ENISA on PIAs

Udo Helmbrecht

Executive Director, ENISA

PIA Symposium

Berlin, 25th November 2011

Agenda

- Overview of ENISA involvement in PIA framework
- Importance and benefits of the PIA process
- Critical success factors for PIAs
- ENISA and RM:
    - Why the focus is on RM
    - Overview of the RM methodology used in ENISA work
    - Examples of ENISA reports where RM has been used
- Next steps for PIAs
- ENISA's prospective role

Overview of ENISA Involvement in the PIA Framework

- ENISA made comments in July 2010 on the draft submitted by the Industry on 30 March 2010.

- Presented initial comments on PIA draft in the Art29WP TS

- The ENISA position was referenced in the Art29WP opinion of July 2010

- Together with the EC facilitated the discussion among stakeholders

- Provided additional comments re the risk management methodology to the industry

Importance / benefits of the PIA process

- **Proactively** identify major impacts and risks of the RFID application with regard to privacy:

  - Privacy & security built-in NOT added-on features

  - Increased efficiency in the development of the application

- **Enhance product marketability and reputation** of the organisations developing the application

- **Minimise challenges** in complying with data protection legislation

Importance / benefits of the PIA process (cont'd)

- **Minimise costs** that would occur from having to apply controls and countermeasures after deployment of the application

- The organisation can gain a **better understanding of its risk environment as regards personal data protection!**

Critical success factors of the PIAs

- Adoption by the industry: companies actually understand and use the framework appropriately

- CAs appropriately assisting the industry in the process

- Framework appropriately binding to existing internal controls and risk management procedures in organisations

Critical success factors of the PIAs (cont'd)

- It's an iterative and dynamic process: it needs to be reviewed and updated!

  - **At the organisation level**: it is not a one-off procedure, it also needs to feed into the RM process

  - **At the EU framework development level**: PIA framework should be evaluated and revisited once enough feedback is collected...
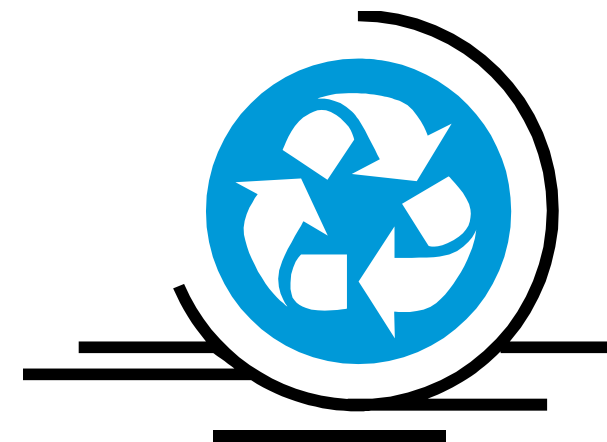
Looking ahead – *next steps re PIAs*

Short term

- Develop sector specific implementation guidelines
- Evaluate the PIAs implementation in MS

