Maintaining Information Security in the New Technological Scenario

Leandro José Aguilar Andrijic Malandrin
University of São Paulo – Polytechnic School (POLI/USP)
São Paulo, Brazil
leandro.malandrin@usp.br

Tereza Cristina Melo de Brito Carvalho
University of São Paulo – Polytechnic School (POLI/USP)
São Paulo, Brazil
terezacarvalho@usp.br

Abstract

The technological scenario always played a critical role in Information Security. However, in recent years, this scenario has changed substantially, in ways not known so far. Characterized by different technological trends, like IT infrastructure outsourcing, cloud computing and mobility, this scenario created several new security challenges. The usual approach to deal with change in Information Security Management Systems (ISMS) is to execute a risk assessment review and to deploy new security controls. However, because of the disruptive nature of the technological scenario, that is not enough – new ways to plan the ISMS itself seem to be required. In this paper, these needed changed are identified and detailed, using ISO/IEC 27001 as a key reference. Based on risks mapped in the literature for key technological trends, checkpoints were created and inserted into the basic processes for important ISMS planning activities. The result is a support framework designed specifically for Security Policy definition and Risk Management. By modifying the usual process for each activity, the framework drives the creation of a security culture based on the awareness of the external scenario new risks. Applicability tests executed in a medium-sized organization showed that the framework can be easily plugged into real world situations. The main contribution of this research is the definition of new tool to help security practitioners better cope with the security challenges created by a disruptive technological scenario.

Keywords: Information Security Management Systems, ISO/IEC 27001, IT infrastructure outsourcing, Cloud Computing, Mobility, Security Policy, Risk Management

Introduction

Many companies consider the information at its disposal one of its most precious assets. Unfortunately the reality does not match the speech. Despite the relevance given to information nowadays, information security flaws keep happening. Besides that, they seem to become ever more frequent and complex, going from record leaks originated by shared passwords to the interruption of industrial plants due to vulnerabilities in logical programmer controllers.

The truth is that companies continue to deal with "information" in a very different way than when they deal with "information security". In one hand, the idea of "information" encompasses, for example, what is discussed in meeting rooms, printed documents, corridor talks and e-mail exchanges. In the other hand, the idea of "information security" is more restrict, constantly leading back to ideas of virus, system crackers, spam and hackers, what makes it constantly seen as a competence of Information Technology (IT) teams (Corriss, 2010).

The Information Security Management System (ISMS) introduced by International Standards Organization (ISO) on its ISO/IEC 27001 standard represents one attempt to close the gap between these two concepts. It adopts an approach of four phases – Plan, Do, Check and Act – focused on process changes by the introduction of new security practices. This approach is represented by Figure 1. This system uses the execution of risk analysis as a base, where new risk situations are identified and adequate actions are taken for their mitigation. Due to the lack of specific security knowledge these tasks are usually complicated for most companies.

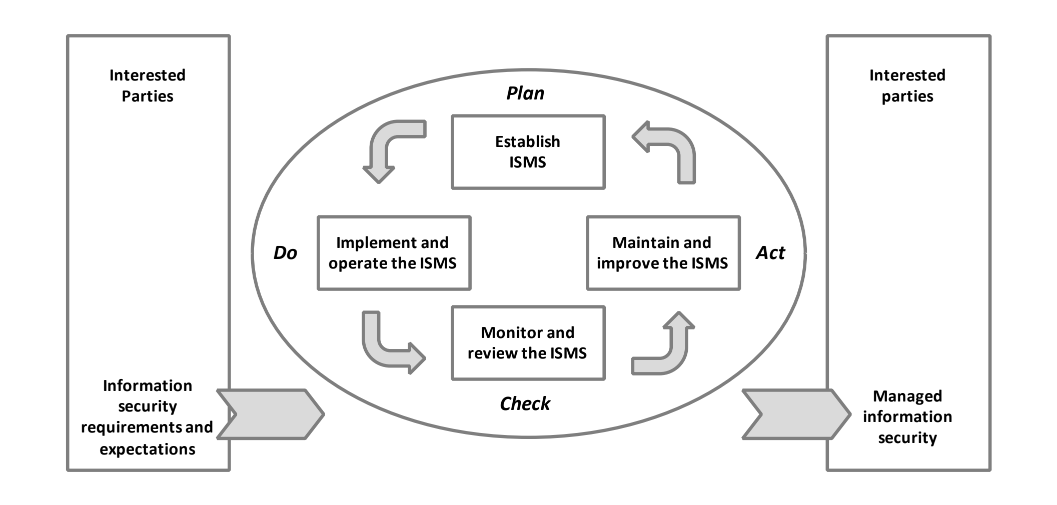
Interested Parties
Plan
Establish ISMS
Do
Implement and operate the ISMS
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check
Interested parties
Information security requirements and expectations
Managed information security

Figure 1- The ISO/IEC 27001 approach for ISMS creation (ISO/IEC 27001, 2005)**.**

Adding to these difficulties, companies face an even harder problem. The current external scenario brings to the context a series of new technological and paradigms changes. Among them can be highlighted: high dependency of IT infrastructure outsourcing services, cloud computing and strong need for mobility. Derived from these basic factors, new work paradigms appear, like the constant use of social media, personal and corporate environment convergence and finally the *consumerization* of IT. It is a highly disruptive scenario, where new ways of working are being established and new concepts introduced on companies day to day operations, unlike anything ever saw to date.

Usually, the ISMS process for considering changes like the ones mentioned in the external scenario is the risk assessment review. This happens during the beginning of the ISO/IEC 27001 cycle: the Plan phase. This process results in the identification of new risks and the deployment of new security controls in the Do phase. This approach premises that the Security Policies and Risk Management methodology used during the Plan phase allow new risks to be identified. Unfortunately, in this new external scenario, there are just too many variables to consider and security becomes, more than ever, a moving target. Proper protection nowadays depends of more and more people with a grasp on basic security concepts. This is not easily achieved if only the mentioned approach is considered, since most of these security concepts seem to be very abstract to most people.

Therefore, it is plausible to think that something must be adapted in this typical ISMS approach. The development of new tools is needed. These tools must help companies during the creation of a new type of security culture, which focus not only on technology, but on closing the gap between "security" and "information security". This can be only be done by changing the way people think about security and how process manipulate information.

In this research it is proposed a change to the typical ISMS approach above mentioned, by considering the new technological scenario not only during the risk analysis review, but in the entire security planning. This is done by the introduction of a support framework focused on the ISO/IEC 27001 Plan phase. The proposed framework provides checkpoints for the two key activities that take place in this phase – Security Policy definition and Risk Management.

In order to evaluate the proposed framework in a real world situation, one company was selected for an applicability study. The selected company, INTEGRA (fictional name) is a very successful company in the Brazilian ITC systems integration market. INTEGRA is also successful in adapting its practices, by means of solid and mature management practices. INTEGRA bases its ISMS on ISO/IEC 27001. These characteristics make INTEGRA a very adequate candidate for the evaluation of the proposed framework.

