Checking the Maturity of Security Policies for Information and Communication

Mauricio Rocha Lyra, Ph.D., COBIT Foundation, CTFL, ISO 20000, ITIL, MCSO, OCUP, PMP, RUP, is a leading professor at Centro Universitário de Brasília and has more than 25 years of experience in the computer science field. He is the author of *Segurança e Auditoria em Sistemas de Informação (Informational Systems Security and Auditing).*

Jose Carlos Ferrer Simoes has more than 10 years of experience working in the Bank of Brasil in the field of information security.

The transformations experienced by organizations due to technological advances has made information, arguably, an enterprise's most valuable asset. As a result, this highly sensitive and vulnerable asset must be protected from potential threats. Organizations are increasingly experiencing risk susceptibility and financial losses due to their information systems and computer networks.

As an example of how to check the level of maturity of security policies for information and communication, this article analyzes the case of a Brazilian government agency. While a Latin American example, this analysis can be applied to any government agency or private entity at the national or international level.

With the importance of information processed in federal public administration departments and entities in mind, the president of Brazil issued Decree, no. 3505, on 13 June 2000,[1] establishing Brazil's National Information Security Policy. The decree mandates that all departments and entities of the federal government have a security policy for information and communication (SPIC). This decree presented the need for protecting information considered sensitive and for general guidelines that should be adopted to prevent and treat vulnerabilities, threats and risk factors that deserve special treatment by all departments and agencies of Brazil's Federal Public Administration.

For this decree to be effective, the federal government has focused its efforts on implementing information security measures in the Federal Public Administration. The implementation consists of applying best practices such as ISO/IEC 27002: 2013,[2] federal legislation such as Decree no. 3505 and the Federal Public Administration's Information Security Policy and Regulatory Instruction no. 01,[3] established by the presidency's Institutional Security Office.

Decree no. 3505's publication established and ruled that all areas of the federal government should establish an SPIC. This Decree is aimed at ensuring the SPIC maturity level in all Federal Public Administration entities.

To achieve this goal, the best practices for creating an SPIC were mapped for organizations using the ISO/IEC 27000 family of international standards. Next, 10 federal government departments in various areas were identified in order to complete a comparative analysis of these best practices. Finally, a critical and comparative analysis, introducing an SPIC maturity-level matrix within those chosen organizations was performed, as well as an analysis of SPIC regarding each area of expertise.

ANALYSIS OF SPIC

The objective of the SPIC comparative analysis was to compare 12 standard requirements for their usefulness for an SPIC. The analyses were to be performed according to ISO 27002:2013, among the 40 federal government entities (the presidency and 39 ministries) of Brazil. **Figure 1** presents the requirements met by each department studied.

ATTRIBUTES REQUIREMENT ANALYSIS

To better understand the aspects dealt with in an SPIC, the 12 essential requirements were classified, according to the best practices in three major groups by their similar attributes, which were designated as regulation, prevention/control and responsibility/penalty. Among the 12 requirements, four requirements were identified with attributes of regulation, five attributes with requirements of prevention/control and three requirements with attributes of responsibility/penalty, as shown in **figure 2**.

In **figure 2**, the percentage of the requirements are also presented and mapped to the creation

Figure 1—Consolidated SPIC Requirements Analyzed

	Requirements for SPIC According to ISO 27002:2013	SPIC—Ministry of Defense	SPIC—Ministry of Justice	SPIC—Ministry of Health	SPIC—Ministry of Science, Technology and Innovation	SPIC—Ministry of Planning, Budget and Management	SPIC—Ministry of Culture	SPIC—Ministry of Tourism	SPIC—Ministry of Labor and Employment	SPIC—Ministry of Education	SPIC—Ministry of Agriculture, Livestock and Supply
1.	Does it contain regulations, laws and contracts that must be SPIC-supported?	Yes	No	No	Yes	Yes	No	Yes	No	Yes	No
2.	Does it contain a framework for setting control objectives and controls, structure analysis, evaluation and control management, and assessment and risk management?	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No
3.	Do scope, concepts, definitions and a description of information security importance exist?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.	Are principles of information security and communications policy declared?	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No
5.	Are there objectives and principles to guide all activities related to information security?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6.	Is there attribution of responsibilities, general and specific to information security management, for defined roles?	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	Yes
7.	Is there a provision for the management process of business continuity (business continuity management)?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
8.	In case of violation of the SPIC, are the consequences (penalties) stated in this document?	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
9.	Are there specific policies that require the implementation of security controls and that are structured to consider the needs of certain interest groups within the organization or to cover specific topics (e.g., access control, classification, processing of information)?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
10.	Are the policies of information and communication security communicated to employees and relevant external parties so that they are understood, relevant and accessible to users (i.e., in the context of a program of awareness, education and training in information security)?	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	Yes
11.	Are the security policies of information and communication critically analyzed at planned intervals?	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No
12.	Is there a statement of commitment directly supporting the goals and principles of the organization?	No	No	No	No	No	No	Yes	No	No	No

Source: Jose Carlos Ferrer Simoes and Mauricio Rocha Lyra. Reprinted with permission.

of an SPIC per ISO 27002:2013, as observed by the Federal Public Administration, among the departments that were analyzed. Further, the average percentage of the requirements was verified for each attribute properly classified, and for this percentage, the arithmetic mean was used for the requirements classified into each of the attributes.

