1 – Information integrity loss	High	Very Deep	Very High
A2	Official documents recorder computer equipment	Unauthorized copy of sored information by company hired by the institution.	Enables the company to have information access without the proper control.	R2 - Information confidentiality loss.	Very High	Deep	Very High
A3	Document Management System	Server connection interruption.	Absence of redundancy activation routine.	R3 – Information availability loss.	Very Low	Critical	Low
A3	Document Management System	Server does not hold the system access demand.	Server access limitation.	R4 – Information availability loss.	Medium	Low	Low
A3	Document Management System	Document unauthorized visualization.	The system has only two restriction levels for document access, which does not address all circumstances.	R5 – Confidentiality loss.	Very High	Very Deep	Very High
A4	Printer	Unauthorized people obtaining information stored in the printer memory.	Absence of routines of memory cleaning or disposal of the printer information storage device.	R6 – Information confidentiality loss.	Very High	Deep	Very High
A5	Laptops	Theft.	Critical information storage inside the laptop.	R7 – Information confidentiality loss.	Medium	Very Deep	Very High
A6	Desktops	Unauthorized visualization of business critical information.	Operation system accessible in the absence of the user-owner.	R8 – Confidentiality loss.	High	Critical	High
A7	Physical documents	Document unauthorized visualization.	There are no mechanisms of documents access control.	R9 – Confidentiality loss.	Very High	Very Deep	Very High

Source: the authors

Chart 1 shows the risk matrix, in which the probability relation between the occurrence of an event and the level of impact on the information resources or information assets functionality is presented.

The following definitions were applied in this context:

Probability

Very Low: Very unlikely to happen – (0% - 10%);
Low: Unlikely to happen – (10.1% - 30%);
Medium: Occasionally happens – (30.1% - 70%);
High: Likely to happen – (70.1% - 90%);
Very High: Frequently happens – (90.1% - 100%).

Impact

Insignificant: The damages are insignificant for the organization;
Low: The organization is able to fix the damage with its own resources;
Critical: The damage recovery requires resources that were not foreseen by the organization;
Deep: Damage that may harm the body image or generate incidents that may be difficult to fix;
Very Deep: Damage or irreparable loss of the body image or of the resources functionality.

For an information management system, some adequate processes of identification and risks control

Chart 1:
Risk Level

		Probability				
		Very Low	Low	Medium	High	Very High
Impact	Very Deep	High Risk	High Risk	Very High Risk	Very High Risk	Very High Risk
	Deep	Medium Risk	Medium Risk	High Risk	High Risk	Very High Risk
	Critical	Low Risk	Medium Risk	Medium Risk	High Risk	High Risk
	Low	Very Low Risk	Low Risk	Low Risk	Medium Risk	Medium Risk
	Insignificant	Very Low Risk	Very Low Risk	Very Low Risk	Very Low Risk	Very Low Risk

Quadro 2:
Definição de prioridades

		Control Actions Efficacy				
		Strong	Satisfying	Unsatisfying	Weak	Inexistent
Risks Ranking	Very High Risk	High Priority	High Priority	Very High Priority	Very High Priority	Very High Priority
	High Risk	Medium Priority	Medium Priority	High Priority	High Priority	Very High Priority
	Medium Risk	Low Priority	Medium Priority	Medium Priority	High Priority	High Priority
	Low Risk	Very Low Priority	Low Priority	Low Priority	Medium Priority	Medium Priority
	Very Low Risk	Very Low Priority	Very Low Priority	Very Low Priority	Very Low Priority	Very Low Priority

must be established, in which "the risks are identified through an inspection of threats and weaknesses of which these documents are vulnerable to and the resulting impact, in case a threat explore any vulnerability". (PORTELA, T.N.O; SILVA, N.P. 2011).

Therefore, some security actions and controls able to mitigate or eliminate the risk must be implemented, following a priority order.

According to PORTELA et SILVA (2011), the risk treatment must by started by the risk that presents the highest probability of occurring and that may cause an impact relevant to business.

Chart 2 presents a priorities definition scale that assist the implementation of actions, facilitating the efficiency of resources allocation for the organization.

