Information security: DP enabler

Fidel Santiago

DPO meeting

5 November 2015

This workshop

- Security as a fundamental **enabler** for data protection
- Security based on (information security) **risk management**
- The **involvement** of the DPO is of paramount importance

SECURITY → CONTROL

SECURITY → DP

Security as a DP enabler

Security principles

- Confidentiality
- Integrity
- Availability

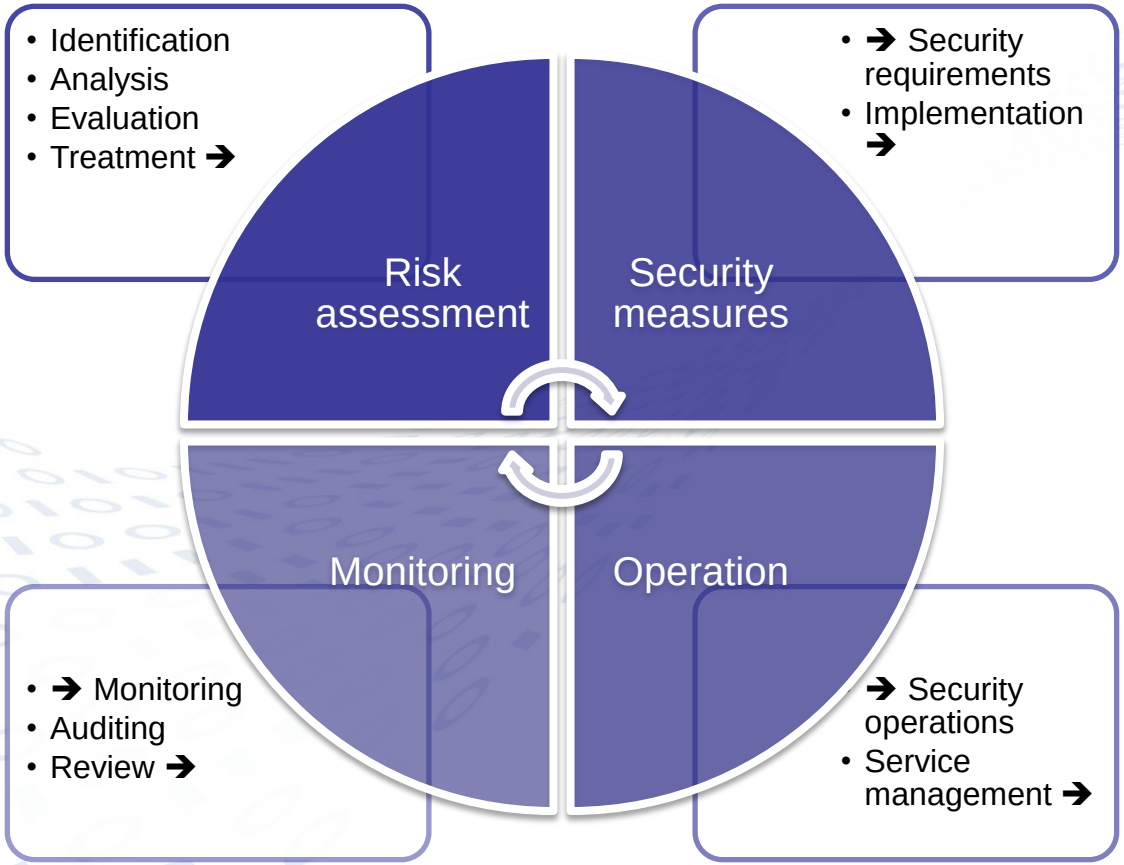
SECURITY ⇒ DP

DP principles

- Fair & lawful
- Purpose limitation
- Accurate and up-to-date
- Conservation periods
- Data subject rights