Figure 2 makes it clear that there were attributes with greater or lesser levels of maturity. However, although none of

Figure 2—Attributes Requirements Analysis

Attributes of the Requirements	Requirements Checked by Attribute	Percent of Requirements Attended by the Department Analyzed	Average Percent of the Requirements Checked by Attribute
Regulation	1. Does it contain regulations, laws and contracts that must be SPIC-supported?	50%	77.5%
	3. Do scope, concepts, definitions and a description of information security importance exist?	100%	
	4. Are principles of information security and communications policy declared?	60%	
	5. Are there objectives and principles to guide all activities related to information security?	100%	
Prevention and/or Control	2. Does it contain a framework for setting control objectives and controls, structure analysis, evaluation and control management, and assessment and risk management?	60%	82.0%
	7. Is there a provision for the management process of business continuity in an SPIC (business continuity management)?	100%	
	9. Are there specific policies that require the implementation of security controls and that are structured to consider the needs of certain interest groups within the organization or to cover specific topics (i.e., access control, classification, processing of information?)	100%	
	10. Are the policies of information and communication security communicated to employees and relevant external parties so that they are understood, relevant and accessible to users (i.e., in the context of a program of awareness, education and training in information security)?	70%	
	11. Are the security policies of information and communication critically analyzed at planned intervals?	80%	
Responsibility and Penalty	6. Is there attribution of responsibilities, general and specific to information security management, for defined roles?	70%	56.7%
	8. In case of violation of the SPIC, are the consequences (penalties) stated in this document?	90%	
	12. Is there a statement of commitment directly supporting the goals and principles of the organization?	10%	

Source: Jose Carlos Ferrer Simoes and Mauricio Rocha Lyra. Reprinted with permission.

the three attributes had full classified prediction, it should be emphasized that the prevention and/or control attribute has a greater predictability in an SPIC, and of the five requirements that comprised this attribute, two requirements (numbers 7 and 9) were provided in all SPICs analyzed. Requirement number 11, despite being absent in two SPICs, was performed in all 10 departments that had recently updated their policies. In practice, the requirement has been observed; however, there is no formal prediction to support best practices. Thus, it is necessary that requirements 2 and 10 should be revalued so that those attributes are handled as soon as best practices are established.

The control attribute, which had the second best predictor in the SPICs, is composed of four requirements, and two of these requirements (3 and 5) are fully provided in all SPICs analyzed in this work. Requirements 4 and 5 are provided in only five and six departments, respectively, which shows the need for the Federal Public Administration to act in partnership so that there is greater interaction when drafting or reviewing a department's SPIC. These two requirements are simple requirements and are generally already included in an SPIC because the entities already directly or indirectly respect the precepts of information security and legislation in which these requirements are supported.

The responsibility/penalty attribute was identified with less predictability in the SPICs—possibly because it is an area that involves issues related to IT and is often an area of little knowledge by managers. This is verified by the point that only one of the 10 departments analyzed shows the requirement of "12" that had the lowest prediction in SPIC analyzed. For greater support of activities and responsibilities related to information security, and to improve the IT governance of public entities, the use of organizational structures is suggested (i.e., the creation of a committee connected directly to top management [strategic IT committee] to support the IT strategy development, in addition to monitoring the achievement of strategic IT goals, using, among other instruments, periodic reports on actions related to IT, generated to give greater technical protection to the top management who will be able to act with higher effectiveness). Thus, top management is engaged in guided predictability of the 12 SPIC requirements while also managing the periodic update of this policy.

SPIC MATURITY-LEVEL MATRIX

In **figure 3**, the amount and the percentage of checked requirements in an SPIC, per ISO 27002:2013, are presented for each department analyzed in this work.

Figure 3—Amount of Requirements Met in the Analyzed Departments

Ministry	Number of Checked Requirements	Percent of Conditions Verified in Departments
Tourism	12	100%
Science, Technology and Innovation	11	91.67%
Planning, Budget and Management	11	91.67%
Defense	11	91.67%
Justice	9	75%
Culture	8	66.67%
Labor and Employment	7	58.33%
Education	7	58.33%
Agriculture, Livestock and Supply	7	58.33%
Health	6	50%

Source: Jose Carlos Ferrer Simoes and Mauricio Rocha Lyra. Reprinted with permission.

Figure 3 verifies the amount of attributes checked in the ministries. Then, by performing calculations, the arithmetic mean (8.90) of SPIC conditions is verified and the standard deviation (2.07) of these requirements can be observed. Hence, a maturity matrix of the analyzed departments was applied, as shown in **figure 4**, where the ranges of the quantity of verified SPIC conditions are presented and their respective maturity is analyzed.

