

# An Economic Approach to GRC

Rudy Meert

CRISC CGEIT CISM CISA CISSP

08 June 2011



## Presentation Objectives

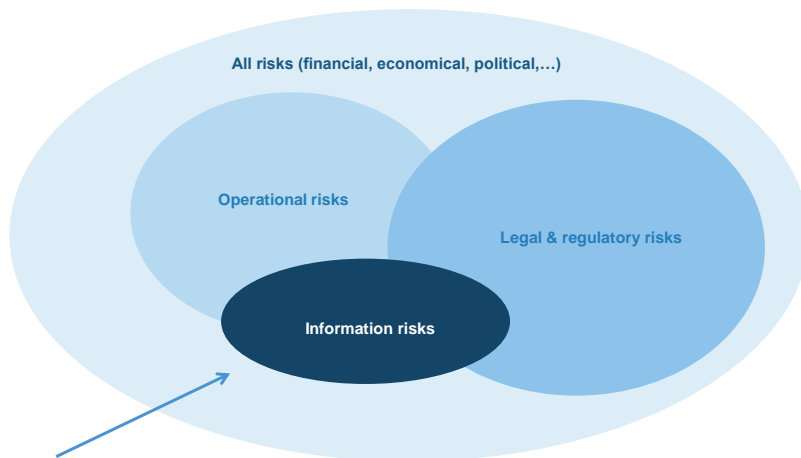


- Share our experience in the area of GRC:
  - Customer assistance in information security management & IT governance
  - Information risk (value) & - compliance assessment → improvement plan
- Show needs & challenges GRC supporting methods & tools
- Present our own developed method
- Show how this method faces the challenges
- Present some lessons learned

Agenda

1. Addressed GRC area
2. Why risk (value) management?
3. Risk management supporting methods & basic needs
4. Challenges for supporting methods
5. The Belgacom-Telindus ISAMM method
6. How does ISAMM face the challenges?
7. Some lessons learned

## 1. Addressed GRC area - risk management



## 1. Addressed GRC area - frameworks



### Control frameworks:

- ISO 27001 (ISMS), 27002, 27005 – information risks
- COBIT - IT governance
- ITIL – IT service management

### Regulatory requirements:

- FDA, PCI, BASEL II

Type here level of Sensitivity "Unrestricted", Internal Use Only" or "Confidential"

June 8, 2011 Slide 5

## 1. Addressed GRC area - IT governance



### *IT processes – **link** to business capabilities*

- *IT control & performance increase → **Risk reduction**, but also*
- ***Value increase**: productivity, quality, efficiency, time to market*

### Basic problem:

- **Most appropriate target level** for control & performance?

→ Let it depend on current **risk (value)** & improvement **contribution**

Type here level of Sensitivity "Unrestricted", Internal Use Only" or "Confidential"

June 8, 2011 Slide 6

## 2. Why risk (value) management?



Perform & target *'without risk (value) assessment'*, experience:

- **Do maximum approach** (target 100% compliancy, maturity level 5)
  - Costly & unrealistic!
- **Benchmarking approach** (e.g. do better as the others)
- **Intuitive approach**, by decision maker:
  - Ineffective & unbalanced!

Is a **requirement** in some international standards:

- E.g. **ISO 27001** → systematic **risk management** as ISMS foundation

Type here level of Sensitivity "Unrestricted", Internal Use Only" or "Confidential"

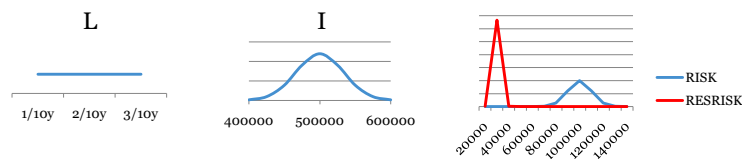
June 8, 2011 Slide 7

## 3. Risk management supporting methods



4 generations, maturity levels:

0. Paper & pencil method – *start from a blank paper*
1. **Scoring** methods – E.g.  $R = L \cdot I / M^2$  ( $L, I, M: 1..5$ ) + thresholds
2. **Qualitative** methods – E.g.  $R = L \cdot I$  (M-related) + risk matrix
3. **Quantitative** methods – E.g. **Risk ALE (in €)**
4. **Probabilistic** methods – Also dealing with **uncertainty**



