



Above SECURITY

1919, Lionel-Bertrand Blvd.
Suite 203
Boisbriand, Quebec J7H 1N8
Canada
Telephone :
450-430-8166
Toll Free :
866-430-8166
Fax :
450-430-1858
info@abovesecurity.com

Peace of mind

White Paper

Risk Management Standards Applicable to the Implementation of an ISO27001 Information Security Management System (ISMS)

Prepared by
Martin Dion
CISSP, CISM, ISO:27001 Lead Auditor & Trainer
Above Security

Publication date
March 2008



'Above Security is the only pure-play MSS provider that merits consideration as a potential leader.'

IDC Canadian Managed Security Services 2006 Vendor Analysis

Table of contents

EXECUTIVE SUMMARY.....	3
INTRODUCTION	4
BS7799-3:2006 GUIDELINES FOR INFORMATION SECURITY RISK MANAGEMENT.....	5
AS/NZ 4360:2004 RISK MANAGEMENT GUIDELINES.....	6
AS/NZ HB 231:2004 INFORMATION SECURITY RISK MANAGEMENT GUIDELINES	7
ISO/IEC 27001:2007 INFORMATION SECURITY MANAGEMENT SYSTEMS - REQUIREMENTS ..	8
ISO/IEC 27002:2005 CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT	9
ORGANIZATIONAL PROFILE	10
CONTACT US	10
COPYRIGHT	10

Executive Summary

When introducing a procedure for risk management in an organization, it is up to management to choose a method compatible with the needs of the organization.

Not only should the method allow to identify and to deal with the risks, but it should also allow for the introduction of a frame of reference for them.

Risk management refers to the introduction of a reproducible process which insures:

1. The identification of threats and vulnerabilities which the organization faces;
2. The identification of the levels of tolerance of the organization towards these risks;
3. The establishment of a measureable approach that would allow for the evaluation and the prioritization of the risks while handling them;
4. The establishment of a clear method of risk treatment; and
5. The follow up of the residual risks and the operating methods to identify the new risks and to reevaluate the existing risks that the company faces.

This white paper aims at supplying you with an insight into the standards and methods that we recommend for setting up an organization's risk management system.

It describes the various ISO standards that support the introduction of this management system as well as the ISO: 27001 and ISO: 27002 standards, which are specific to the set up of an ISMS.

The ISO methods that were selected and which are described in this white paper were chosen because they respond to the needs of the ISO :27001 standards as to the certification of the ISMS (Information Security Management System) in regards to the risk management process, that must necessarily be put in place, in order for a company to obtain its certification.

It is important to note that other specifications and risk management methods exist (NIST, Octave, EBIOS, Mehari for example). They will not be treated in this white paper, which covers only the ones recognized by the International Standards Organization (ISO).

Enjoy your reading,

A handwritten signature in black ink, appearing to read 'Martin Dion'.

Martin Dion, CISSP/CISM
ISO:27001 Lead Auditor & Trainer
CTO, Above Security

Introduction

This white paper will cover the following five standards:

- BS 7799-3:2006 Guidelines for Information Security Risk Management
- AS/NZ 4360:2004 Risk Management Guidelines
- AS/NZ HB 231:2004 Information Security Risk Management Guidelines
- ISO/IEC 27001:2007 Information Security Management Systems - Requirements
- ISO/IEC 27002:2005 Code of practice for information security management

These five standards complete one another, as you will see on the next pages.

Each one of these standards will be presented summarily in this white paper.

BS7799-3:2006 Guidelines for Information Security Risk Management

The identification, the evaluation, the treatment and the risk management in matters of information security are key processes for the organization that wishes to preserve the safety and security of its information. Even though these processes are identified in the ISO 27001 :2005 standards, instructions and supplementary guidelines must be established, on how risk management, and their alignment with the other risks of the company, must be handled.

BS 7799-3 :2006 supplies these instructions and guidelines and covers the following elements :

- Risk analysis
- Risk treatment
- Management decision process in the face of risk
- Reevaluation of the risks
- Surveillance and review of the risk profiles
- The risks related to information security in the context of corporate governance
- Compliance with other specifications, standards and regulations in risk management.

BS 7799-3 :2006 supplies clear instructions supporting the many prerequisites established by ISO/IEC 27001 :2005 standards, in regards to all the aspects of the risk management cycle, as required when setting up an Information Security System.

