



Devoteam

Risk Standardization

How it could lead to a better Risk approach

Version 1

CONNECTING BUSINESS & TECHNOLOGY



ICT & Standardization

- Standardization is essential for Information and Communication Technologies (ICT) : without it, networks, services, unable to share information wouldn't work. It authorizes interoperability between systems and equipments and contribute to create trust among users.

- Three main advantages for enterprises :
 - New go-to-market
 - Economy of scales
 - Savings



CONNECTING BUSINESS & TECHNOLOGY

- « *Many information systems have not been designed to be secure. The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures..* »

- Introduction to ISO/IEC 17799:2000(E)

DEVOTEAM GROUP

CONNECTING BUSINESS & TECHNOLOGY

Information Security Process

- Information Security (IS) is not only a technical issue.
- Information Security implies a global approach:
 - Organisational
 - Technical
 - Legal

DEVOTEAM GROUP

CONNECTING BUSINESS & TECHNOLOGY

Don't reinvent the wheel ... of Deming !

- Given the scale and complexity of the process, two lanes are typically followed :
 - Best practices
 - Standards

Approaches

Several frameworks used within the IS field		
Approach orientation	Best practices / Methods	Standards (i.e.)
Risk Management	MEHARI EBIOS OCTAVE	ISO/CEI 27005:2008 ISO/FDIS 31000 IEC/FDIS 31010
Process Management	ITIL	ISO/CEI 9001:2008 ISO/CEI 13335-1:2004 ISO/CEI 20000-1:2005 ISO/CEI 18044 :2004
Controls / Security measures	COBIT	ISO/CEI 27002:2005 ISO/CEI 20000-2:2005
Products		ISO/CEI 15408-1:2005 (common criteria)

Why getting standardized ? (1/4)

- Among the lessons of implementation of successful management systems, we can identify some key success factor :
 - Management Board commitment
 - Users awareness
 - Business targets taken into consideration
 - Iterative approach



CONNECTING BUSINESS & TECHNOLOGY

Why getting standardized ? (2/4)

- How to repeat this success by using prescriptive compliance ?

One example with
ISO/CEI 27001:2005

- 7 management principles to shift from a system protection information to a logic of **information protection**



CONNECTING BUSINESS & TECHNOLOGY

Why getting standardized ? (3/4)

- Common advantages:
 - Cost reduction and and revenue increase
 - Market expansion
 - Innovation
 - Risk Management
 - Trust and recognition
 - Competitive advantage

DEVOTEAM GROUP

CONNECTING BUSINESS & TECHNOLOGY

Why getting standardized ? (4/4)

- Common advantages :
 - Cost reduction and and revenue increase
 - Market expansion
 - Innovation
 - **Risk Management**
 - Trust and recognition
 - Competitive advantage

DEVOTEAM GROUP

CONNECTING BUSINESS & TECHNOLOGY

Risk Management standardization

- 3 key concepts :
 - The Risk
 - The Risk Management
 - The Integrated Risk Management

Common definition of « Risk »

- *« Risk refers to the uncertainty that surrounds future events and outcomes. It is an expression of likelihood and impact of an event that could influence the achievement of organizational goals. »*

■ Source: Conseil du Trésor du Canada (2006)

Normalized definition of « Risk »

- *"potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization."*

- NB: It is measured in terms of a combination of the likelihood of an event and its consequence.

- Source: ISO/IEC 27005:2008

GROUP
DEVOTEAM

CONNECTING BUSINESS & TECHNOLOGY

Information Security Risk

- *« A systematic approach to determine the best course of action under uncertainty by identifying, assessing, understanding, communicating risk issues and taking action against them. »*

GROUP
DEVOTEAM

CONNECTING BUSINESS & TECHNOLOGY

Integrated Risk Management

- « *Integrated risk management is a systematic, proactive and continuous process to understand, manage and communicate risk from the perspective of the entire organization. These are strategic decisions that contribute to achieving the overall objectives of the organization. »*

DEVOTEAM GROUP

CONNECTING BUSINESS & TECHNOLOGY

Integrated Management of IS Risk

- « *Integrated risk management is a **systematic**, proactive and continuous **process** to understand, manage and communicate risk from the perspective of the entire organization. These are strategic decisions that contribute to achieving the overall objectives of the organization. »*

DEVOTEAM GROUP

CONNECTING BUSINESS & TECHNOLOGY

Why complying with an IT Risk Management method ?

- To optimize risk assessment and treatment in terms of:
 - Identification of risks that we must face
 - Evaluation of financial and non financial consequences
 - Response level determination,
 - Major and minor risks distribution
 - Actual security level evaluation
 - Considering measures for elimination, prevention or protection against risks
 - Forming a "survival" plan and major risks arbitration, regarding organization's general objectives
 - Balancing minor risk based on the cost/benefit ratio they represent



CONNECTING BUSINESS & TECHNOLOGY

To get standardized ... or die ?

- Laws and regulations more and more stringent :
 - which weight on IT departments' resources
 - requiring them to constantly adapt
 - which represent a source of costs and problems



CONNECTING BUSINESS & TECHNOLOGY

Standardize ... proactively

- With a standardized framework such as ISO/IEC 27002:2005, to streamline processes and reduce costs.

- Companies strive to develop a proactive compliance benefit on multiple levels :
 - Sustainability
 - Consistency
 - Efficiency
 - Transparency



CONNECTING BUSINESS & TECHNOLOGY

Proactive approach ...

- To control the risk

- To get a true vision and limit operational risk rather than "firefighting" by reacting "case by case ..."



CONNECTING BUSINESS & TECHNOLOGY

... within a common framework

- *A healthy home is built on solid foundations.*
- To achieve a sustainable IT compliance, consistent, efficient and transparent, we must organize and control devices compliance on a common ICT architectural framework.



CONNECTING BUSINESS & TECHNOLOGY

Time to choose

- The company that wants to optimize the implementation of its IT risk management will consider building its risk and compliance management on an ICT standard that allows :
 - To maximize flexibility => Agility
 - To limit the constraints
 - To adopter a common approach
 - To spread up internal best practices
 - To highlight the needs for risk assessment
 - To initiate a certification process



CONNECTING BUSINESS & TECHNOLOGY



ANY QUESTION ?