4. ACTIONS PLAN

The selection of information security controls, as described on ISO/IEC 27002 (ABNT, 2005), depends on the decisions of the organization, based on the risk acceptance criteria, on the options of risk treatment and on the risk management general focus applied to the organization. It is also subject to all international and national relevant laws and regulations. (SILVA, E.M. 2011a).

Nevertheless, according to SILVA (2011a), these controls must not be independent, they must be part of the Information and Communication Security Policy – PoSIC in order to comply with the rules of access and provision of supervision and monitoring devices.

4.1 CRISIS MANAGEMENT PLAN - CMP

Organizational plans must be defined in the security policy in order to face possible incidents, as the Crisis Management Plan – CMP, which accurately defines the functionality of the teams before, during and after the occurrence of the incident. It aims at defining the procedures that must be executed until the activities return to their normal course. (SILVA, E.M. 2011).

4.2 DISASTERS RECOVERING PLAN - DRP

All institutions are subject to loss of information assets for the vulnerabilities inherent to business that may be jeopardized by external and internal threats. Therefore, "it is necessary to ensure the continuity of important processes and information of the institution as soon as possible in order to avoid or minimize the impacts of an incident". (OLIVEIRA et SILVA SAVIO, 2011).

In this context, the DRP comprises the recovery and restoration of the functionalities of human, operational and technological assets, in addition to those that support the business. It aims at reestablishing the environment to the original conditions of operation.

Table 2 presents a draft of the actions that will be executed as an integral part of the DRP, considering the risk associated to the information assets, as described on table 1.

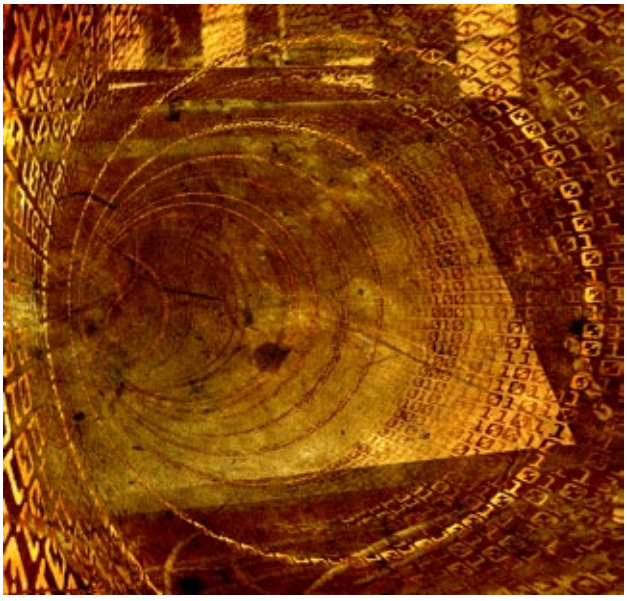


Table 2:
CMP Model

Crisis Management Plan		
Id.	**Asset**	**Actions**
R1	A1	1) Activating the building security team. 2) Verifying if there was damage to the archive, access to confidential information and changes in archived data. 3) Informing about the incident and the service reestablishment forecast to the proper hierarchical level.
R2	A2	1) Consulting the identification record of people that had access to the equipment room. 2) Verifying the logical access records and data integrity. 3) Informing about the incident to the proper hierarchical level, requesting the opening of an investigation.
R3	A3	1) Contacting the information support team. 2) Requesting the activation of the system for replacement processing center. 3) Verifying the service term in the contract of the respective supplier. 4) Informing about the incident and the service reestablishment forecast to the proper hierarchical level.
R4	A3	1) Contacting the information support team. 2) Requesting the temporary permission of a greater number of simultaneous access to the server. 3) Verifying the service term. 4) Informing about the incident and the service reestablishment forecast to the proper hierarchical level.
R5	A3	1) Identifying violated information. 2) Identifying documents related to the information. 3) Verifying records of access to the violated documents. 4) Informing about the incident to the proper hierarchical level, requesting the opening of an investigation.
R6	A4	1) Verifying which printers are being discarded. 2) Suspending the printers discard process. 3) Informing about the incident to the proper hierarchical level, requesting the opening of an investigation.
R7	A5	1) Verifying if the stolen laptop had any systems of information distance blocking or tracking. 2) Verifying the place the theft occurred, activating the building security team, if it took place in the organization´s facilities. 3) Informing about the incident to the proper hierarchical level, requesting the opening of an investigation and a police report.
R8	A6	1) Verifying which critical information was available and accessible. 2) Verifying if there were changes in the integrity and information access permissions. 3) Informing the information support team to perform the adequate security procedures. 4) Informing about the incident to the proper hierarchical level and to the areas involved with the compromise of that information.
R9	A7	1) Identifying violated information. 2) Identifying documents related to the information. 3) Informing about the incident to the proper hierarchical level, requesting the opening of an investigation.