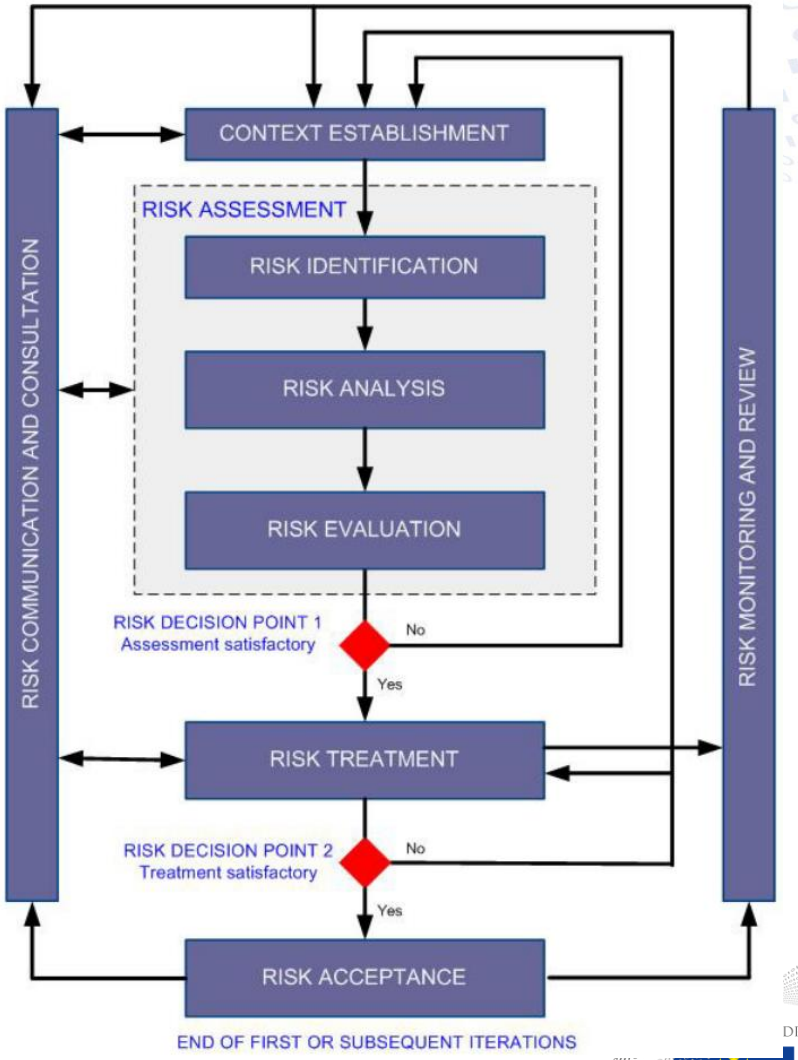
EDPS

Information/IT security



ISRM 101

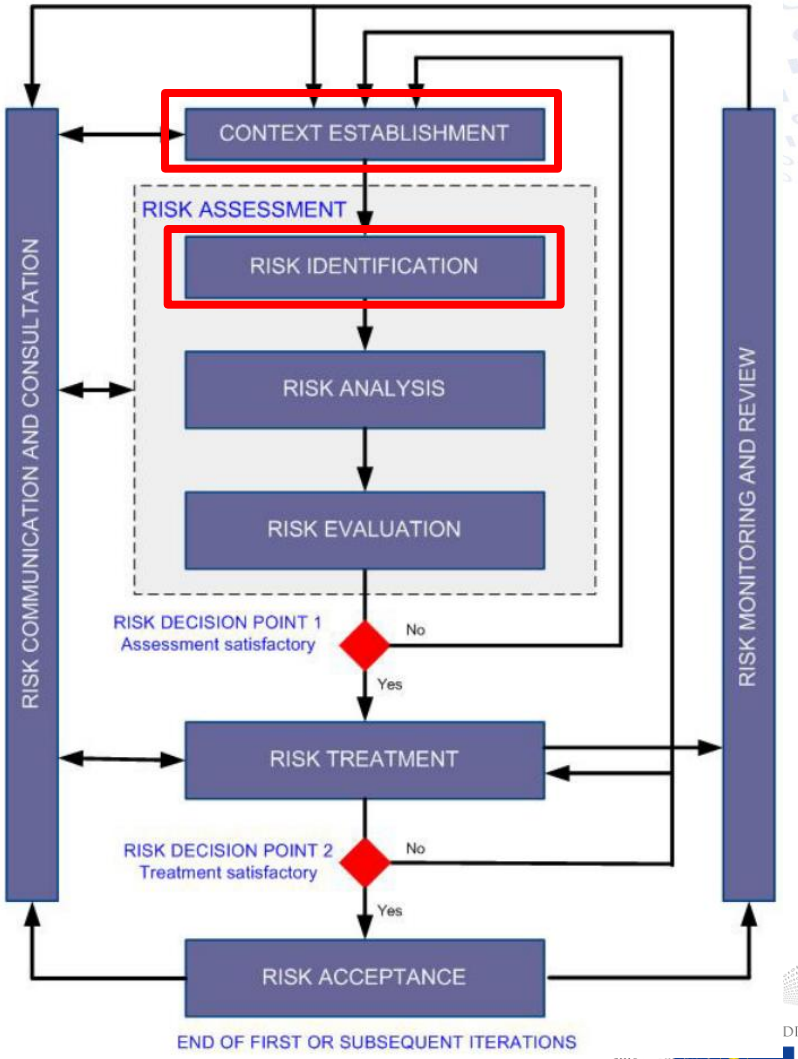
- ISRM : Information Security Risk Management
- ISO 27005 (among others…)