Method

The work was executed based on a three step research method. The first was of Research and Information Structuring, the second of Construction of the support framework and the third of Evaluation based on an applicability study.

This method was selected because the nature of the proposed framework creation required the combination of research from many different topics in information security. These topics ranged from the technical aspects of new technological trends to aspects of ISMS creation. The split between the first and second steps, for example, proved to be adequate for obtaining a needed initial view of the relations that could exist between all of these topics. These relations were later translated into important concepts incorporated into the proposed framework.

The Research and Information Structuring step included the understanding of the ISMS creation process and the issues which arise during this activity. Special focus was given for the Plan phase of the PDCA cycle. After that, a referenced research for the characterization and understanding of the technological scenario resulted in a list of typical risks seem by market institutions regarding IT outsourcing, cloud computing and mobility. Most of the references used in this phase came from market institutions or market-oriented organizations. This was done due an understanding that the resulting framework had to be easily understood and used by information security practitioners. In fact, this proven to be correct, since many risks identified for specific technological trends did not seem to be covered by academy research on the same trend.

The Construction step identified, among the risks of the external scenario, the most common security problems. The previous research on Policy Creation and Risk Management methods was used to analyze the impacts of these security problems to the basic process of each of these two activities. Based on the relationships found a set of checkpoints was created and inserted into the basic process, originating the support framework.

The Evaluation step identified a company suited for tests with the proposed framework. The company's ISMS was studied and compared with the results from research. Finally the framework was applied to the Plan phase of the ISMS and the results analyzed.

Literature Review

Currently there is a large body of researchers working on Information Security; however this research is split unequally between different specific fields. It can be said that there are four major fields of research on information security (Siponen & Oinas-Kukkonen, 2007):

- Access to Information Systems;
- Secure Communication;
- Development of Secure Information Systems;
- Security Management.

Research showed that the vast majority of publications are directed at technological fields, namely the first three on the list. This research draws from the fields of Security Management and Development of Secure Information Systems, as shown below.

Security Management

One of the common mistakes on Information Security initiatives is not realizing the relevance of international standards (Solms & Solms, 2004). Because of that, many studies focus on how standards can be applied to different types of organizations, either by correlation of different ones (Tsohou, et al., 2010) or by general application models (Milicevic & Goeken, 2011). Related to this, authors provide models to help the deployment of ISO/IEC 27001 (Gillies, 2011), (Anderson & Rachamadugu, 2006). This research uses the concept of creating support models for this kind of initiative, but applies it to the planning phase of ISO/IEC 27001, with a whole new set of constraints, derived from the external scenario.

Other point of interest is how these initiatives try to change security culture. Doing it requires strong executive support, that must set the examples for the rest of the employees (Knapp, et al., 2006). Besides that, security awareness programs must be defined (Corriss, 2010). Finally, in this process organizations must be capable of preparing employees to the new technological scenario, due to the profound changes taking place (Lacey, 2010).

Development of Secure Information Systems

On this topic, this research focuses on the understanding of three key technological trends that define the external scenario. Related to the first, IT infrastructure outsourcing, a decision support framework based on security risks can help define whether or not to outsource some system (Khidzir, et al., 2010), while security models can also help monitor external providers (Jakoubi, et al., 2010). The second, cloud computing, drives the creation of different security risk analysis models (Zhang, et al., 2010), (Müller, et al., 2011). For the third, mobility, research seems to focus on the presence of well-known risks on the new mobile platforms (Leavitt, 2011), (Goode, 2010).

External Scenario Security Risks

The ISO standard states that the main sources of information security requisites are the organizational principles and culture, applicable legislation, and mainly, the risk analysis (ISO/IEC 27001, 2005).

The first two present little variation during the organization life cycle. However, the last, risk analysis, always represented a challenge to organizations, since the external scenario is always changing. New technologies and behaviors represent new sources for attack vectors, to which countermeasures must be found.

To characterize the external technological scenario security-wise, three key technological trends, were identified: IT infrastructure outsourcing, cloud computing and mobility. In fact, recently these have been identified as main trends by IT market analysts. (Gartner, 2011).

Each trend is first briefly presented in the following sections. After, a combined analysis of the security aspects of each of them is shown. The results of this analysis are the basis for the construction of the proposed support framework.

IT infrastructure outsourcing

IT outsourcing is a very common idea nowadays. As companies are pressed to be more efficient, they tend to transfer some activities to third parties, reducing the need for new resources or internal knowledge. This movement has gone beyond simple processes, reaching the infrastructure to support these activities. Companies with IT infrastructure based on services are those who outsource the acquisition and maintenance of IT infrastructure on which depend its business processes. This model has been spreading quickly in the corporate world (Khidzir, et al., 2010). It is said that a good portion of future organizations will have no ownership over infrastructure in the next years, depending exclusively on this type of services.

However, this type of changes leads to different security issues, a topic which has received little attention in recent research (Doomum, 2008). Based on the identified risks for IT infrastructure outsourcing, a few recurrent themes become evident. One of them is the fear of poor integration between internal team processes and external provider processes. Another risk is the uncertainty about the provider capability of providing services which respect external laws and legislations and internal policies. Finally, it is common that companies worry about the availability of the provider services.

Cloud Computing

Cloud computing is an extension of the IT infrastructure outsourcing model described earlier. The basic NIST definition describes it as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (Mell & Grance, 2011).

To offer services with the characteristics of the NIST definition, cloud service providers make intense use of virtualization technology. This technology allows a high degree of flexibility and resource sharing, allowing the provisioning of services to many different clients. These resources can vary a lot, and are usually split into Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Depending on the client needs, the service provider can combine these resources to offer a customized solution.

However, this level of sharing and automation brings a relevant reduction on the level of control that a customer has over the infrastructure it uses. Besides that, the intense use of new technologies brings a series of new risks, due the potential vulnerabilities that might have not been found yet.

Observing the risks for cloud computing mapped in this research, one can note a series of recurrent issues, similar to the ones found in IT infrastructure outsourcing mapping. Besides that, new risks are also found, related to the new technologies used in cloud environments. On this second group, we can list uncertainty regarding the use of new technologies (like virtualization hypervisors) and lack of control over data in the third party infrastructure.

Mobility

The need for mobility is probably the clearest trend in the current technological environment. The vast amount of mobile devices available, including smartphones and tablets, is here to answer to this demand. Until some time ago, these devices presented limited resources and functionalities. Nowadays they are comparable to and many times overcome desktops and notebooks. When combined to services available in, for example, cloud services, they enable a paradigm shift on the typical work of most companies. If before work was confined to specific locations, like in an office and house, now it can be executed from several different places.

