ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

CESIA | CENTRO SERVIZI INFORMATICI DI ATENEO

ANACOM-ENISA on Risk & Innovation

Risk & Innovation in big organisation (public)

Organisational/Technological innovations and their risks

Luisa Consolini
Director, CeSIA – ICT Central Services, University of Bologna

The contest: Bologna University and its ICT services

- UNIBO: one of the largest higher education institutions in Italy
  - 80,000 students, 3,000 tenured academics, 3,000 staff
  - a complex, articulated organization of autonomous structures
    - 70 research departments
    - 23 faculties
    - inter-departmental research centres
    - service centres (ICT, E-learning, Linguistic centres…)
    - libraries, museums
    - a large central administration…
- In the last ten years we have strongly invested in extensive ICT services for students, academics and administrative staff
  - we are seen at the forefront of innovation among Italian universities
  - our users have become used to pervasive on-line services and expect a constant improvement in our services in terms of performance, availability and security

Extensive use of technology brings about higher information security risks

- In the last years some factors have raised the relevance and our sense of urgency of improving our information security processes:
  - a stricter legislation on Privacy (even stricter of the current EC Directive) and Information Security in Italy (due to an anti-terrorism government act)
  - the raising profile of information security threats and the increased frequency of security incidents
  - the intrinsically vulnerable nature of a university ICT infrastructure
    - we are "open" by definition
      - it's very hard to enforce standards (freedom of teaching and research are one of our constitutional principles and tend to reverberate on almost everything)
      - our departments are completely autonomous entities and central ICT is sometimes seen as by them as imposing and beurocratic
      - A strong security culture is not in place and the risk is not perceived as it should
  - the pervasiveness of automation in our front-end services
    - "an on-line university administration"

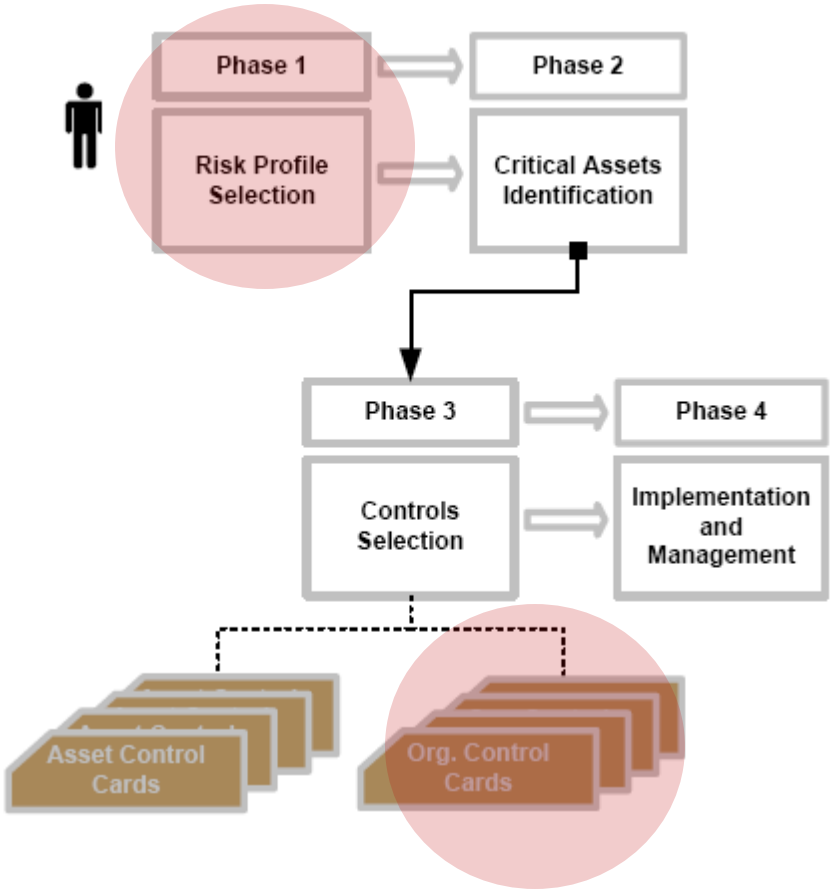
Risk containment: before and after developing a risk management culture

- CeSIA had to reconcile security enforcement with internal "autonomies"
    - our methodology was based upon an assessment of the typical local usage of IT resources such as labs, personal computers and so on. This initial methodology was very simple and IT structure-based
- Our initial approach was ad hoc
    - every organizational unit (departments, faculties etc.) provides different services, and its users have different levels of awareness regarding information security
- We were stuck to a post-incident involvement

At this point we came in contact with ENISA

we found out that ENISA's process-based approach to risk management could overcome the drawbacks we were facing at the time

Piloting ENISA's risk package for SMEs



1. Map decision makers and working staff to our organisation
2. Adapt risk profiles to University Research Depts.
3. Adapt control cards selection

Application of ENISA "Information Package for SMEs" to UniBO Research Departments (1/2)

- **Decision makers and outsourcing**
  - decision making is very diffused in a University
    - Departments' Councils & Directors.
    - Faculty deans
    - opinion leaders
    - "showstoppers"
  - The working staff model is based on partial outsourcing
    - it assumes that the initial risk assessment is provided by CESIA
      - we act as an external consulting service
      - the initial assessment provides knowledge transfer to the dept. personnel
      - the implementation phase is performed by CESIA in collaboration with dept. technicians.

