EUROPEAN DATA
PROTECTION SUPERVISOR

Risk management and data protection

Fidel Santiago
DPO meeting
8 May 2015

This presentation

- Advice on Article 22 of Regulation 45/2001
- Based on good practices in Information Security Risk Management (ISRM)
- Aims to help controllers assume their responsibility and apply accountability

Some definitions

- **Information security:** preservation of confidentiality, integrity and availability of information

- **Risk**: effect of uncertainty on objectives
  - (Note 6) […] the potential that threats will exploit vulnerabilities of an information asset […] and thereby cause harm […]

- **Risk management:** coordinated activities to direct and control an organization with regard to risk

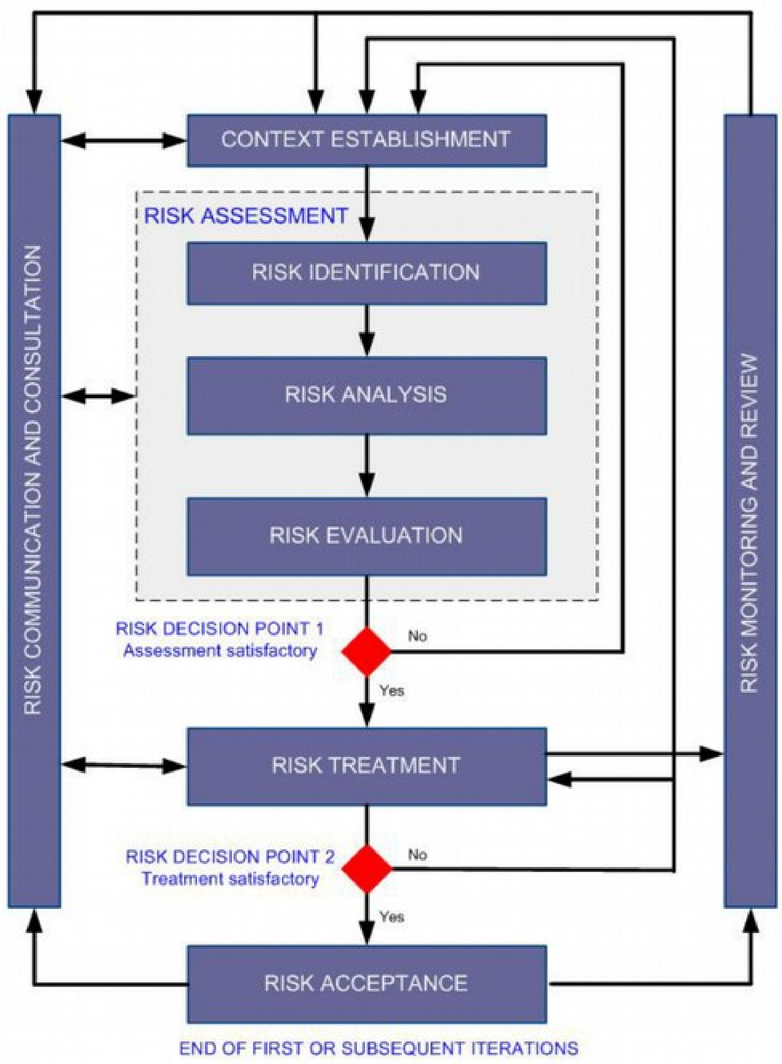
- **Risk management process:** systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk

- *From ISO 27000:2014*

ISRM 101

- ISRM : Information Security Risk Management

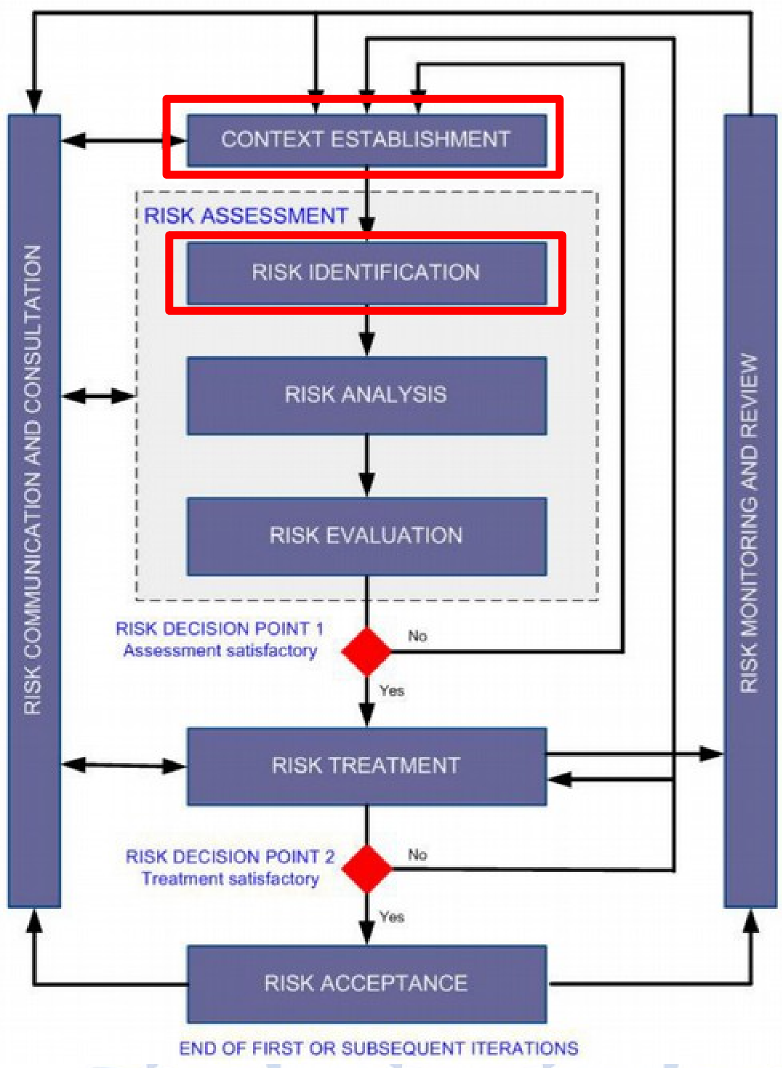
- ISO 27005 (among others…)



ISRM 101: Risk identification

1. Context establishment

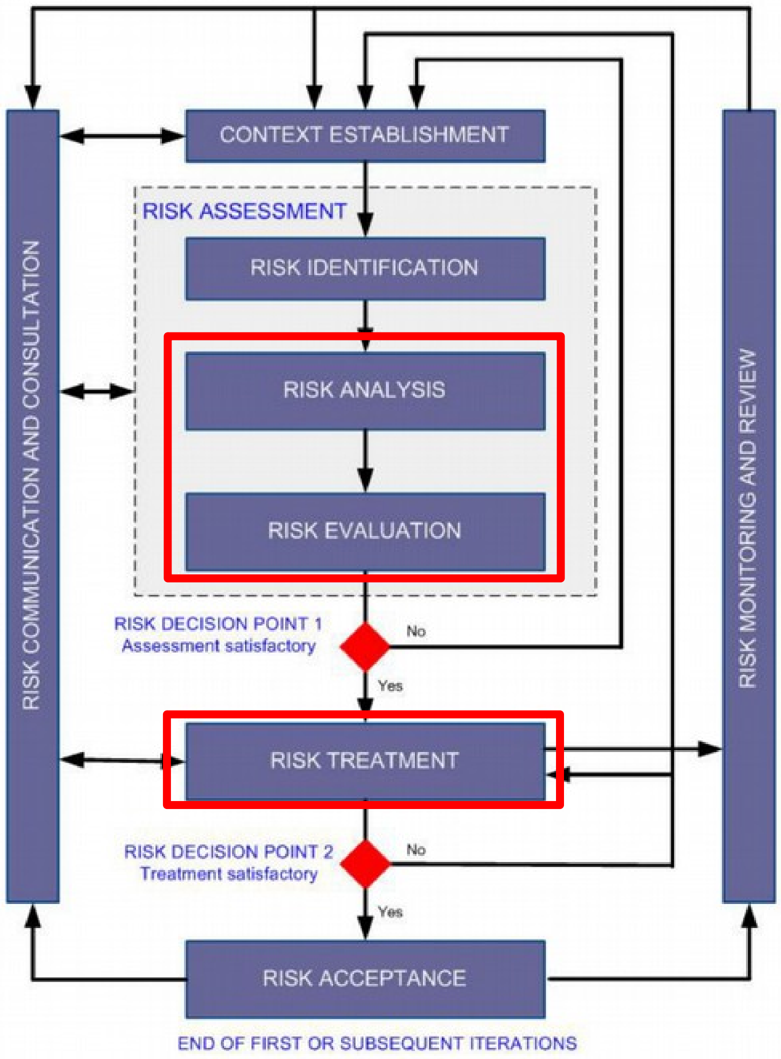
2. Risk identification
   - Assets (p.d. and more…)
   - Vulnerabilities
   - Threats
   - Existing controls
   - Impact