The search for innovation in the mobile environment made many vendors focus on shipping devices with more and more functionalities, but forgetting about security (Leavitt, 2011). Despite the fact that these devices are very close to desktops and notebooks, they fail to present the same security features available to those systems. Therefore, there is a great concern regarding the uncontrolled use of them. Because of that, the large part of the risks mapped for this technology is still mirroring the risks identified in the past to other platforms. For example, it is common to find risks related to viruses and unauthorized data access through wireless networks. Adding to this problem, it must be pointed out another related trend, which is employees using their own devices on work environment. This is known as BYOD ("Bring your own device") and it's becoming one major force in organizations. Therefore, besides the typical technological risks mentioned, it is also necessary to address risks related to weak segregation between personal and professional information contained in these mobile devices.

Combined Analysis

Each of the risks identified for the technological trends was classified on its relation to Technology, Processes and People with the purpose of easing the understanding of the risk itself and making visible how broadly security is taken when each trend is considered.

A quantitative combined analysis of the risks and their classifications sums up to what is shown in Table 1. It is interesting to notice how low the number of risks mapped to people is, despite the trend it is related to. Even though People play a key role when dealing with security, organizations seem to avoid mapping risks to them. However, in the external scenario characterized by IT outsourcing, cloud computing and mobility, people play an even more critical security role, because of the need to adapt quickly, identifying and avoiding new threats as they appear.

Table 1- Results from compilation of risks identified for each trend.

	Related to Technology	Related to Processes	Related to People	Total
IT infrastructure outsourcing	2	19	1	**22**
Cloud Computing	29	31	4	**64**
Mobility	13	3	1	**17**
Total	**44**	**53**	**6**	**103**

A qualitative analysis shows that it is possible to identify common security issues among those risks, which are presented in Table 2. They represent situations companies will likely face when dealing with the new scenario, after repeated risk analysis reviews.

Table 2- List of identified security issues and corresponding number of mapped risks

Issue	Description	Mapped risks
[1]	Low trust in the external party to execute the agreed services	8
[2]	Low trust in the external party to execute specific services	3
[3]	Insufficient knowledge about vulnerabilities in new technologies	19
[4]	Uncertainty regarding the integration of services into pre-existing processes	18
[5]	Difficulty to choose the best service and service provider for the company	6
[6]	Likely non-compliance to best practices, policies and regulations	21
[7]	Difficulty of integration of the company infrastructure with new technology	5
[8]	Difficulty of adequate control of data outside the company boundaries	16
[9]	Inexistence of adequate security controls for third party infrastructure	7

In this research, these security issues provide the basis for the definition of changes that must be introduced in the proposed support framework for the Plan phase of ISO/IEC 27001. Considering these 9 broader issues as a reference in the Plan phase instead of the 103 specific security risks has a very important positive effect, which is preparing the ISMS for similar, but yet unknown issues that may arise in the future.

Proposed Support Framework

The proposed support framework for the ISO/IEC 27001 Plan phase was constructed to be used during the execution of the main activities from this phase, which are the Security Policy definition and the Risk Management. Therefore, the framework is composed of two separate frameworks actually, one for each activity.

The construction of the individual frameworks took place in two steps: the identification of the basic processes for each activity and the modification of these, by the introduction of specific checkpoints related to the security issues identified earlier.

Step 1 – Identification of basic processes

In order to modify the activities from the Plan phase of ISO/IEC 27001, it is important to understand the process that must be followed for each of the activity. In this research, this was accomplished by the identification of basic processes in ISO standards and literature when needed.

Security Policy definition is a very common activity on most organizations. However, on ISO/IEC 27000 standards there seems to be no well-known and commonly accepted basic process for the execution of this activity. Most of the references found in the standards refer to the contents that should be inserted in the Security Policy instead of the steps required to define one (ISO/IEC TR 13335-3, 1998), (ISO/IEC 27002, 2005). Fortunately, other references can be found in the literature (Bacik, 2008), which help establish some sort of order. Based on the combination of these references, a basic process can be defined for the Security Policy definition activity (Figure 2a).

Differently, the Risk Management literature provides many references on models and processes to execute this activity (Khanmohammadi, 2010), (Ma, 2010), (Khidzir, et al., 2010), (Gerber & von Solms, 2005). However, ISO itself proposes one reference process for risk management on its risk management standard (ISO/IEC 27005, 2011). Therefore, for the purposes of this research, this is considered as the basic process for the activity (Figure 2b). This way people already used to the standard can easily follow the models.

Step 2 – Definition of Checkpoints

Once each basic process was identified and understood, it was necessary to provide a way to insert relevant modifications to the basic activities. This was accomplished by the definition of checkpoints.

The checkpoints introduced in the basic processes seek to make the security issues identified and listed in Table 2 explicit earlier in the ISMS cycle. This way, these checkpoints create a direct link between the ISMS Plan activities and the risks identified to the key technological trends characterizing the external scenario. The checkpoints themselves are derived from best practices and insights from the literature focused on the security risks of the technological scenario.

All of these checkpoints are presented and matched to the issues they are addressing in Table 3 and Table 4. Following each table it is provided a brief description of the checkpoint.

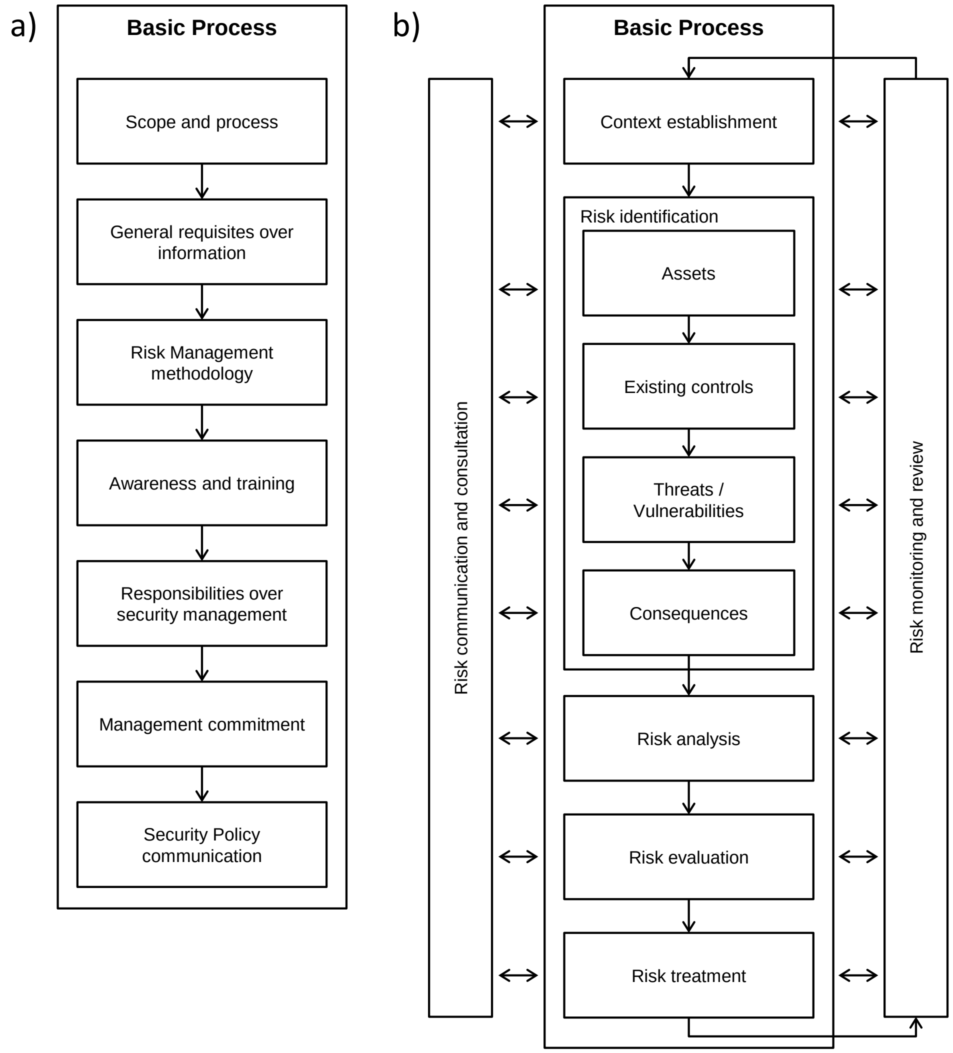
a)
Basic Process
Scope and process
General requisites over information
Risk Management methodology
Awareness and training
Responsibilities over security management
Management commitment
Security Policy communication
b)
Basic Process
Risk communication and consultation
Context establishment
Risk identification
Assets
Existing controls
Threats / Vulnerabilities
Consequences
Risk analysis
Risk evaluation
Risk treatment
Risk monitoring and review

