Privacy in the workplace conference 2012

Standards in data protection audit

Szádeczky Tamás PhD

TÜVRheinland®

What is TÜV Rheinland?

- Founded in 1872 as DÜV, now 140 years old
- German global company 61 countries, 500 offices
- 13300 employees, 1.1 billion EUR yearly income
- Main profile: Safety and quality testing, audit and certification
- Young business unit in Hungary: information security
  - ISO 27001 certification
  - IT project quality assurance
  - IT security expert services: smart metering, computing cloud
  - Data protection services
    - We need to formalize requirements
    - We love standards

What is technical data protection or data security?

- Technical aspect of personal data protection
- Requirements defined by law
  - Act CXII of 2011 (DP&FOI act in Hungary)
  - Directive 95/46/EC
  - (New directive – detailed rules?)
- Not separable from information security
  - Not only personal data: even business data (plans, contracts, know-hows)
  - Different data set (PD=subset), but similar controls (PDP=subset)

Personal data breaches due technical reasons

- 1984 TRW: 90 million credit data
- 2005 CardSystems, Visa, MC: 40 million credit card data
- 2007 TJX: 94 million credit card data
- 2007 UK Customs Service: personal data of 25 million citizen
- 2011 Cyworld: 35 million user data
- 2011 Sony: 100 million user data

Data security requirements DP&FOI act 7. §

- The **controller must plan and execute control operations** in a way that these ensure the protection of the private sphere throughout the application of the present Act and other regulations applicable in connection with data control.
- The controller, as well as the data processor within their respective scope of activities, is **obliged to ensure data security, institute technical and organizational measures and develop procedural rules** required to enforce the present Act, as well as other data protection and confidentiality rules.
- Through the institution of the appropriate measures the **data must be** particularly **protected from unauthorized access, modification, transfer, disclosure, deletion or destruction**, accidental destruction and **damage** as well as disabled access occurring **due to changes to the technology** applied.

Data security requirements DP&FOI act 7. §

- Data stored in files **cannot be directly connected** and linked to the data subject by **ensuring** the appropriate **technological solutions**.
- During the course of the automated processing of personal data:
  - Prevent unauthorised data entry, log data entry
  - Prevent external attacks
  - Set transfer authentication and log transfers
  - Disaster recovery planning and error reporting needed
- Take care of technical improvement and use best protection **needed** (not the best protection available)

Problem & solution

- Perfunctory regulations are hard to interpret
- No official recommendations or help is available
- Management does not know what to require
- IT staff does not know what to do
- Edge between legislation and actual legal practice
- Have to interpret, give concrete rules
- Thesis:
  - Any legal regulation can be mapped to an IT security standard
  - Reciprocal mapping is possible
  - It can definitely help in interpretation

Problem & solution

- Selected (de facto) standard: COBIT
  - Huge literature
  - Well-known
  - Mapping is worked out (13 volumes)
- Selected act:
  - Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest (general DP&FOI act of Hungary)
- Along unified principles
- Along experience if principles does not work
- This was my PhD thesis
- Review in 2011: Act CXII of 2011 on Informational Self-determination and Freedom of Information (new general DP&FOI act of Hungary)

Mapping to COBIT

- 231 COBIT controls
- 86 section-control mapping
- Least common multiple principle

COBIT 4.1 processes	1	2	3	4	5	6	7	8	9	10	11	12	13
Plan and Organise(PO)													
Acquire and Implement (AI)													
Deliver and Support (DS)													
Monitor and Evaluate (ME)													

Mapping to COBIT

	COBIT control		Requirement of the act
PO4.5	IT Organisational Structure	N	
PO4.6	Establishment of Roles and Responsibilities	P	**24. §** (1) An **internal data protection officer** – with a higher education degree in law, economics, IT or equivalent - under the immediate supervision of the head of the organisation **must be appointed** or designated within the organisation of the controller or data processor a) at the controller and processor controlling or processing national official, labour or criminal files; b) at the financial organisation; c) at the electronic telecommunications and public service corporation.

Mapping to COBIT

	COBIT control		Requirement of the act
DS11.6	Security Requirements for Data Management	F	**7. §** (2) The controller, as well as the data processor within their respective scope of activities, is **obliged to ensure data security, institute technical and organisational measures and develop procedural rules** required to enforce the present Act, as well as other data protection and confidentiality rules.

Mapping to ISO 27001

- COBIT is
  - Mostly used by banks and other financial organizations
  - Not certifiable!
- Change standard to ISO 27001
  - Information Security Management System
  - Well known in most of industries
  - TÜV Rheinland's clients use this
- Easy cross-mapping with
  - COBIT-DP act mapping in my PhD thesis / with review
  - COBIT/ISO 17799 mapping made by ISACA in 2006

Most important requirements

- IT security management
- Oganization, employees
- Roles and responsibilities,
- IT and communication networks, firewalls, segmentation
- Hardening, vulnerability management, change management
- Application and development security
- Authentication and authorisation
- Logging, log analysis, monitoring
- Backups and testing of restore

- All of above based on risk management, adequate solutions
  - See privacy impact analysis (PIA)

Results

- Data protection audit consists of two parts:
  - Legal conformity audit
  - Data security audit
- Data security compliance can be achieved by compliance with IT security standards like COBIT and ISO 27001
- Ability to do integrated audits: DP and ISO 27001 in certain cases
  - Less time on site: cheaper, less redundant

Thank you for your interest!

tamas.szadeczky@hu.tuv.com

TÜVRheinland®

References

- ISACA: COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0 ISBN 1-9332284-78-1
- Jóri A.: Adatvédelmi kézikönyv, Osiris, Budapest, 2005.
- Neszveda, J.: Redundáns struktúrák és a biztonság sérthetetlenség szint kapcsolata ZMNE, Hadmérnök II. évf. 1. szám, 2007, p. 186-196. ISSN 1788-1919
- Szőke, G. L.: Data Protection at organizations' level, Cyberspace 2009, Brno, Czech Republic