Best Practices to implement ISMS
The role of Risk Management

Luigi Carrozzi
ISMS Research Group
AIEA - ISACA Milano Chapter

Mission and findings of the Research Group

Mission and activity of ISMS Research Group

- ***To adopt, implement and operate effectively an ISMS*** *manager has to face organizational* ***inner*** *and often* ***hidden barriers***
  The RG gathered in a ***White Paper*** *the experiences 'on the field' from managers (Security, IT, Audit, etc.) who have successfully put in place ISMS in primary organizations developing specific skills and practices on ISMS implementation.*

- *A chapter of the WP is dedicated to present* ***16*** *'on the field'* ***best practices*** *to overcome barriers for a successful implementation of ISMS. Some of these are related to RM*

- *The RG also supported the ISCOM WGs on Critical Infrastructure Protection and will continue operations starting from the WP best practices. A new organizational formula based on 'internal workshops' will be adopted*

RM as a founding practice to set up ISMS

- ***Through Risk Management organizations become aware of:***
  - *how ICT support the **business value chain**;*
  - *the real business **value of information assets**;*
  - *the **risky environment** in which businesses operate;*
  - *the unexpected **source of risk**;*
  - *the current **vulnerabilities**;*
  - *the meaning of **information security requirements**;*
  - *the meaning of **protection measures** and safeguards to be implemented;*
  - *the economic **trade-off** between **security and non-security**;*
  - *the role of top management in **risk-acceptance decisions**;*
  - *the cross organization (reach and range) **impact of action plans**;*

Risk Management enables a deeper understanding of information security issues at all levels and fosters cross-organization cooperation on a continuous base

From 'Our best practices' (*AIEA White Paper on ISMS*)

1 ***Calculate the economic value of information assets***

Calculate the **economic value of information assets**: it enables the decision process on **investment in information security** (cost-benefit analysis based on *Reduced Risk On Investment*)

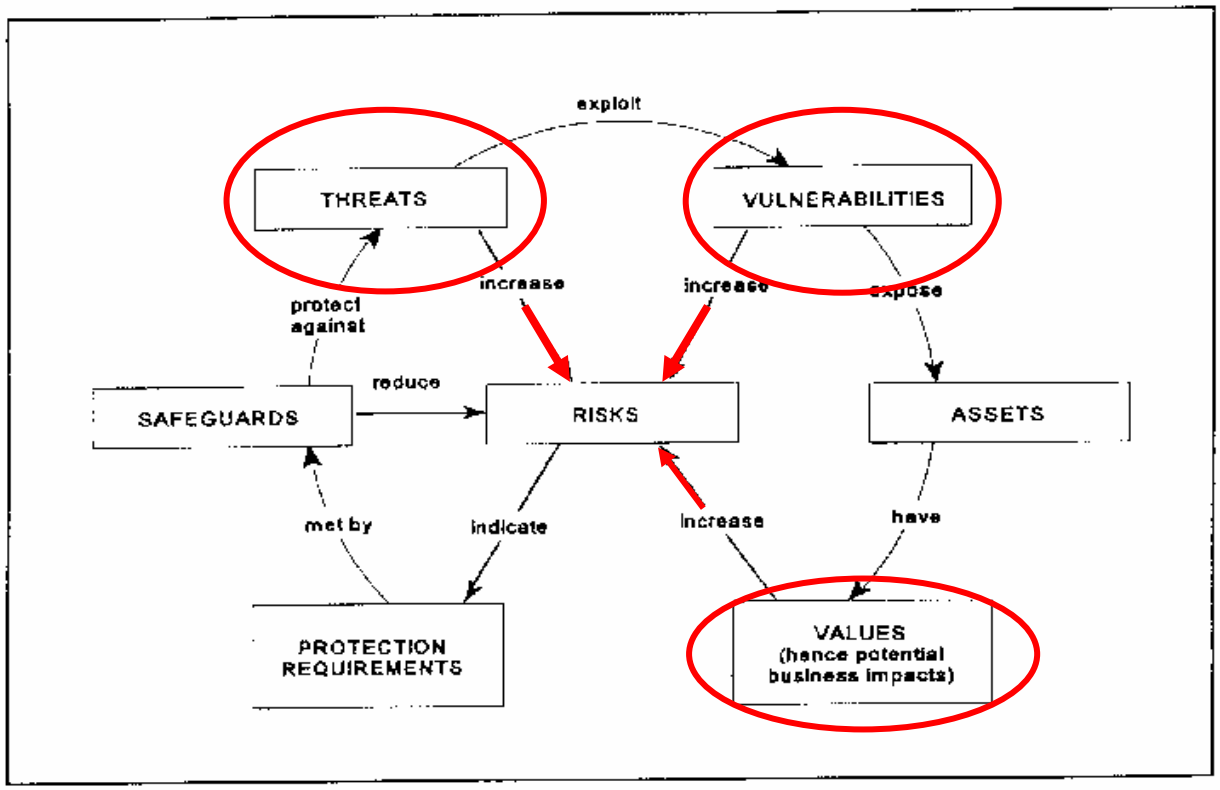
2 ***Adopt perspective Analysis of Risk***

Performing Risk Analysis take into account not only the current scenario but put in place '**perspective', 'forward looking' analysis** to figure out **emerging threats and vulnerabilities**

Next activity on Risk Management

Risk Management Process

ISO/IEC TR 13335-1:1996(E) © ISO/IEC



Relationships in Risk Management

The core components of Risk

Asset Value and Business Impact, Threats, Vulnerabilities ...

- **How do we get this information ?**
- **Who is the owner ?**
- **Do we have the right methodology to gather properly this information inside and outside the organization?**

RM is a 'knowledge intensive-organization wide process' that needs a specific operational method to be implemented

Research objective

Identify a methodology to support knowledge creation in Risk Management process

Requirements

- **Business focus**
- **Make explicit the organization knowledge on asset value, threats, and vulnerabilities.**
- **Target to any form-any type of information and information based assets.**
- **Organization fitting work-method**
- **Organization wide 'reach and range' involvement (top managers, line managers, staff) along different Business Units**

Research tracks/tools

1) Identification of main actors to be involved in RM Knowledge gathering process

2)Identification and 'Test' of specific methods to gather information inside/outside organization and to build up a Corporate Risk Management Knowledge Base such as:

- ***Brainstorming***
- ***Scenario planning***
- ***Delphi method (experts' views)***
- ***Simulations***

3) Draw a guideline for RM operators to make the RM Knowledge gathering a more effective, structured, repeatibile and hence improvable process.