Figure 2- Basic processes identified for a) Security Policy Creation and b) Information Security Risk Management.

Table 3- Security Policy definition support framework - Match between identified security issues and proposed checkpoints.

Security issues Checkpoints	Issue [1]	Issue [2]	Issue [3]	Issue [4]	Issue [5]	Issue [6]	Issue [7]	Issue [8]	Issue [9]
Scope and objectives									
Create scope focused on information			X					X	
Insert security in day-to-day activities	X	X		X	X	X			
Promote obedience to controls	X	X				X			X
General requisites over information									
Abstract information media			X				X	X	X
Risk management methodology									
(Specific Risk Management framework)	X	X	X	X	X	X	X	X	X
Awareness and training									
Promote awareness as a result			X	X	X	X	X	X	X
Customize awareness program				X		X			X
Responsibilities over security management									
Distribute security responsibilities	X	X		X		X			X
Management commitment and Security Policy communication									
Communicate by example						X	X	X	X
Create Security Policy hierarchy			X				X	X	X

Checkpoints Description:

- **Create scope focused on information** – The ISMS scope should be specified in terms of information, not teams or areas, creating the culture of protecting it anywhere – even when in external infrastructure.

- **Insert security in day-to-day activities** – Security must be truly inserted into the company culture. This is not achieved when security is seemed as one “additional” concern and not as intrinsic on every activity.

- **Promote obedience to controls** – Employees and third-party must know that security controls are there for a reason and should be executed, even if they seem too intrusive or as promoting inefficiencies.

- **Abstract information media** – When information can be stored or transported in so many unknown media formats (i.e. cloud) it is hard to keep track of it. Security Policy must focus on information itself.

- **Promote awareness as a result –** Security awareness should not be a synonym to security training. Training is just one of the methods that should be used to achieve the final goal that is awareness.

- **Customize awareness program** – Developing security culture is not viable without practical examples. Different awareness methods are needed, but each must also be tailored to apply to day to day activities.
- **Distribute security responsibilities** – Dealing with the lack of control in the new scenario is hard. Companies must make every individual responsible for sensitive information at all times.
- **Communicate by example** – As in most management situations, acting as expected is the best possible way to achieve peer and subordinate compliance. Security management is no different.
- **Create security policy hierarchy** – The security policy should originate different sets of policies, hierarchically organized, to help people learn how to react to different security situations.

Table 4- Risk Management framework - Match between identified security issues and proposed checkpoints.

Security issues Checkpoints	Issue [1]	Issue [2]	Issue [3]	Issue [4]	Issue [5]	Issue [6]	Issue [7]	Issue [8]	Issue [9]
Context establishment									
Understand third party scope	X	X	X	X	X		X		
Select appropriate services			X	X	X		X		
Risk identification (Identification of assets)									
Consider third party devices								X	X
Consider remote work environment							X	X	X
Consider provider environment							X	X	X
Obtain information from provider	X	X	X	X	X		X		
Consider service vulnerabilities	X	X	X	X			X	X	
Focus on processes and people				X		X			X
Risk identification (Identification of existing controls)									
Know third party security features	X	X	X	X			X		
Risk analysis									
Trust provider expertise	X	X							
Risk evaluation									
Validate risks with provider		X	X					X	
Risk treatment									
Extend awareness programs			X	X		X			X
Isolate work environments			X				X	X	X
Provide secure remote access								X	X
Have backups to SLAs	X	X		X					

Checkpoints Description:

- **Understand third party scope** – Companies should try to obtain as much information about the services it has access to. Consulting with providers is a good way to obtain better insight during context definition.
- **Select appropriate services** – Some services don't offer enough information to make security decisions. Selection of services to satisfy business needs must make sure that security needs are also satisfied.
- **Consider third party devices** – Use of personal devices is upon any business nowadays. There is no way of not considering information stored on these devices during the risk assessment.
- **Consider remote work environment –** Due to new scenario paradigm shifts, work environments located physically outside office perimeters are now common and the information used there must be accounted.
- **Consider provider environment –** Infrastructure used by the service providers must be considered during the assessment. If detailed overviews can't be obtained, at least the service itself must be included.
- **Obtain information from provider –** One key reasoning behind using third party services is the provided external expertise, what includes information about dealing with its services security risks.
- **Consider services vulnerabilities** – Usually third party services have specific vulnerabilities that should be considered, like capacity overflow, link downtime, operations shutdown, etc.
- **Focus on processes and people –** It is unlikely that all risks from the external scenario can be mapped. Focusing on processes and people information assets and their impact can mitigate some of these gaps.
- **Know third party security features –** An inquiry to the provider about security features of its services should be obtained to establish what the current level of security of the environment is.
- **Trust provider expertise –** The lack of control over the third party services cannot transform into fear while evaluating them, since it is likely they will offer smaller technical risks than in-house equivalents.
- **Validate risks with provider –** After identifying risks, it is important to discuss those with the provider. Based on this validation, it is possible that unnecessary investments on the client side are prevented.
- **Extend awareness program** – Because of the scenario dynamics, security training must focus on broader topics, like incident identification and avoidance, instead of narrower issues, like password sharing.
- **Isolate work environments** – Virtualization technology, which powers cloud computing, can be used to offer workers a more controlled work environment, without potentially causing harm to other resources.
- **Provide secure remote access –** Most companies will have to provide users with adequate remote access tools to answer demand for mobility.
- **Have backups to SLAs –** Even though they are an easy way to force service providers into compliance, SLAs can lead into a false sense of security. Other security controls must be in place for failures.