Application of ENISA "Information Package for SMEs" to UniBO Research Departments (2/2)

- **Risk profile selection**
  - **the risk areas in the table of risk profile selection had to be adapted from SMEs to Depts.**
    - **Legal and Regulatory and Reputation and loss of customer confidence are appropriate for a Department**
    - **Financial Stability and Productivity were replaced by:**
      - **Teaching**
        - » **risk is high when the unavailability of ICT services blocks teaching activities and/or when causes the loss of data and information related to examinations or student's careers**
      - **Research**
        - » **Risk is high when the unavailability or the incorrect management of services (f.i. unavailability of labs and devices, breakdown of connectivity) has a direct impact on this strategic activity.**
      - **Patents**
        - » **infringement of patents may cause economic losses or loss of edge on competitiors**

Risk management project structure

Round 1

Assess risks and risk profiles

Deliver a full risk assessment report

Draft a risk management plan

Gain decision makers commitment

Round 2

Implement risk management plan

Bring risk to an acceptable level

The department can now manage its risks

Keep decision makers committed; manage change wrt plan

Round 3

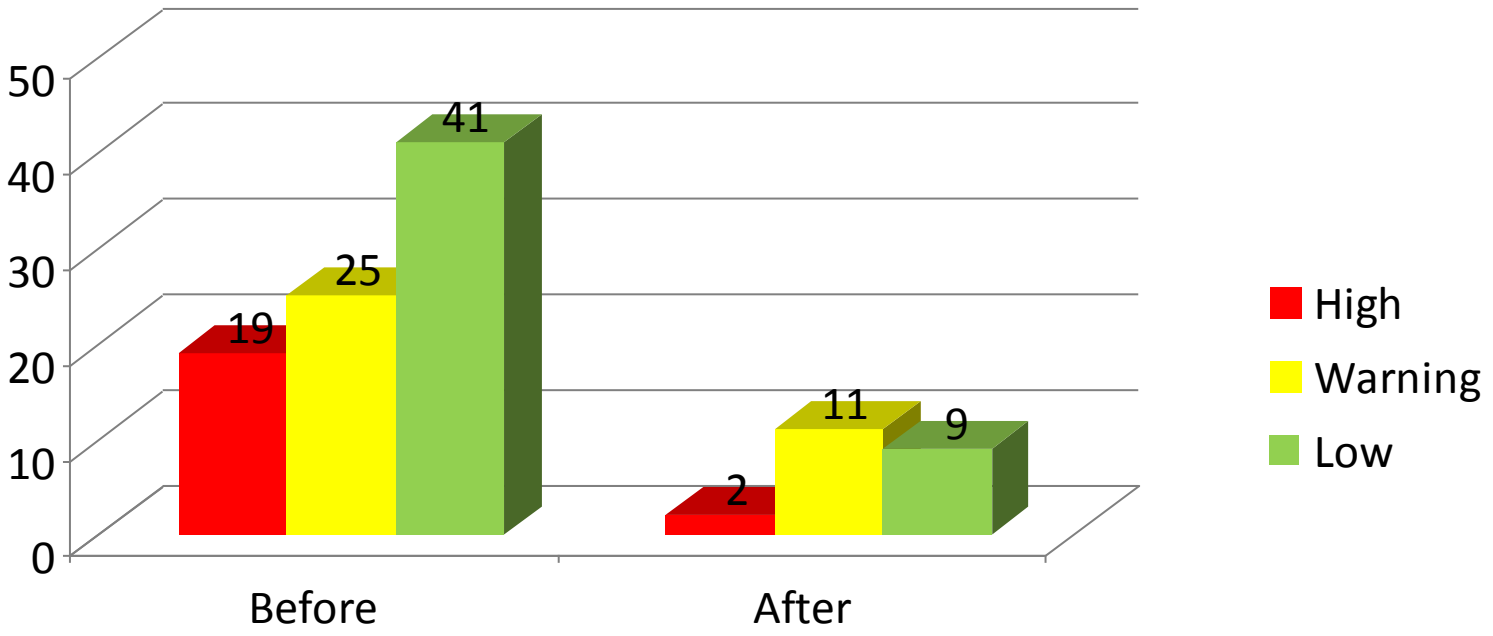
Ongoing monitoring

Regular information security check-ups

Keep decision makers committed

Measure Improvement

Vulnerability pre and post risk management project



ENISA's approach: towards a standard solution

- Thanks to ENISA's methodology "Information Package for SMEs" we adopted a process-based approach and not just an IT based approach
- As a result we achieved:
  - a scalable risk assessment and risk management project structure.
    - In fact we have been able to apply it to 30 department by now
  - an almost infallible way to raise IT security consciousness not only in the technical staff but also in the management and administrative staff
    - this is the main step to get the commitment necessary to manage risk
  - a means to provide stability in terms of IT security, quality and continuity by putting in place a logical reorganization of IT resources and services provided