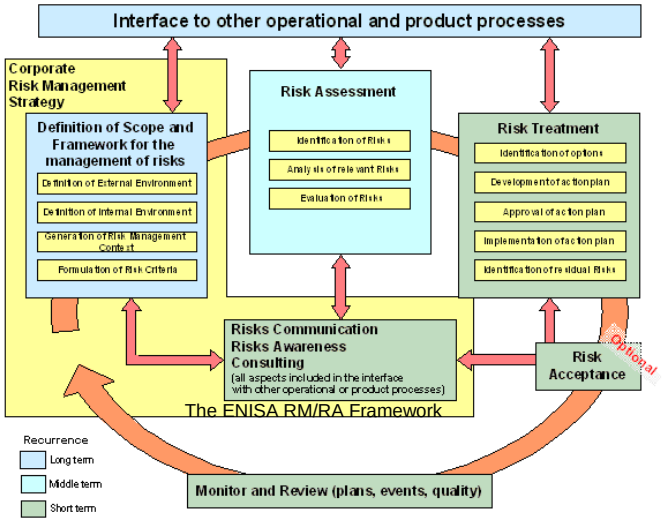
Integration RM/RA with Operational Processes

Risk Management and Risk Assessment are vital processes for the establishment of security in an organization. The effectiveness of the Risk Management process highly depends on the level and quality of its integration with important operational business processes. ENISA presents results achieved in the area of Risk Management integration with business processes as foreseen in the Work Programme 2007.

The Problem

- Corporate IT Risk Management is frequently implemented as an isolated process
- Usually little interaction with operational processes can be stated, i.e. lack of inclusion of operational risks
- As a consequence the isolated corporate IT Risk Management is largely ineffective and fails its objectives
- A negative impact on the security and the overall quality of the business processes is likely, especially regarding:
    - Execution time
    - Reliability
    - Cost efficiency



The Solution

ENISA developed a framework demonstrating the **integration** of IT Risk Management with important operational processes. This material is a good practice for ways to successfully introduce Risk Management in organisations. As basis we took:

- Risk Management process based on the **ENISA Risk Management/Risk Assessment Framework**
- De facto standard **operational processes** such as:
    - IT Service Management based on **ITIL**
    - Application Development based on **RUP**
    - Project Management based on **PRINCE2™**
    - Process Maturity based on **CMMI**

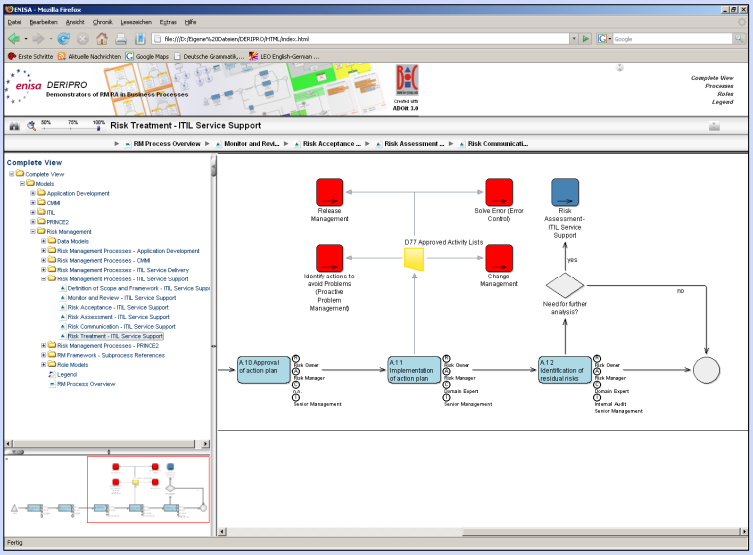
The Integration covers:

- **Interfaces** between IT Risk Management and de facto standard operational processes
- Input/output data and role **mappings at the** level of activities
- Description of **role responsibilities**
- Description of exchanged **information** between the particular activities
- **Guidelines** for dealing with operational risks according to the enterprise-wide risk strategy

The Deliverables

- Highly detailed and comprehensive **graphical models** offering full navigability and showing the interrelations of the processes
- All models are represented through a Tool (**ADOit**® of BOC, www.boc-group.com/ADOit). This offer good navigation and expansion capabilities
- Activities, input/output information flows as well as roles have been included in the models

*The graphical models developed are an ideal basis for **adaptation**, **GAP analysis/compliance**, **refinement**, **training** and **further elaboration**.*

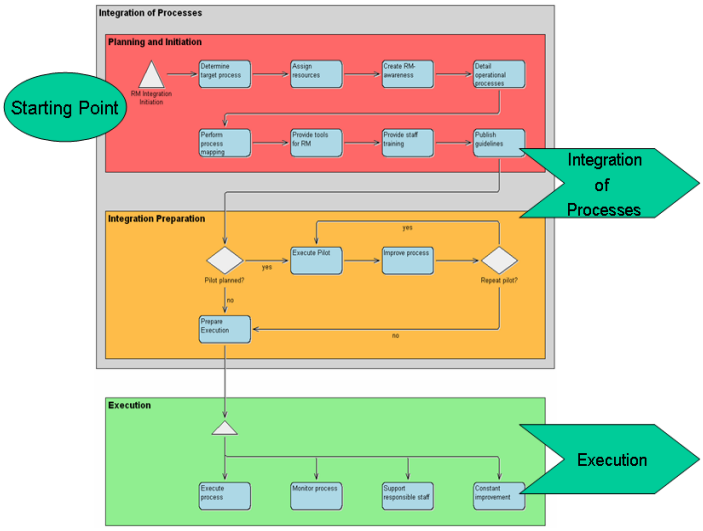


An Exemplary Risk Management Process

The Benefit

Potential users of this material get good practices for:

- **Implementing Risk Management** through a risk management framework
- **Implementing operational processes** through highly detailed reference models (ITIL, CMMI, PRINCE2™, RUP)



The Integration Process

- **Implementation and integration of risk management and operational processes** through documented interfaces, data definitions, data flows as well as data and role mappings
- **Planning and executing the whole integration process** through the included process model

This results in

- A **strong overall guidance** along the whole implementation and integration process
- A **better quality** of global and local risk management as well as operational IT processes
- An **improved line-up** regarding compliance with frameworks which include regulations on corporate risk management (e.g. SOX, Basel II)

Contact Information

ENISA
P.O. Box 1309
71001 Heraklion, Greece
www.enisa.europa.eu/rmra
RiskMngt@enisa.europa.eu