Type here level of Sensitivity "Unrestricted", Internal Use Only" or "Confidential"

08 June 2011 Slide 8

### 3. Risk management basic needs



Supporting methods & tools should basically assist in:

- Identification of **assets & threats**
- Assessment of threat **likelihood & impact**
- Representation of **current** risks
- Decision support for **risk acceptability**
- Decision support for **risk treatment**
- Graphic supports for **risk communication**

Type here level of Sensitivity "Unrestricted", Internal Use Only" or "Confidential"

June 8, 2011 Slide 9

### 4. Challenges for supporting methods



Experienced problems with some existing methods & tools:

- **Reinventing the wheel** syndrome:
  - *Own set of safeguards & vulnerabilities*
  - **Complexity** (e.g. mapping to ISO 27002 – 27001 SOA)
- **Configuration management** syndrome:
  - *Detailed technical decomposition of IT assets*
  - **Time consuming** & redundant with CM

Type here level of Sensitivity "Unrestricted", Internal Use Only" or "Confidential"

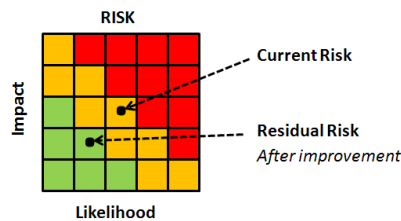
June 8, 2011 Slide 10

## 4. Challenges for supporting methods



Many methods limit to a **qualitative approach** (2<sup>nd</sup> generation):

- **Limited number** of possible risk levels
- **Artificial**, difficult to compare with financial risks
  - *E.g. How to add a number of individual 'qualified' risks in an area?*
- No consideration of **mitigating cost**
- No method for **simulation of residual risk** (what if?)



Type here level of Sensitivity "Unrestricted", Internal Use Only" or "Confidential"

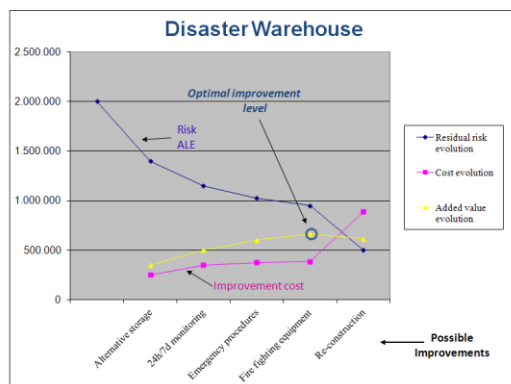
June 8, 2011 Slide 11

## 4. Challenges for supporting methods



We defined some additional requirements for supporting methods:

- **Quantify effectiveness** of potential improvements
- **Realistic** improvement simulation and **residual risk determination**
- **Quantified** approach, **economical justification** & improvement action **challenge**



Type here level of Sensitivity "Unrestricted", Internal Use Only" or "Confidential"

## 5. The ISAMM method



### Information Security Assessment and Monitoring Method

- RM supporting method & tool
- Quantitative method: risk ALE (3<sup>rd</sup> generation)
- Designed to cope with experienced challenges & requirements
- First version in 2003 – currently version 3

Type here level of Sensitivity "Unrestricted", "Internal Use Only" or "Confidential"