ISRM 101: Risk identification

1. Context establishment

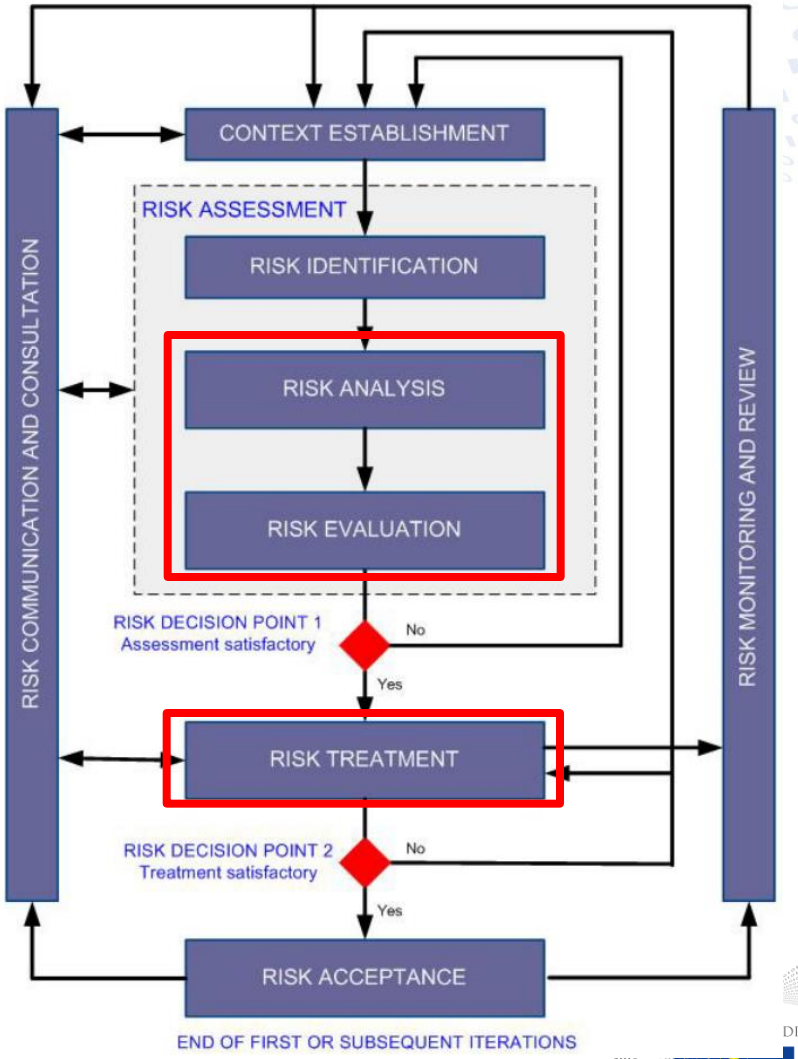
2. Risk identification
   - Assets (p.d. and more…)
   - Vulnerabilities
   - Threats
   - Existing controls
   - Impact