Final Support Framework

The support framework for Security Policy, depicted in Figure 3 inserts a total of 10 checkpoints through the 7 steps from the basic process usually taken during this activity. The support framework for Risk Management, depicted in Figure 4 includes a total of 15 checkpoints through the 8 steps of the basic process.

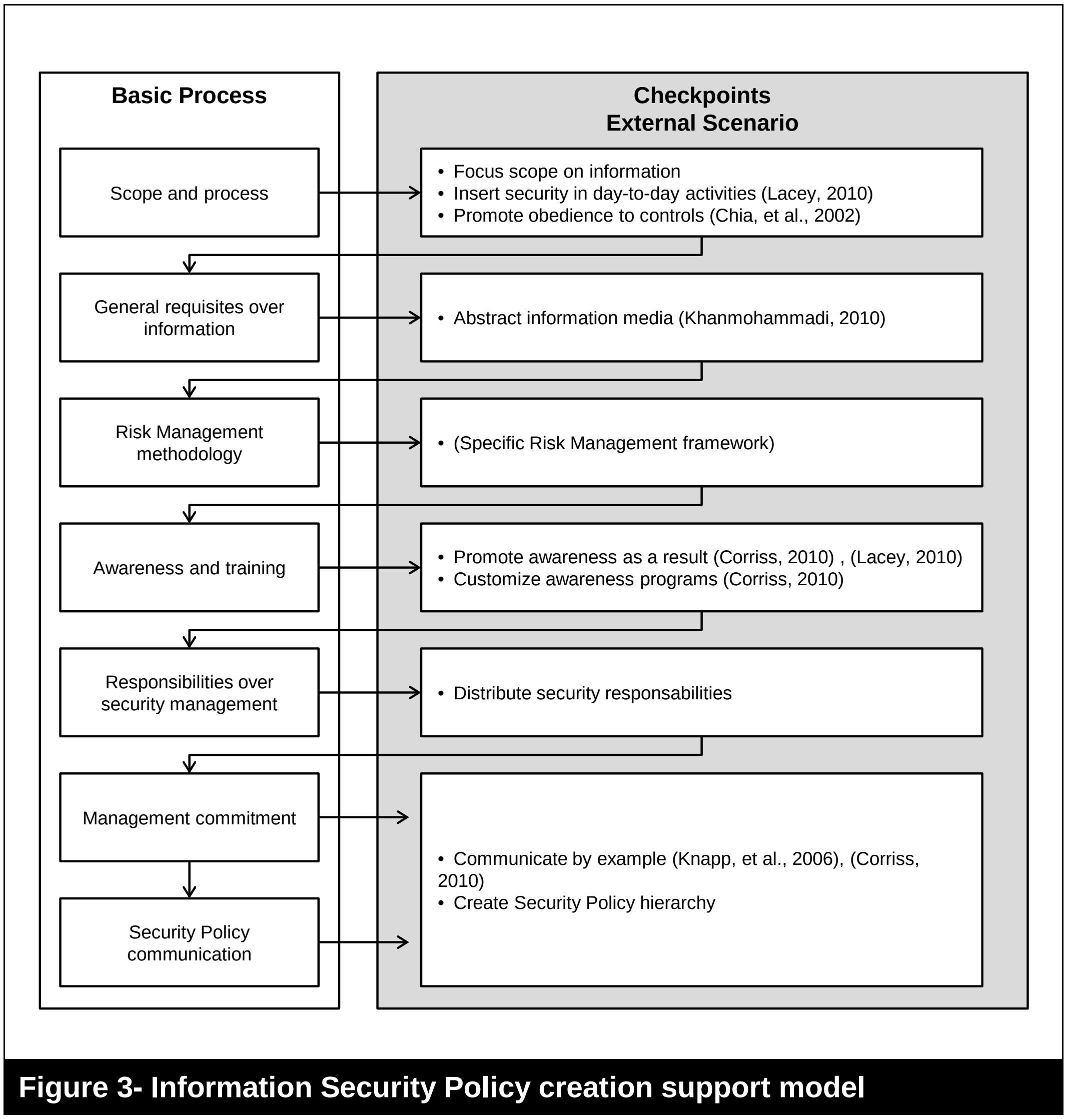
Basic Process
Checkpoints External Scenario
Scope and process
• Focus scope on information
• Insert security in day-to-day activities (Lacey, 2010)
• Promote obedience to controls (Chia, et al., 2002)
General requisites over information
• Abstract information media (Khanmohammadi, 2010)
Risk Management methodology
• (Specific Risk Management framework)
Awareness and training
• Promote awareness as a result (Corriss, 2010) , (Lacey, 2010)
• Customize awareness programs (Corriss, 2010)
Responsibilities over security management
• Distribute security responsabilities
Management commitment
Security Policy communication
• Communicate by example (Knapp, et al., 2006), (Corriss, 2010)
• Create Security Policy hierarchy

Figure 3- Information Security Policy creation support model

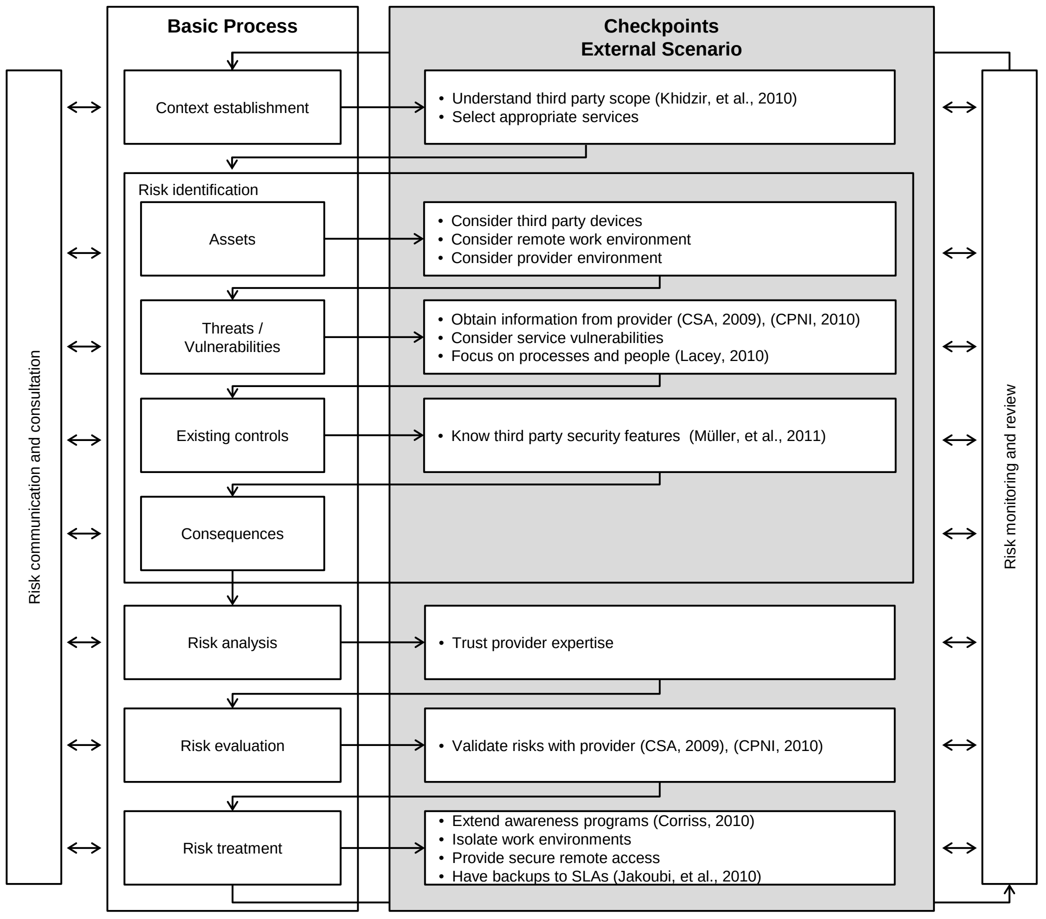
Basic Process
Checkpoints
External Scenario
Risk communication and consultation
Risk monitoring and review
Context establishment
• Understand third party scope (Khidzir, et al., 2010)
• Select appropriate services
Risk identification
Assets
• Consider third party devices
• Consider remote work environment
• Consider provider environment
Threats / Vulnerabilities
• Obtain information from provider (CSA, 2009), (CPNI, 2010)
• Consider service vulnerabilities
• Focus on processes and people (Lacey, 2010)
Existing controls
• Know third party security features (Müller, et al., 2011)
Consequences
Risk analysis
• Trust provider expertise
Risk evaluation
• Validate risks with provider (CSA, 2009), (CPNI, 2010)
Risk treatment
• Extend awareness programs (Corriss, 2010)
• Isolate work environments
• Provide secure remote access
• Have backups to SLAs (Jakoubi, et al., 2010)

