NEW SCHEME FOR THE INFORMATION SECURITY MANAGEMENT WITH ISO 27001:2013

INTRODUCTION

The Organization´s tendency to implement and certificate multiple Managements Systems that hold up and align theirs IT´s operations, process, services and infrastructure in an integrated and combined, raised the need to adjust the management standards (recent case: ISO 22301:2012 - Management Systems Business Continuity and aligns next to: ISO 9001 – Management System Quality) in a simple manner, but ensuring the efficiency and effectiveness has characterized the Management Standards.

For this, was important that common parts or sections, were aligned under the same schema or format, but warranting that save the differences that exist between them. Thus, to achieve this relationship, has been applied the **SL ANNEX – ISO/IEC**, framework that provide the common guidelines and requirements documentary development of any Management System, and allowing customized conservation requirements each standard (Quality, Environmental, IT Service, Continuity and Information Security, among other), so as to standardize the terminology an fundamentals requirements to supply the interpretation and implementation of joint.

Specifically to standard ISO 27001:2005, for this year 2013 is a need to restructure under the new approach, since March the BSI (*British Standard Institute*) published the draft international standard **ISO/IEC – 27001:2013**, and whose final product is expected to publish on October this year, bringing renewal in terms to integrality, risk, controls and security.

NEW STRUCTURE

The new standard structure **ISO 27001:2013** includes the following levels of management:

0 Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Context of the organization
5 Leadership
6 Planning
7 Support
8 Operation
9 Performance evaluation
10 Improvement

Additionally, in to regard the annexes:

- Annex A (Controls and Objective Controls) was unchanged (updating, adding and removing controls), as detail below.
- Annex B (OECD principles and the International Standard) and C (Corresponding between ISO 9001:2000, ISO 14001:2004 and the International Standard), were removed.

Know a little more in detail the changes in each clause of **ISO 27001:2013** version.

0. Introduction

The Processing Approach, used in ISO27001:2005, and which houses the PDCA model, was eliminated), to the new structure it´s immersed in all mandatory clauses and is an integral part of standard.

In his absence, the General numeral is strengthened by the review of the risk management applications that protect the pillars of the information security (confidentiality, Integrity and availability) and gives confidence to stakeholders that the risk are properly managed.

Also, it states that the information security management system it´s part of and combined with Organization´s process.

1. Scope

Forming in ISO27001:2005, by paragraphs 1.1 Generals and 1.2 Application, was removed to 2013 version, and formed a single section where established the mandatory fulfillment of the requirements defined in numerals 4 to 10, in order to obtain compliance and apply for certification.

2. Normative references

In **ISO 27001:2013** is excluded as normative references to application of the standard, ISO27001:2005, however, is still necessary for the development of the Statement of Applicability.

Additionally, the **ISO 27000:2013** happened to be the only and obligatory normative reference for **ISO 27001:2013**, unified way to understand the terms and definitions.

3. Terms and Definitions

The terms and definitions applied to standard ISO 27001:2005 were transfer to **ISO 27000:2013**, which as announced in the previous section, the issue is to have a guide only to these items.

4. Context of the organization

Formerly Information Security Management System was renamed in the **ISO 27001:2013** by Context of the Organization, approach on understanding the organization and composition (independent of the type, scope and conditions), in to the interpretation of the needs and

expectative of stakeholders (aspect becomes more relevance to defined the scope and witch generated independent clause), in defining the scope to information security management system and information security government.

5. Leadership

The Management´s responsibility in **ISO 27001:2013** is reconsidered, in order to take into consideration the need for leadership and Management commitment, where you can look at the specific requirements of the Senior Management in the ISMS, underlining the detail as the Management must commit with the system so that it lead to relate to the needs of the Organization.

It states that the important roles and responsibilities of information security are established and communicated.

And in additional, to establishing an information security policy before Policy Information Security Management System (ISO 27001:2005), which together with the ISMS´s objectives should ensure alignment with the business's objectives.

6. Planning

In the new structure, ISMS Internal Audits disappears to give way in **ISO 27001:2013** to Planning, where the establishment of the information security´s objectives and outlining specific plans for achieving them and guides ISMS´s principles.