ISRM 101: Risk analysis and treatment

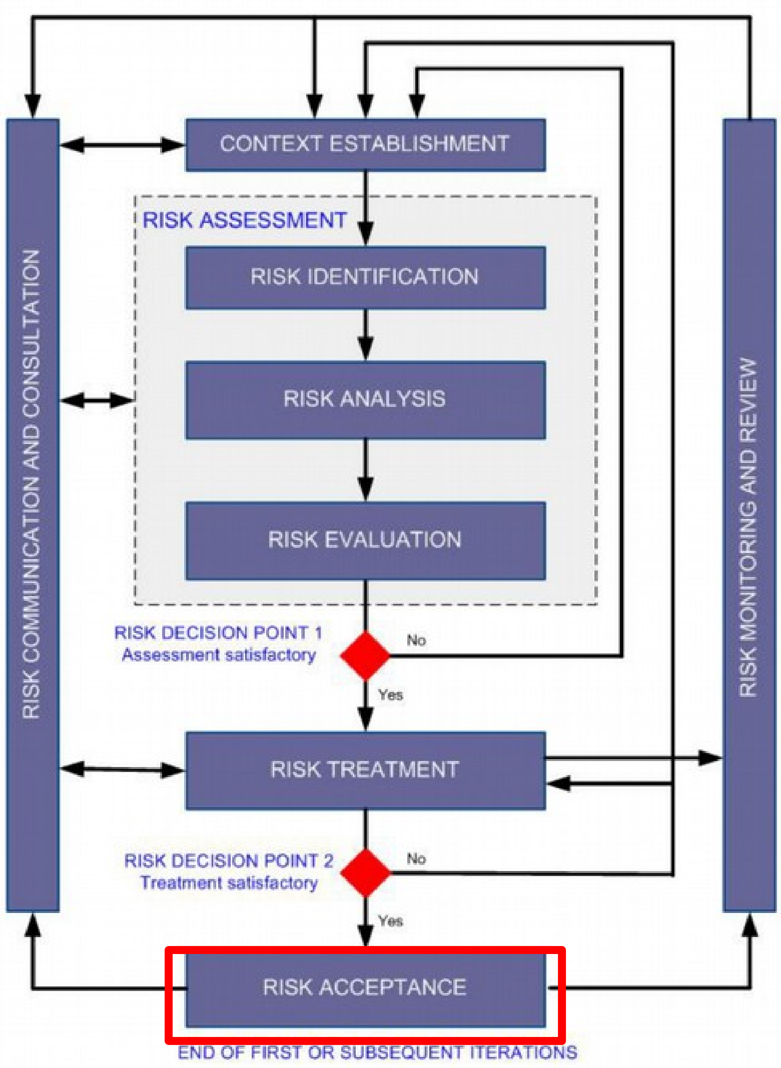
3. Risk analysis
   - Methodology
   - Impact assessment
   - Likelihood assessment
   - Risk

4. Risk treatment
   - Avoid
   - Reduce
   - Transfer
   - Accept



ISRM 101 – Outcomes

- Security plan
- Residual risk
- Monitoring and review



Regulation 45/2001 (I)

- Security of processing (Art. 22.1)
  - “Having regard to the state of the art and the cost of their implementation, **the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected**.”

Regulation 45/2001 (I)

- Security of processing (Art. 22.1)
  - "Having regard to the state of the art and the cost of their implementation, **the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected**."

Regulation 45/2001 (I)

- Security of processing (Art. 22.1)

Risk management: *coordinated activities to direct and control an organization with regard to risk*

Risk management process: *systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk*

protected.”

Regulation 45/2001 (II)

- “Such measures shall be taken in particular to prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other unlawful forms of processing.”

Regulation 45/2001 (II)

– “Such measures shall be taken in particular to prevent any unauthorised disclosure or

Information security: *preservation of confidentiality, integrity and availability of information*

Art. 22.1

- Measures has to be analysed in light of the **risks** to the processing of personal data and the nature of the personal data processed.