Figure 4—SPIC Maturity Matrix

Average Number of Requirements Verified in SPIC	Degree of Maturity	Number of Analyzed Departments Attending This Range of Requirements
Above 10.97	High	4
Between 8.9 and 10.97	Good	2
Between 6.83 and 8.90	Reasonable	3
Less than 6.83	Undesirable	1

Source: Jose Carlos Ferrer Simoes and Mauricio Rocha Lyra. Reprinted with permission.

STRATEGIC, FUNDAMENTAL AND SPECIAL AREA

For better analysis, the 10 departments observed in this study were classified into three groups (strategic, fundamental and special) and by area of expertise (**figure 5**).

Figure 5—Amount of Requirements Attended Per Area of Operation

Area	Ministry	Number of Checked Requirements in Each Department
Strategic	Planning, Budget and Management	11
	Science, Technology and Innovation	11
	Defense	11
	Justice	9
Fundamental	Health	6
	Education	7
	Labor and Employment	7
	Agriculture, Livestock and Supply	7
Special	Tourism	12
	Culture	8

Source: Jose Carlos Ferrer Simoes and Mauricio Rocha Lyra. Reprinted with permission.

The areas that determine the guidelines and planning of the state were classified as strategic. Departments engaged in services essential to survival and social well-being were classified as fundamental. The areas not related to strategic and key themes were classified as special.

The four ministries classified in this work as strategic showed an SPIC with a level of maturity above average in comparison with other analyzed departments. This study indicates that the departments classified as strategic use a standard based on best practices for building and updating their SPICs. Finally, it can be said that strategic areas' SPICs have a good homogeneity and are consistent with their degree of expertise, presenting documents with nearly all essential requirements for compliance with the policy.

The four departments classified as fundamental areas showed a degree of maturity, as shown in **figure 5**, ranging from reasonable to undesirable. This homogeneity and lower SPIC maturity level are probably due to a lack of benchmarking. Apparently, these departments developed their SPIC without much critical analysis of their current affairs, but instead by simply using a previous SPIC model, generating policies with the absence of several essential requirements of information security. As for the departments that had their SPIC classified as special, a heterogeneity was observed in their SPIC, ranging from reasonable to high maturity.

FINAL REPORT ANALYSIS

In the study, it is inferred through the analysis of several decrees and laws that the federal government is directing its efforts to implement information security standards to be followed by departments in order to consistently conduct business with best practices and in compliance with specific legislation. However, based on data collected from the government areas studied, one can verify that an SPIC is applied in direct Federal Public Administration departments at a very diverse level of maturity.

> "A well-implemented SPIC can mitigate or even determine responsibility for undesired actions in an organization."

Regarding the compliance with essential requirements in an SPIC, it was found that only one of the departments studied met all 12 requirements, which shows a deficiency and a risk to public administration in general, especially because a well-implemented SPIC can mitigate or even determine responsibility for undesired actions in an organization.

Another aspect addressed in this study was the analysis of the essential requirements in an SPIC based on attributes in which it was identified that the departments analyzed had greater predictability when the attribute related to prevention and/or control. This fact is due to the culture of the Federal Public Administration, which is directly supervised by control entities of the federal government.

When the analysis from the perspective of the Federal Public Administration expertise area was conducted, it was found that the departments classified as strategic, as well as the ones classified as critical, showed a similarity to the requirements in their SPIC for area performance, which can be interpreted as these entities making an effort to meet best practices with respect to information security, although there is no study or a more critical analysis of this tendency addressed in their policies' requirements.

For an SPIC in the Federal Public Administration to reach a high level of maturity, it is necessary to create a temporary, multidisciplinary safety committee, which should have a central management with the responsibility of analyzing, evaluating, criticizing and reviewing SPICs before these policies are published. It is worth noting that the decision to accept this committee's recommendations would be the responsibility of each department's management. However, surely the department, while receiving feedback from a specialist in the subject area, would be inclined to at least predict, even in a partial way, those recommendations in its SPIC.

Finally, although this work has been conducted in 10 departments, it is not possible to assess or infer the maturity level of the 30 departments that were not analyzed. Another fact that needs to be emphasized is that this study considered only the quantitative value of the requirements, which do not evaluate the merits of qualitative requirements. Based on these facts, it is understood that for an accurate assessment of how the SPIC is applied in public administration, a larger study addressing not only every department, but a detailed analysis of the qualitative value of these essential requirements is necessary.

This study aimed to verify the applicability of the SPIC in organizations and to analyze the maturity of this document on the best information security practices. To facilitate the analysis,

the study was made based on the SPIC of Brazilian public organizations. However, this methodology can be used in any company in the public or private sectors. This study can be extended beyond merely analyzing the predictability in SPIC—to also evaluating the merits of these attributes.

ENDNOTES

[1] Decree, no. 3505, 13 June 2000 established the Information Security Policy in the organizations and entities of the Brazilian Federal Public Administration.

[2] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 27002:2013, *Information technology—Security techniques—Code of practice for information security management*, 2013

[3] Federal Public Administration's Information Security Policy and Regulatory Instruction no. 01. This document presents directives for the preparation of an SPIC in organizations and entities of the Brazilian Federal Public Administration.