June 8, 2011 Slide 13

## 5. The ISAMM method



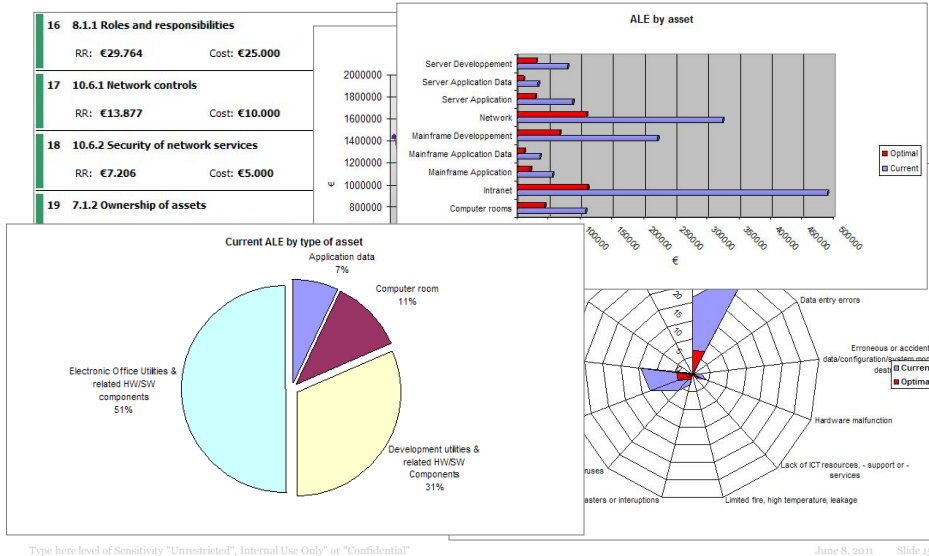
An ISAMM risk assessment contains 4 main phases:

- **Scoping** :
  - Predefined assets, threats, controls:
- **Assessment** of compliance (**vulnerability**) and **threats**
- **Validation** of compliance and threats
- Result – **analysis** and **reporting**

Type here level of Sensitivity "Unrestricted", "Internal Use Only" or "Confidential"

June 8, 2011 Slide 14

## 5. The ISAMM method



## 6. How does ISAMM face the challenges?



Contribution to **'effectiveness & quantification'** requirement:

- **Non-compliance** with ISO 27002 control = **vulnerability**
- **Effectiveness** = **risk decreasing potential** of vulnerability reduction (improvement action)
- Allows ranking of **improvement actions** by effectiveness!
- Also **re-use of experience** - contained in risk reduction capability calculation

## 6. How does ISAMM face the challenges?



Realistic improvement simulation & residual risk determination:

- Select most appropriate improvement action:
  - Calculate residual risk & adapt effectiveness remaining actions!
- Select most appropriate remaining action:
  - ...

## *Realistic simulation!*

Type here level of Sensitivity "Unrestricted", Internal Use Only" or "Confidential"

June 8, 2011 Slide 17

## 6. How does ISAMM face the challenges?



**Economical justification** & support of ISO 27001 **SOA**:

- Direct link between ISO 27002 controls compliance (vulnerability) & risks:
  - **Default criterion** for risk acceptability & justification of controls:
    - **Economic added value of control**
  - **Other** risk acceptance **criteria** possible:
    - E.g. **ALE** (risk) of each asset must be < **€ 30,000**

Type here level of Sensitivity "Unrestricted", Internal Use Only" or "Confidential"

June 8, 2011 Slide 18

## 6. How does ISAMM face the challenges?



Contributes to ‘**efficiency and flexibility**’ requirements:

- No separate safeguards & vulnerabilities, ISAMM derives these from ISO 27002 compliance → **efficiency**
- ‘*Generic infrastructure*’ asset type option → maximal **efficiency high level RA**
- **In-dept ‘asset based’** assessment possible as well → **flexibility**

Type here level of Sensitivity "Unrestricted", Internal Use Only" or "Confidential"

June 8, 2011 Slide 19

## 7. Some lessons learned



- **Organisational** improvements: **difficult** to implement
- Changing **attitude** of management towards **security**
- The importance & value of **GRC awareness & training**
- Added value of **cross-domain approach** for improvements programs
  - E.g. ISMS – FDA compliance assurance: 95% of FDA requirements could be incorporated in the ISMS
- Standard IT frameworks – many **controls are generally applicable**
  - E.g. change management, capacity management, risk management, ...
- Scope – **limit the number of ‘assets’** per individual assessments
  - **Multiplication factors:** assets, threats, vulnerabilities .... !

Type here level of Sensitivity "Unrestricted", Internal Use Only" or "Confidential"

June 8, 2011 Slide 20



Type here level of Sensitivity "Unrestricted", "Internal Use Only" or "Confidential"

June 8, 2011 Slide 21