Source: authors

5. ORGANIC SECURITY

Considering the patterns suggested by the ISSO/IEC 27.002/2005M, it is possible to perform an analysis of the variables that compose the requirements set related to the physical controls necessary to an adequate management of the Information and Communication Security applied to the organizational environment.

The creation and implementation of physical access controls were suggested for the control of identified information assets. Thus, the areas classified as sensitive must be protected by appropriate entrance controls in order to ensure that only authorized personnel have access to them, considering:

a. Visitors in security areas must be monitored or led by the security staff and the dates and time of their entrance must be recorded.
b. The access to sensitive information must be controlled and restricted to authorized personnel only. Authentication controls with identification systems, as magnetic cards, must be used to authorize and validate all accesses.
c. All personnel must use any visible identification and must be encouraged to question unaccompanied strangers and anyone without visible identification.
d. The materials received must be inspected regarding possible danger before they are transferred from the storage to the place of use.

The implementation of a training policy was suggested once the cooperation of authorized users is essential for the efficacy of the security, for all must be aware of their responsibilities regarding the main-

Table 3:
Security controls and compatibility with the identified information assets

ISO/IEC Control	Existing or suggested controls	Asset
7.1.2	It is necessary to implement a physical access control in order to consider the controls suggested by ABNT 27002 standards. There is an access control through the ratchet, the building and the receptionist in the reception. There is no restriction of internal crossing, even if the sectors present doors and restrictions on defined office hours.	A1 to A7
7.1.5	The access to the delivery and loading area from an external area must be allowed for identified and authorized personnel only. It is necessary that external doors of a delivery and loading area are protected when the internal doors are open.	All
7.2.4	An equipment preventive maintenance is performed from time to time (laptops, computers and printers). It is necessary to elaborate and implement a capacity management process. The resources and systems monitoring is performed in an informal manner, not periodically.	A2 to A6
7.2.6	It is necessary to elaborate standards for the Organic Security (Physical and Environmental) considering section 9.2.6 – Reuse and safe alienation of the equipment (ABNT 27002) in order to ensure all sensitive data and licensed software have been removed or safely overwritten.	A2 to A6
7.3.1	It is necessary to create a training policy for the sensitization and awareness of matters related to the Information and Communication Security and attention it must be giver by the users.	All

Source: the authors, adapted from the ISO/IEC 27002/2005

tenance of effective access controls, especially the use of passwords and equipment security.

6. CONCLUSION

Based on the observation of the information assets that compose the institution´s assets collection, the relevance of the use of standards and methodologies for the implementation of a security structure that considers the information assets inventory and the associated risks analysis, among other aspects, was verified.

After the verification of the compliance of the assets with the existing physical controls, the prioritization of security actions was performed according to the evaluated risk level, which assists on the management of resources that must be allocated in these actions.

A model of the Crisis Management Plan - CMP was presented with those procedures, detailing the actions that must be followed if an incident occurs, including the functioning of the teams before, during and after the event.

With this instrument, it is possible to elaborate the Disasters Recovery Plan –DRP in order to comprise the recovery and restoration of the functionalities of the assets previously mentioned, once the plan aims at reestablishing the environment to its original operation conditions.

Finally, it was verified that the physical security controls that will be improved must consider the features established in the ISSO/IEC 27.002/2005, aiming at providing a reasonable guarantee that the environment will be protected against existing threats, which will facilitate the studied institution to have a better management of information resources.