These requirements include the analysis and the evaluation of the risks, the implementation of controls to deal with the risks, the surveillance and the review of the risks as well as the maintenance and improvement of the risk management system.

The focus of this specification is the attainment of efficiency in matters of information security by the introduction of a continual training program of risks related activities.

The instructions and continual guidelines in the BS 7799-3 standards are applicable and are suited to all types of organizations, regardless of their type, size or nature of activity.

They address themselves to many players, executives and their teams, involved in the risk management activities related to ISMS.

This standard, being already under review by the ISO, will be integrated, when completed, under the name of ISO :27005 – Security techniques – Information security risk management.

AS/NZ 4360:2004 Risk Management Guidelines

This standard provides instructions and general guidelines to risk management. It applies, as does BS7799-3, to a wide range of activities, decisions or operations in private, public and governmental contexts and even at the organizations' departmental level.

Even though this standard addresses itself to a wide range of customers, it is important to understand that the risk management process is common to almost all types of entities, which is why we use the term 'organization' to define them.

This standard specifies all the elements that compose the process of risk management. It puts in perspective the independence of this process in relation to the industry or to the economical framework of the organization.

It takes into consideration that the adoption and implementation of a risk management process will be influenced by the many individual needs of an organization, its particular objectives, its products and services, its procedures and its regulated obligations.

Even though the standard applies to different stages in the life cycle of the activities, functions, projects, products or assets of the organization, it is understood that the maximum benefit cannot be attained, unless the process is respected from the beginning of the life cycle of the elements previously mentioned.

The different stages suggested, when setting up the procedure and operation of the organization, take into consideration the strategical aspects as well as the operational aspects of the organization.

It is important to note that the standard takes into account not only the potential gains, but also the potential losses, all in a systematic spirit, in order to treat the different aspects of risk in the organization during their life cycle.

The standard is completed by the manuals HB :436 – Risk Management Guidelines Companion Guide, which offers the methods of identification, analysis, appreciation and treatment of risk in the organization.

A second manual, the HB :231 – Information Security Risk Management Handpaper, which addresses more specifically, like the BS7799-3, the risks related to the information security of the organization, is available. (Please see the following section for our review of the manual HB :231.)

AS/NZ HB 231:2004 Information Security Risk Management Guidelines

Risk management is known as being an integral part of good management practices for an organization. The risk management process is an interactive process consisting of steps, which, when followed in sequence, allow for an improvement in the decision making process.

Generally, the risk management process, applied to the information security, aims at the entire information security system and the ways of treating it, but the proconcised methods in this manual also allow for the evaluation of a subset of components or of service when practicable, realistic or necessary.

It is a reference manual aimed at three specific audiences:

1. The members of management in charge of information security;
2. The personnel responsible for the initiation, implementation and/or surveillance of the risk management of the organization; and,
3. The personnel responsible for the initiation, implementation and/or maintenance of the Information Security Management System of the organization.

Since this manual is based on the standard AS/NZ 4360 :2004, it respects the following main instructions :

- The adoption and implementation of a risk management process is influenced by the various needs specific to each organization, its particular objectives, its products and services, its procedures and regulatory obligations;
- Even though the standard applies to different stages of the life cycle of activities, functions, projects, products or assets of the organization, it is understood that the maximum benefit cannot be attained, unless the procedure is adhered to from the beginning of the life cycle of the previously mentioned elements; and,
- That the various stages suggested, when setting up the procedures and operations of the organization, take into account the strategic aspects as well as the operational aspects of the organization.

It is important to note that this manual is specific to the information systems and components of an ISMS (ISO :27001) and that it was not created in order to cover the risk management in the context of a >health and safety< or >safety in the utilization of electrical/electronic/programmable devices<.

This manual was prepared in order to support the needs of the ISO :27001 standards and the selection of adequate controls in the treatment of risks, as detailed in the ISO :27002 standards.

ISO/IEC 27001:2007 Information Security Management Systems - Requirements

The origins of the ISO/IEC 27001 :2007 standard go back to the mid 90's, when the British Standard Institute (BSI) set up several work groups and committees, in order to elaborate specific standards in information security management and in the certification of the Information Security Management System.

Over the years, and following the massive adoption of this standard across the British Commonwealth (standard known originally under the name BS :7799), ISO decided to adopt and integrate the BS7799 in its standards' corpus. A sub-committee was formed, today known as SC27000, which adopted and standardized the numbering of the standard.