ISRM 101: Analysis & treatment

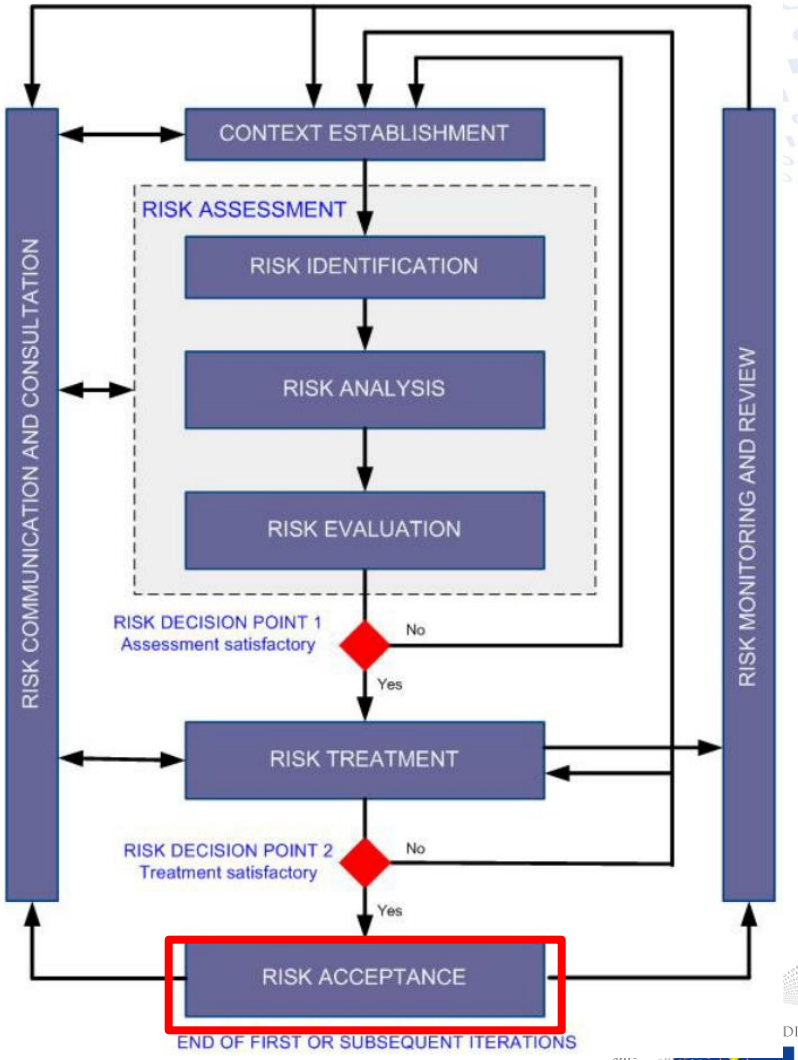
3. Risk analysis
   - Methodology
   - Impact assessment
   - Likelihood assessment
   - Risk

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



ISRM 101 – Outcomes

- Security plan
- Residual risk
- Monitoring and review



Art 22.1. Reg 45/2001 – *Security of processing*

- "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**."

Art 22.1. Reg 45/2001 – *Security of processing*

- "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.**"

Art 22.1. Reg 45/2001 – *Security of processing*

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**

**ISO 27000*

Art 22.1. Reg 45/2001 – *Security of processing*

- “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.”

Art 22.1. Reg 45/2001 – *Security of processing*

– "Such measures shall be taken in particular to

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

**ISO 27000*

"The Data Protection Officer (DPO) is fundamental in **insuring the respect** of data protection principles within institutions/bodies."

- EDPS Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001 (28 November 2005)

Professional Stds. DPO

- 3.5.1. Advice on application of DP provisions:
  - Discusses any legal, **practical or technical** issues having impact on DP;

- Best practices. Involvement in relevant discussion groups: "*For instance, the DPO should be involved in the work of the **security committee**, if existing*"

- Art. 24 Reg 45/2001 - *[…] tasks of the DPO*

Art 24. Reg 45/2001 - *[…] tasks of the DPO*

- "1.*(c)* ***ensuring*** *in an independent manner the internal* ***application of the provisions*** *of this Regulation;"*

- *"[The DPO] shall thus ensure that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations."*

EDPS

How?

- (The DPO) Not alone!!

- With the LISO/SSO/SO…
  - Information Security complex enough → specific professionals!

- **Controller accountable** but DPO also a very important role "*fundamental in **insuring the respect** of data protection*"

Accountability

- (GDPR):
  - measures to be able to **demonstrate** that the processing […] is performed in compliance with this Regulation.
  - mechanisms to **verify** the effectiveness of the measures taken.

- Controller's accountability instruments:
  - Policies
  - Security requirements
  - Data Protection Officer
  - Audits

(Other) Stakeholders

- *Information Security Officer (LSIO/SSO/SO…)*
- *Data Protection Officer*

- Business process owners (controllers)
- Process/Project officers
- Documents Manager
- …

Recap

- InfoSec DP enabler (**control**)
- InfoSec based on **ISRM**
- **Together** (DPO & Sec)!!!!!!

Some Q's for you

- Approach to Art 22. of Reg 45/2001
- Relation with the LISO/SSO/SO…
- Involvement in security governance