Models for IT risk mitigation and BCP
Towards Dynamic Risk Management

Emmanuele Zambon, Damiano Bolzoni, Sandro Etalle (University of Twente)
and Marco Salvato (KPMG Italia S.p.a.)
Agenda

- The TD model for mitigation of Availability Risks
- The TDR model for assessing BCPs
- Dynamic Risk Management
Context

- Information IRM and Business Continuity
  - Best practice in most organizations

- Goal
  - Incidents → loss
  - Countermeasures → cost
  - Minimize the cost of Incidents (losses) + Countermeasures

- CIA
  - Confidentiality
  - Integrity
  - Availability
Risk Management Cycle

- Risk
- Likelihood
- Incidents
- System Characterization
- Mitigation (countermeasures)
- Impact
- Budgeting
About Availability

- **Important**
  - E-commerce
  - Web services
  - …

- **Challenging**
  - Temporal dependencies
  - Propagation
  - COBIT or BS2599 do not consider dependencies

3h downtime = 40K EURO losses
The Time Dependency Model & Tool

- IT infrastructure → nodes
- Dependencies → edges
- Incidents
  - Frequency & Repair Time
- Possible Countermeasures
  - Cost & Effects
- Business goals
  - Downtime → Losses
The Time Dependency Model & Tool

- IT infrastructure → nodes
- Dependencies → edges
- Incidents
  - Frequency & Repair Time
- Possible Countermeasures
  - Cost & Effects
- Business goals
  - Downtime → Losses
In Practice

- Most of the data is available after standard COBIT RA or BS 25999 BCP

- Crucial addition: objective
  - Impacts (Business goals)
  - Response to incidents

- Our tool is a plugin of KARISMA
  - Can be a plugin for any COBIT-based RM tool
  - Tested on (some) KPMG data
TOWARDS DYNAMIC RISK MANAGEMENT
Example

- Usually

Emmanuele (IT CEO):
- “look, Pieter”
- “After 3 months of hard work I have developed a fantastic solution for our problem on service X”
- “With 100K$ I can deploy it everywhere”

Pieter (Business CEO):
- “Great job, Emmanuele!”
- “But don’t worry. Service X will be discontinued anyhow”.
Changes in the TD model
Dynamic Risk Management

- Immediate reaction to changes to IT & Business
- Precision by refinement of the assessment

Diagram:
- Risk
- Tool
- Likelihood
- Incidents
- System Characterization
- Mitigation
- Impact
- Budgeting
Conclusions

- **Motto**
  - Free the business from the IT
  - And vice-versa
  - Use a tool

- **Future Work**
  - Further validation of the tool
  - Complexity of the Optimization
  - A model for Availability and Confidentiality
  - Methodology for Dynamic Risk Management