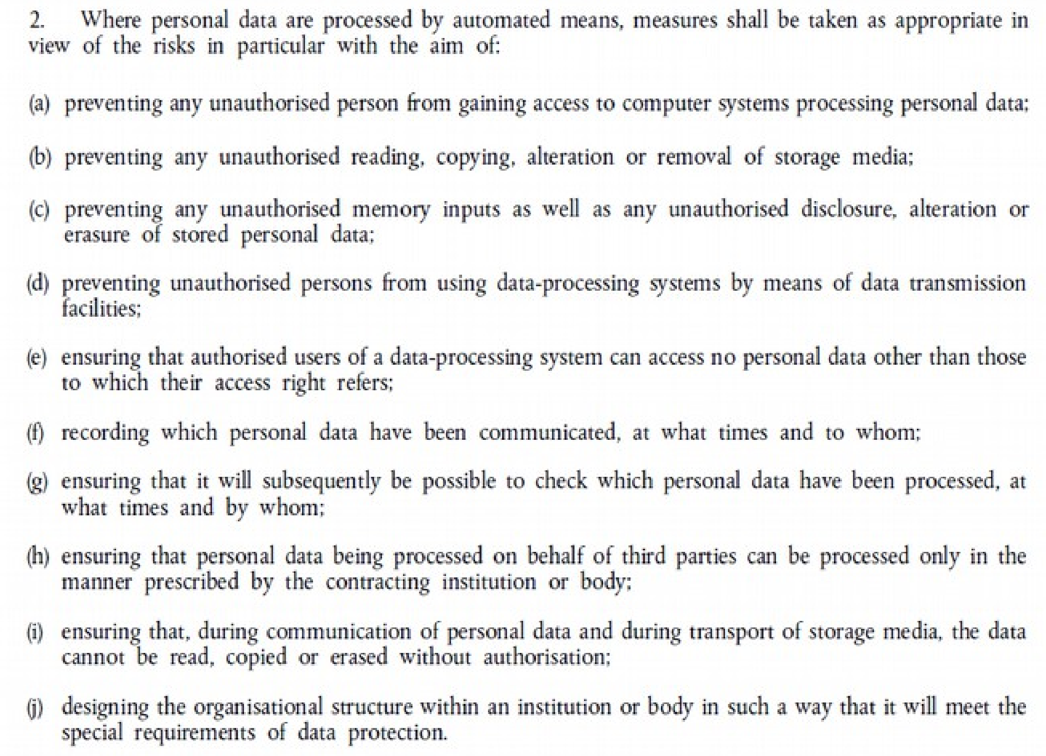
- All processing operations: manual or automated

- All factors that are relevant: systems used, infrastructure, physical security, etc.

- Directive 95/46/EC - Article 17
  - Recital 46: measures have to be taken "*both at the time of the design of the processing system and at the time of the processing itself*".

Security measures

- Article 22.2 – minimum needed but not enough
  - Exceptions ne
- Security meas
  - EC CD 3602,
  - ISO 27002, N Critical Secur Defense…



2. Where personal data are processed by automated means, measures shall be taken as appropriate in view of the risks in particular with the aim of:

(a) preventing any unauthorised person from gaining access to computer systems processing personal data;

(b) preventing any unauthorised reading, copying, alteration or removal of storage media;

(c) preventing any unauthorised memory inputs as well as any unauthorised disclosure, alteration or erasure of stored personal data;

(d) preventing unauthorised persons from using data-processing systems by means of data transmission facilities;

(e) ensuring that authorised users of a data-processing system can access no personal data other than those to which their access right refers;

(f) recording which personal data have been communicated, at what times and to whom;

(g) ensuring that it will subsequently be possible to check which personal data have been processed, at what times and by whom;

(h) ensuring that personal data being processed on behalf of third parties can be processed only in the manner prescribed by the contracting institution or body;

(i) ensuring that, during communication of personal data and during transport of storage media, the data cannot be read, copied or erased without authorisation;

(j) designing the organisational structure within an institution or body in such a way that it will meet the special requirements of data protection.

Accountability

- Management is accountable:
  - Risk management process
  - Risk assessments/treatment
  - The security measures selected and their implementation
  - Residual risks

- Responsibility: many stakeholders!!

Stakeholders

- **Information Security Officer**
- **Data Protection Officer**
- Security Officer
- Documents Manager
- Business process owners
- Process/Project officers
- …

Regular assessment

- Threats, technologies, business processes… evolve constantly
- EU institutions need to review its risk assessment and the selection of security measures regularly
- ㅍISRM a process not a project!!

Implications for EUIs (I)

- Management commitment and decision on the acceptable levels of risks.
- Selecting a ISRM methodology and applying it consistently:
  - (EC) CD 3602 and security standards
  - ISO 27005, BSI standard 100-3, EBIOS, Octave Allegro, NIST SP 800-30…

Implications for EUIs (II)

- Allocating resources to tackle all tasks related to ISRM
- Adequate training and awareness on the ISRM process
- Proper linking of ISRM process to other ones, e.g.:
  - IT/DP governance
  - overall risk management process

Implications for EUIs (III)

- Documenting all key steps of the ISRM process

- Use tools to ease the implementation of all steps of that process
  - *Although not easy to find*

Information Security Management System

- Evolution and maturity

- Information Security Management System: 27001

What about you?

- InfoSec governance/management
- ISRM in your organizations
- ISRM and data processing feasibility

Exists?

Is the DPO/DPC involved?
If not, why?

Recap

- InfoSec & data protection
- InfoSec based on ISRM
- Accountability

Thanks!

www.edps.europa.eu

edps@edps.europa.eu

@EU_EDPS