Figure 4- Risk Assessment development support model

Applicability Study

The company selected for the applicability study of the proposed support framework was INTEGRA (fictional name), which works with Information Technology in the Brazilian market. INTEGRA is part of a larger conglomerate, called INFRA Group (fictional name), which is specialized in the construction of different types of basic infrastructure.

The applicability study was not meant as a way to test the effectiveness of the framework – the improvement in security due to its application. It is meant as a study on the effort needed to use the framework with ISMS already in place in an organization. It is also meant as an study on the level of effort required to adjust the organization`s practices due to the framework checkpoints.

Contextualization

The INFRA Group has been active in Brazil for over 50 years, while INTEGRA has been active for over 13 years (created in 2000). Since its creation, INTEGRA went through different changes to adapt its line of business to the ever changing Brazilian technology market. Currently, INTEGRA employs over 600 people and it is one the largest systems integrators in the country.

In its market, INTEGRA has specialized itself in combining equipment from different manufacturers to construct solutions that fulfill its customer`s needs. In order to do that, it built a solid set of relationships with different partners, most of them hardware manufacturers, and trained its employees to use their solutions. Because of the expertise acquired over the years, INTEGRA now have most of the country top corporations as its customers, including all telecommunications service providers.

To provide these services, INTEGRA must rely on a very robust and flexible ITC infrastructure. This infrastructure includes most of the typical corporate solutions – e-mail, file servers, Enterprise Resource Planning software, etc. – as well advanced solutions. This last group comprises the type of solution which INTEGRA also sells to its customers – telepresence, videoconference, telephony, collaboration, messaging, social networks, etc.

Because of the need to maintain high standards for all the services provided, INTEGRA has certified three of its management systems: Quality, with ISO 9000; Services, with ISO/IEC 20000 and finally and most important for the purpose of this research, ISO/IEC 27001.

As expected from a company with these characteristics, INTEGRA is deeply inserted in the technological external scenario described in this paper. Following is a brief analysis of the role of each of the key technological trend at INTEGRA.

IT Infrastructure Outsourcing

INTEGRA has gone through two different phases regarding IT outsourcing. During its first phase it has outsourced its entire infrastructure to an external provider, as part of INFRA’s strategy of costs reduction and focus on the core activities its child companies.

After 2010, INTEGRA started to provide outsourcing services to its customers. These services were executed by a specific team trained for this task. As a result, all INFRA’s companies decided to insource their infrastructure back from the external provider to this team, which started to act as an internal provider. For all effects, all these companies are treated the same way as regular customers by this internal provider.

As expected, several security adaptations were needed in both transitions. In the first transition, to the external provider, different negotiations took place to ensure that all security policies from INTEGRA were going to be respected. That was necessary to maintain ISO/IEC 27001 certification. In the second transition, to the internal provider, the main issue was to incorporate in the internal infrastructure the same security controls deployed by the external provider.

Because of this background, it is noticeable that INTEGRA has a large experience with IT outsourcing. Not only it has been using it for years, but it also provides it to its customers.

Cloud Computing

INTEGRA was one of the first companies to use services from cloud providers in Brazil. Currently it deploys three applications in the SaaS model.

The first one is Customer Relationship Management (CRM) software, accessed directly only by a fixed group of people and indirectly by a large group of people (only reports). The second application is a IT Service Management (ITSM) software, which stores information from incidents detected in the customer`s infrastructure. This information is usually accessed only by analysts and specialists from the services team. The last one is a Web Conference service, used for internal and external meetings.

Currently INTEGRA has a lot of questions regarding the security of these applications, mostly because all of them handle very sensitive information, which must be protected according to the ISO/IEC 27001 ISMS.

Mobility

Recently INTEGRA has gone through a complete refresh of all notebooks and smartphones, where a large set of new applications were made available to employees. With these applications, they are able to reach a large share of the infrastructure available from inside the office.

Besides corporate devices, a large number of personal smartphones and tables are allowed into the infrastructure. INTEGRA recognizes the importance of the devices to work and the benefits of their use to productivity. Recently INTEGRA also made a remote work program available to employees.

Application of the support framework

Because of the vast amount of information manipulated by INTEGRA during its activities, it has developed a strong sense of information security within the company. The certification on ISO/IEC 27001 received by the company in 2006 was one of the first that happened in Brazil.

To support its management systems, INTEGRA developed a documentation system where it stores key information about them. To analyze the applicability of the proposed support framework to INTEGRA, these documents were carefully analyzed. When doubts were found about any document, informal meetings took place with INTEGRA security managers to clarify each issue.

Based on INTEGRA documentation, one can find clear evidence of the execution of each of the steps mentioned in the basic processes shown in Figure 2. Therefore it is possible to verify, for each part of these processes, the checkpoints available in the support framework and identify if the checkpoints could require changes to the ISMS approach used by INTEGRA.

The criteria used to quantify the level of change required by each checkpoint are depicted in Table 5.

Table 5- Criteria used to evaluate each checkpoint from the support framework.