Set alignment with ISO 31000:2009 – Standard for Risk Management. Where the scheme of information assets, threat and vulnerabilities no longer the basis for risk assessments, the methodology is oriented to identify the risks associated with the loss of Information´s Confidentiality, Integrity and Availability. It remains, the establishing the risk level form the consequence or impact and likelihood of risk occurrence.

It adopts the concept Owner or Proprietor´s risk, like a new function in risk management as a order to ensure that responsibility for risk is in the high levels of the Organization and disappears the concept of Ownership of Asset.

SoA Requirements (Statements of Applicability) have greater clarity in determining the controls for the risk management process.

7. Support

This new paragraph outlines the support requirements for the establishment, implementation and improvement (Resources, Skills, Awareness, Stakeholders communication and documented information) ISMS.

Specifically, the Documentation Requirements described in the ISO 27001:2005, although was removed the requirement of maintaining documented procedures, remains the documentation of

the results of such proceedings. Also, there is the concept Documented Information, which combines the documents and registers (previously covered by ISO 27001:2005), so that all the rules and guidelines for the control of documentation are valid and legitimate for both (documents and registers).

Furthermore, the section Communications provide the statement to the Organization of the Information Security is an integral part of the business and not something that purely technical matter solely for the areas of Technology, highlighting the importance of information´s protection.

Remember that the PDCA model, as driving in the ISO 27001:2005 disappeared explicitly for the new version. However, so far, the numerals described (4 to 7) area a component of the Plan stage, since it´s where you enter and define the requirements to be considered to establish the ISMS.

8. Operation

This new clause of **ISO 27001:2013**, is a component of the stage Do, that describe the requirements for measuring the performance (efficiency and effectiveness) ISMS, the expectations of the Senior Management and the compliance with the standard.

Also, it includes the definition of a program to regularly assess the information security risk management, for purposes of planning and controlling the security´s operations and requirements.

In addition, management is performed (evaluation and treatment) information security risk, based on the defined approach (methodology and levels).

9. Performance evaluation

They focus in this clause, the guidelines given in ISO 27001:2005 Internal Audits and ISMS Reviews, to identify, measure, monitor and evaluate the effectiveness and performance management system by the Senior Management responsible, being a component Check stage.

10. Improvement

Being a part of the stage Act, refers explicitly to detected nonconformities to be identified, quantified and collated to establish corrective actions to minimize repetition and continuous improvement.

In **ISO 27001:2013**, does no refer to the Preventive Actions described in ISO 27001:2005, which were immersed in the risk evaluation and treatment like actions to address risk and opportunities.

Annex A

The security controls and objectives controls (Annex A) were changed in order to support withstand current (mobility, cloud, etc.), changes that are reflected in the ISO 27002.

You go from having 11 to 14 sections, for reorganization, addition and removing in the same objectives controls and controls:

5 Information security policy
6 Organization of information security
7 Human resource security
8 Asset management
9 Access control
10 Cryptography
11 Physical and environmental security
12 Operations security
13 Communications security
14 Information systems acquisition, development and maintenance
15 Relationship with external parties
16 Information security incident management
17 Information security in business continuity management
18 Compliance with legal and contractual requirements

These improvements impact the alignment with the business policies, process and procedures existing and necessary to construct, given the new technologies and environment (cloud computing case and the relationship with suppliers).

Additionally, another novelty in Annex A, is that since the controls are a complement to the information security controls that must be defined in the risk treatment, giving the Organization the possibility to take controls of other standards or frameworks and compare with Annex A or ISO 27002, to ensure that all have been considered necessary.

CONCLUSION

In the 2013 version of ISO 27001, the changes to which it was subjected, project not only the integration with others standards for the implementation of several managements systems to speak the same structural languages, but also provides for the adoption to new technology trends, allowing the implementation of guidelines and requirements in line with reality technology and business.

This new structure of ISO 27001, involves challenges, changes and variations in how the Organizations should address it, because companies that are certified under the 2005 version, have a period of time (usually two years) to upgrade to the new version (2013), where the impact can be reduced because you can see the development of internal audits (contracted or developed into) to detect respective differences and changes, to establish and develop actions aimed at achieving the requirements defined in the new version of the standard.

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