ISO 27002 vs. COBIT: Security Information Planning

Introduction

There is an important relationship in today´s Organizations: the higher the contact or interaction with the business world, the greater the need to introduce technology to be competitive and greater is the information that is generated. Thus, the more technology has it and more exposed the business (presence or recognition), higher the exposure of information assets. However, this leads to being targeted by all kinds of unauthorized actions or attacks that violates the IT safety in the organization.

It is in these truth moments, when an organization can´t wait, and should determinate that their information assets be protected against threat and vulnerabilities, establishing measures to protect the confidentiality, integrity and availability: key criteria for the information security.

To obtain such measures, the organizations must go to beyond just putting a people’s group to thinking about that, should watch the development of a Security Information Planning, basis to ISMS (Information Security Management System). But don't anticipate us, they simply, must manage a plan to help them define what the organization should be done to warrant the security of information asset, IT and the associated risks. Is where best practices or frameworks as ISO 27002 or COBIT, provide a structural way, the work.

But, let´s begin of basics: What is Information Security Planning?

The Information Security Planning, is the information security system´s design for an organization, which sets the organizational and functional standards and policies of activity of information security, define the responsibilities of each participant in the process of IT assurance, and specify the safeguard, countermeasures and procedures that will prevent, detect and respond to threats and vulnerabilities that impact the security of information assets.

To develop the plan, it is necessary to perform a series of previous activities, to give an exact account the need for protection:
- Classify information assets that need protection, of critical business services and process.
- Identify internal and external threats that can come to realize the assets and vulnerabilities or weakness that could explode.
- Identify and assess risk, calculating the probability of occurrence of threats and vulnerabilities of information assets.
- Establish the risk treatment options, which should be applied to reduce safeguards and countermeasures.

**Now let’s analyze: what are safeguards and countermeasures?**

In the presence of vulnerability (weakness of assets or groups that can be exploit for one or more threats - ISO/IEC 13335-1:2004), the organizations must establish **safeguards**: measures that define what must be achieved, better known as **Control Objectives**. E.g.:

<table>
<thead>
<tr>
<th>Vulnerability: Lack of information security awareness</th>
<th>Provide guidance and support for management information security, according to business requirements, laws and regulations. (ISO 27002 – 5.1)</th>
<th>Communicate Management Aims and Direction (COBIT – PO6)</th>
</tr>
</thead>
</table>

And with a threat (a potential cause unwanted incident, which may result in damage to a system or organization - ISO/IEC 13335-1:2004), organizations must establish **countermeasures**: actions that are applied to achieve the control objectives and allow verify, analyze, measure whether the activity, process, service or system it is meeting or not the expected results, better known as **Controls**. E.g.:

<table>
<thead>
<tr>
<th>Countermeasure: unauthorized use or inappropriate IT resources</th>
<th>Document security policy (ISO 27002 – 5.1.1)</th>
<th>Assurance that IT policies are implemented and communicated to all relevant staff (COBIT – PO6.4)</th>
</tr>
</thead>
</table>

With these sources, is determined by the organization when dealing with IT risks identified must implemented control objectives and controls to mitigated them, have at their disposal standards, best practices proved and internationally recognized, that facilitate and help define what should be done and allow effective governance in the management of information security.
**Why ISO 27002 and COBIT?**

Because, in general:

- They’re internationally designed and tested tools that have effective actions for the assurance IT.
- As standards and practices, enabling organizations, based on its particularities, adjust according to their needs.
- Faced to regulatory entities and contractual, enable the action and effective response.

In particular, **COBIT** framework geared to General Managements, give sponsors and IT responsible elements to control and manage of IT governance, the basis for design the information security planning. As the information and technology the most important assets is the management who is the strategic guidelines, approves and provides the necessary resources for establishing the plan.

**ISO 27002**, best practice that give to information security responsible, the elements needed to manage security, guidelines for structuring the information security planning and control objectives and controls necessary to implement security in the organization, key actions to minimize the risks that jeopardize the information security.

In conclusion, **ISO 27002** and **COBIT** provide the necessary elements to develop an information security planning, not only for being easily adjustable to best practice business, but also from the organizational strategy to allow frame the information security: to understand the IT and security requirements, in designing those policies and procedures, implementing and operating controls to manage risks and to be value added for the protection of information as a core asset in an organization.

---

**Mónica María Toro García**  
Manages Audit of Technology - IT Auditor  
Grupo Bancolombia S.A.  
**ISACA CRISC - Certified in Risk and Information Systems Control**  
**IRCA ISMS Auditor**  
**BSI Lead Auditor ISO 27001:2005**