Low	The analysis shows that the verification proposed by the checkpoint is already incorporated in the ISMS approach of the organization. Because of that, the expected results from that checkpoint can already be observed in the organization`s current state. Therefore, low or no effort is expected from the organization to adapt its ISMS approach.
Medium	The analysis shows that the verification proposed by the checkpoint is partially incorporated in the ISMS approach of the organization. Because of that, only part of the expected results from that checkpoint can be observed in the organization`s current state. Therefore, medium effort is expected from the organization to adapt its ISMS approach.
High	The analysis shows that the verification proposed by the checkpoint is still not incorporated in the ISMS approach of the organization. Because of that, no expected results from that checkpoint can be observed in the organization`s current state. Therefore, high effort is expected from the organization to adapt its ISMS approach.

presents the result of the analysis of each checkpoint from the Security Policy definition framework, respecting the criteria defined before.

Table 6- Evaluation of the checkpoints from the Security Policies definition support framework

Checkpoint	Evaluation according to INTEGRA's context	Expected effort for adaptation
Create scope focused on information	The ISMS scope is complete, however is still expressed in terms of specific teams and areas, instead of the information to be protected.	Medium
Insert security in day-to-day activities	The ISMS processes are still treated as a side module of operations that must be kept.	High
Promote obedience to controls	There is no historical of conscious disrespect to controls. However, incidents are usually not acknowledged or reported.	Medium
Abstract information media	Many information assets are considered to risk analysis only when associated to specific types of media.	High
(Specific Risk Management framework)	The security policy includes the risk analysis methodology. A specific evaluation for it follows this table.	
Promote awareness as a result	Security training is provided to all employees as a one-time only exercise. Besides that, it does not cover basic concepts of security.	High
Customize awareness program	The security training is not customized to any of the areas or teams of INTEGRA.	High
Distribute security responsibilities	The current policy establishes the responsibilities of all employees for the organization's information.	Low
Communicate by example	Specific training was given to top management to make sure they understand their role in developing the security culture.	Low
Create Security Policy hierarchy	There is just one broad security policy in the organization. More specific policies regarding less broad topics are not available.	High

Table 7 presents the result of the analysis of each checkpoint of the Risk Management support framework, respecting the criteria defined before.

Table 7- Evaluation of the checkpoints from the Risk Management definition support framework

Checkpoint	Evaluation according to INTEGRA's context	Expected effort for adaptation
Understand third party scope	Since the ISMS scope is still defined based on specific processes and teams, risk management is not focused on information itself.	High
Select appropriate services	Part of the service providers is already considered in the risk analysis, as well as the internal provider.	Low
Consider third party devices	Data stored in third party devices are not acknowledged in the risk analysis.	High
Consider remote work environment	The remote work program defines some requisites for the infrastructure used at the employee's home. However the same is not done to other locations and this infrastructure is not considered in the risk analysis.	High
Consider provider environment	The environment of the internal provider and cloud providers are not considered in the risk analysis.	High
Obtain information from provider	The internal service provider reports regularly changes in its operations. The same type of information is not obtained from the cloud providers.	Medium
Consider service vulnerabilities	Some service vulnerabilities like unavailability are considered for the risk analysis. However it does not cover all services used by the company.	Medium
Focus on processes and people	Few areas acknowledge people as holding information assets to be protected. None of the organization processes is considered specifically during the risk analysis.	High
Know third party security features	Some of the security features from the internal provider are known and considered. However the same is not done for cloud providers.	Medium
Trust provider expertise	The capacity of the internal provider regarding security is acknowledged. The cloud providers are selected based on their market reputation.	Low
Validate risks with provider	The providers are not considered as a possible evaluators of the risks identified by INTEGRA.	High
Extend awareness programs	The awareness program does not consider training for the identification of different risks.	High
Isolate work environments	Even though workstation virtualization is part of the company offering to its client, it is not used internally.	Medium
Provide secure remote access	Remote secure access is provided to all professionals, through different devices.	Low
Have backups to SLAs	The vast majority of controls related to services is still based only in SLAs.	High

The evaluation of the checkpoints presented in the support framework resulted in a large number of “Medium” and “High” results. That means INTEGRA would have to deploy a considerable amount of effort to adapt its ISMS approach according to the framework, according to the criteria.

Results

From the information presented about INTEGRA and its history, one can see that is a company with solid management practices in the Brazilian market. Some of the evidences of this are the certifications received to its quality, services and security management systems – ISO 9000, ISO 20000 and ISO 27000 respectively.

Besides that, INTEGRA is a company very capable when dealing with the complexities of technology, since it made of it its primary line of business. INTEGRA not only sells top technology to its clients, but is also used to deploy these technologies internally. Finally, INTEGRA is also experienced in adapting itself to changes in this market.

Given this context, one could expect that INTEGRA should easily adapt its security approaches to deal with new uncertainties presented by the new external scenario. However, as the checkpoint evaluation shown, this is not the case.

Discussion

Besides gaining visibility in the last years, information security also gained new challenges. One of these, focus of this paper, is a new external scenario, characterized by three major technological trends: IT infrastructure outsourcing, cloud computing and mobility. Combined, they form a very disruptive context, which require some changes in the way ISMSs are created. In this research, ISO/IEC 27001 is used to show how changes in its ISMS Plan phase could lead to better consideration of these new security requirements.

To do this, the risks associated in the literature with each of the trends were mapped and traced back to a list of common security issues. These were used to define a list of checkpoints that can be used during the activities of the Plan phase. All checkpoints were distributed in a framework, which is split in two models, one of Information Security Policy definition and other for Risk Management. Both models were designed to help individuals facing the difficult task of ISMS deployment, by making clear right from the start issues that otherwise might go unnoticed, resulting in unrealistic policies and risk evaluations.

Both models share the same structure: from each step of the basic process for each activity, the relevant checkpoints related to that step are introduced. Since the basic processes are derived from ISO 27000, it is expected that the usual flow of these activities are not disrupted. Both models share synergy as well. The first one, for security policies, broadens the typical and technology-restricted culture companies have of security, by introducing focus on information itself, despite its media. At the same time, paves the way for the use of the second, since most of the checkpoints also help gather information for risk analysis.

The support framework was tested in a real world organization in Brazil. This applicability study showed that even in an organization very well suited to deal with technological changes, the security risks from the external scenario might be overwhelming. This is because the current approaches for information security might not be enough to deal with this scenario. The proposed support framework help the creation of a new security culture in the organization.

Broader security culture incentive is a key factor of dealing with this new technological scenario. Lacey (2010) explains that “it requires us to re-think both the essence of security management and the nature of the knowledge. In a future world in which citizens are fully connected and services are delivered from within an internet "cloud", the major thrust of security functions will not be to articulate legalistic policies and technical architecture, but to change the perception and behavior of thousands of managers, staff and customers". The proposed framework is a contribution for achieving these goals.