The standards of BSI were in two parts, that is the BS7799-1 and the BS7799-2, this last one being the standard establishing the requirements for the ISMS certification. This certification standard is now known under this name and bears the number ISO :27001.

The standard is adapted to all types of organizations and specifies the conditions to respect at the time of the establishment, implementation, operation, surveillance, review, maintenance, documentation and improvement of ISMS, in the specific context of risks that a particular organization faces. It also specifies the necessity for an organization to introduce the adequate controls, personalized to its own needs.

The certification of ISMS is designed to show that a structured procedure has been respected. This procedure allows the organization to establish and assure independently, through a registry, a level of confidence to interested parties, on the adoption of appropriate controls throughout the organization.

The standard establishes the obligations of the organization in the implementation process and operation of ISMS in matters of:

- Procedure and instructions in matters of information security;
- Identification, treatment and management of risks related to the organization;
- Information Security Management with the aid of applicable controls;
- Responsibility of the management team;
- Documentation of the various procedures related to the ISMS operation;
- Reviews and audits of ISMS; and,
- Continuous improvement to ISMS.

All organizations should evaluate the introduction of the ISO/IEC 27001 :2007 standard. The certification of an ISMS organization assures their customers and suppliers that information security is serious in the eyes of the management team and that the organization has put in place a process that will allow to adequately handle the threats and risks that the organization faces.

ISO/IEC 27002:2005 Code of practice for information security management

As the ISO :27001 standard, the ISO/IEC 27002 :2005 standard originated from the British Standard institute. Previously known under the name of BS :7799-1, this standard, now known under that name and bearing the number ISO :27002, is also overseen by the sub-committee ISO 27000.

The standard ISO/IEC 27002 :2005 establishes the lines of instruction as well as the general principles necessary for the initiation, implementation, maintenance and improvement of the information security management of the organization. Please note that it is not talking about the improvement of the management system, but about the management itself.

In fact, and contrary to the ISO :27001 standard, the defined objectives, in this standard, do not cover the Information Security Management System, but rather the controls generally accepted by the industry, necessary to mastering security in the organization. This document is therefore an essential companion and inseparable to the 27001. The good practices and controls, defined in the standard, are grouped in the following 11 categories:

1. Security procedure
2. Organization of information security
3. Asset management
4. Security related to human resources
5. Physical and environmental security
6. Exploitation and telecommunications management
7. Access control
8. Acquisition, development and maintenance of information systems
9. Management of incidents related to information security
10. Management of the activity continuity plan
11. Compliance

In fact, the ISO :27001 standard expects, as described in its annex, that the control objectives, as well as the controls described in detail in the ISO :27002 standard, be introduced in order to deal with various risks, identified in the organization.

The main objective of this standard is, and has always been, to be a reference and common communication base for the industry professionals, in order to allow the establishment of organizational procedures, while respecting a standard, thereby promoting a standard language and building bases of confidence, by the use of a common extra-organizational system.

Organizational profile

Founded in 1999, Above Security is one of the leading Canadian companies specialized solely in information security. Our mission consists in supporting our customers in the improvement of their information security governance.

With over 200 organizations, our customer base extends to over twenty countries in the three Americas, Europe, the Caribbeans and Africa. It is composed mainly of governmental entities and private industries of Fortune 500 from the financial, pharmaceutical and telecommunications sectors.

Contact us

Above Security Canada

1919 Lionel Bertrand, suite 203
Boisbriand (QC) Canada, J7H1N8

Telephone : (450)430-8166

Fax : (450) 430-1858

E-mail : info@abovesecurity.com

President & Chief Executive Officer

Marcel Dion, CGA

Telephone : (450) 434-8055

Marcel.dion@abovesecurity.com

Chief Technology Officer

Martin Dion, CISSP/CISM

Telephone : (450) 434-8045

Mobile : +41.79.516.0447

Martin.dion@abovesecurity.com

Vice-president, Operations

Daniel Gaudreau

Telephone : (450) 434-8046

Daniel.gaudreau@abovesecurity.com

Vice-president, Strategic Consulting

Guy Langevin, Eng.

Telephone : (450) 434-8051

Guy.Langevin@abovesecurity.com

Copyright

The information contained in this document is the exclusive property of Above Security and from its respective creator. Any reproduction in full or in part of this document is prohibited. This document is for the internal use only.