Medium / long term

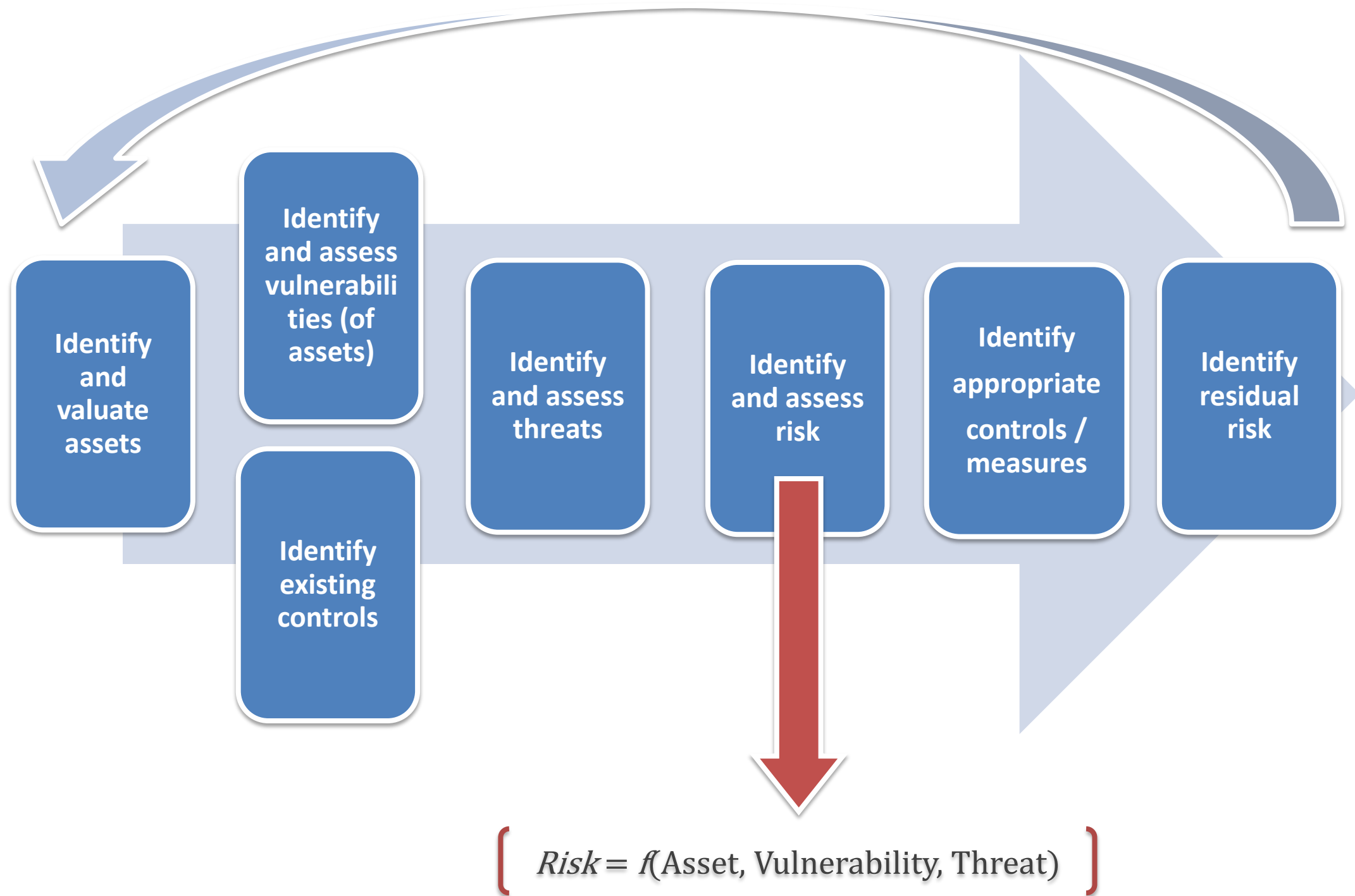- Bring PIAs to the privacy risk management level
- Extend it to more technologies

PROMOTE A EUROPEAN PIA APPROACH!

Why much focus is on risk management

- Allows to think and analyse risks proactively

- Identify risks efficiently and effectively

- Identify and implement measures in proportion to the risks identified

Why much focus is on risk management [cont'd]

- Ability to define different systems of reference and granularity of analysis

- Bind it to the frameworks already in place and in use inside an organization

- Security and privacy risk management working together!

The RM methodology used in ENISA work – *An overview*

Identify and valuate assets

Identify and assess vulnerabilities (of assets)

Identify existing controls

Identify and assess threats

Identify and assess risk

Identify appropriate controls / measures

Identify residual risk

$$Risk = f(\text{Asset, Vulnerability, Threat})$$

Based on ISO/IEC 27005

ENISA's experience with RM methodology

ENISA has published the following technology assessments using RM methodology [indicative list]:

- Cloud computing

- RFID / Internet of Things

- Smartphones

- Life-logging and continuous online activity sharing

- Data mining (on cyber-bullying)

- Remote health monitoring and treatment

ENISA's prospective role

- Assist in the implementation of the PIA framework

- Provide risk management expertise as appropriate, based on our extensive experience on security & technology assessments

- Work with the EC towards developing a European approach on privacy risk management

Contact

European Network and Information Security Agency

Science and Technology Park of Crete

P.O. Box 1309

71001 Heraklion - Crete – Greece

http://www.enisa.europa.eu