Limitations and Future Research

The applicability study does not prove the effectiveness of the framework. It only shows that it can be easily plugged into a real work organization that follows the basic principles of ISO/IEC 27001. Therefore, the results of this research require the empirical testing of the frameworks. These tests should be based on metrics already used in security management.

As technology evolves, more issues might appear that have not been addressed yet in the literature and in the framework. It would be important to understand the level of effort required by security practitioners to adapt the framework new changes in the technological scenario.

It would be also interesting to understand which kind of customization could be made for different types of company and context, since security is most of the time a context-specific problem.

References

Anderson, J. A. & Rachamadugu, V., 2006. *Information Security Guidance for Enterprise Transformation.* s.l., s.n.

Bacik, S., 2008. *Building an Effective Information Security Policy Architecture.* s.l.:CRC Press.

Chia, P. A., Maynard, S. B. & Ruighaver, A. B., 2002. *Understanding Organizational Security Culture.* Tokyo, s.n.

Corriss, L., 2010. *Information Security Governance: Integrating Security into the Organizational Culture.* New York, USA, Association for Computer Machinery.

CPNI, 2010. *Information Security Briefing 01/2010 - Cloud Computing,* s.l.: Centre for Protection of National Infrastructure.

CSA, 2009. *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1,* s.l.: Cloud Security Alliance.

Doomum, M. R., 2008. Multi-level information system security in outsourcing domain. *Business Process Management Journal*, pp. 849-857.

Gartner, 2011. *Gartner Identifies the Top 10 Strategic Technologies for 2012.* [Online] Available at: http://www.gartner.com/it/page.jsp?id=1826214
[Acesso em 16 06 2012].

Gartner, 2011. *Gartner Reveals Top Predictions for IT Organizations and Users for 2012 and Beyond.* [Online] Available at: http://www.gartner.com/it/page.jsp?id=1862714
[Acesso em 16 06 2012].

Gerber, M. & von Solms, R., 2005. Management of risk in the information age. *Computers & Security*, pp. 16-30.

Gillies, A., 2011. Improving the quality of information security management systems with ISO27001. *The TQM Journal*, pp. 367-376.

Goode, A., 2010. Managing mobile security: How are we doing?. pp. 12-15.

ISO/IEC 27001, 2005. *ISO/IEC 27001 - Information technology - Security techniques - Information security management systems - Requirements.* s.l.:s.n.

ISO/IEC 27002, 2005. *ISO/IEC 27002 - Information technology - Security techniques - Code of practice for the information security management.* s.l.:s.n.

ISO/IEC 27005, 2011. ISO/IEC 27005 - Information Technology - Security Techniques - Information Security Risk Management.

ISO/IEC TR 13335-3, 1998. ISO/IEC TR 13335-3 - Information Technology - Guidelines for the management of IT Security - Part 3 - Techniques for the management of IT Security.

Jakoubi, S., Tjoa, S., Goluch, S. & Kitzler, G., 2010. *A Formal Approach Towards Risk-Aware Service Level Analysis and Planning.* s.l., s.n., pp. 180-187.

Khanmohammadi, K., 2010. *Business Process-based Information Security Risk Assessment.* Melbourne, Australia, s.n., pp. 199-206.

Khidzir, N. Z., Mohamed, A. & Arshad, N. H. H., 2010. *Information Security Risk Management - An Empirical Study on the Difficulties and Practices in ICT Outsourcing.* s.l., s.n., pp. 234-239.

Knapp, K. J., Marshall, T. E., Rainer, R. K. & Ford, F. N., 2006. Information security: management's effect on culture and policy. *Information Management & Computer Security,* 14(1), pp. 24-36.

Lacey, D., 2010. Understanding and transforming organizational security culture. *Information Management & Computer Security*, 18(1), pp. 4-13.

Leavitt, N., 2011. Mobile Security: Finally a Serious Problem. *IEEE Computer Society,* pp. 11-14.

Ma, W.-M., 2010. *Study on Architecture-Oriented Information Security Risk Assessment Model.* Springer-Verlag Berlin, Heidelberg, Association for Computer Machinery (ACM), pp. 218-226.

Mell, P. & Grance, T., 2011. *The NIST Definition of Cloud Computing,* s.l.: s.n.

Milicevic, D. & Goeken, M., 2011. *Application of Models in Information Security Management.* s.l., s.n.

Müller, I., Han, J., Schneider, J.-G. & Versteeg, S., 2011. *Tackling the Loss of Control: Standards-based Conjoint Management of Security Requirements for Cloud Services.* Washington, DC, s.n., pp. 573-581.

NIST, 2011. *SP800-144 - Guidelines on Security and Privacy in Public Cloud Computing,* Gaithersburg: National Institute of Standards and Technology.

Schnjakin, M., Alnemr, R. & Meinel, C., 2010. *Contract-based Cloud Architecture.* s.l., s.n., pp. 33-40.

Siponen, M. T. & Oinas-Kukkonen, H., 2007. A Review of Information Security Issues and Respective Research Contributions. *ACM SIGMIS Database*.

Siponen, M. & Willison, R., 2009. Information security management standards: Problems and solutions. *Information & Management*, pp. 267-270.

Solms, B. v. & Solms, R. v., 2004. The 10 deadly sins of information security management. *Computers & Security*, pp. 371-376.

Tsohou, A., Kokolakis, S., Lambrinoudakis, C. & Gritzalis, S., 2010. A security standards` framework to facilitate best practice` awareness and conformity. *Information Management & Computer Security*, pp. 350-365.

Zavarsky, S. O., Ruhl, R., Lindskog, D. & Igonor, A., 2009. *Managing Risk of IT Security Outsourcing in the Decision-Making Stage.* s.l., s.n., pp. 456-461.

Zhang, X., Wuwong, N., Li, H. & Zhang, X., 2010. *Information Security Risk Management Framework for the Cloud Computing Environments.* Bradford, s.n., pp. 1328-1334.

About Authors

Leandro Malandrin is a graduate student at the Polytechnic School of the University of São Paulo in Brazil. He earned his degree in Computer Engineering (2008) and his Master of Science in Computer Engineering (2013) from the same university. His research interests focus on Information Security Management and IT Governance, and how these practices are affected by technological developments. He also is a senior consultant at one of the largest ITC infrastructure and services providers in Brazil. There, he works for the largest companies in Latin America providing advisory services in Information Security and other topics related to technology utilization.

Tereza Carvalho is Associate Professor at the Polytechnic School of the University of São Paulo. Currently she is also an assessor for special projects of STI (Superintendence of Information Technology), coordinator of LASSU (Laboratory of Sustainability on ITC) and project coordinator at LARC (Laboratory of Computer and Network Architecture). She is responsible for the research and development of systems in IT, network communication, network management, security, on-line business, IT Governance and Sustainability in IT. She got her degree in Electrical Engineering (1980), Master of Science in Electronic Engineering (1988) and her Ph.D. in Electronic Engineering (1996) from Polytechnic School. She concluded her Sloan Fellows Program (2002), as postdoctoral work, at MIT – Massachusetts Institute of Technology, USA.