

Approaches to Impact Assessment

Roger Clarke

Xamax Consultancy, Canberra

Visiting Professor in Cyberspace Law & Policy, UNSW, Sydney

Visiting Professor in Computer Science, ANU, Canberra

<http://www.rogerclarke.com/SOS/IA-1401> {.html, .pdf}

Impact Assessment Panels

CPDP'14, Brussels – 22 January 2014

Copyright
2013-14



Approaches to Impact Assessment Agenda

1. Assessment Categories
 - Business Case Assessment
 - Risk Assessment
 - Technology Assessment
 - Social Impact Assessment
 - Compliance Assessment
2. Test Application to the EC's 'DPIA' Concept

Assessment Categories

Technology Focus

Compliance Focus

Project or Proposal Focus

Social Impact Focus

Assessment Categories

Technology Focus

- RFID Tags / NFC Chips

Project or Proposal Focus

- T in clothes ...
- T in anklets ...
- T in people ...

Social Impact Focus

- Impacts of the T or the P on some Asset(s) or Value(s)

Compliance Focus

- Consistency of the T or the P with some (quasi-)legal norm

Assessment Categories

Technology Focus

- Technology Assessment

Project or Proposal Focus

- Business Case Formation
- Security Impact, aka
Threat Risk Assessment (TRA)

Social Impact Focus

- Rights IA
- Ethical IA
- Surveillance IA
- Privacy IA
- Data Privacy IA

Compliance Focus

Business Case Methods

	Mainly Quantitative and Financial Data	Mainly Qualitative Data
Mainly the Sponsor's Perspective	<p>Discounted Cash Flow Investment Analysis</p> <p>Financial Sensitivity Analysis</p> <p>Financial Risk Assessment</p>	<p>Internal Cost-Benefit Analysis</p> <p>Risk Assessment</p>
Multiple Stakeholder Perspectives	<p>External or Economic Cost-Benefit Analysis (CBA)</p> <p>Economic Feasibility Assessment</p>	<p>Cost, Benefit and Risk Assessment (COBRA)</p> <p>Economic, Social and Environmental Impact Assessment</p>

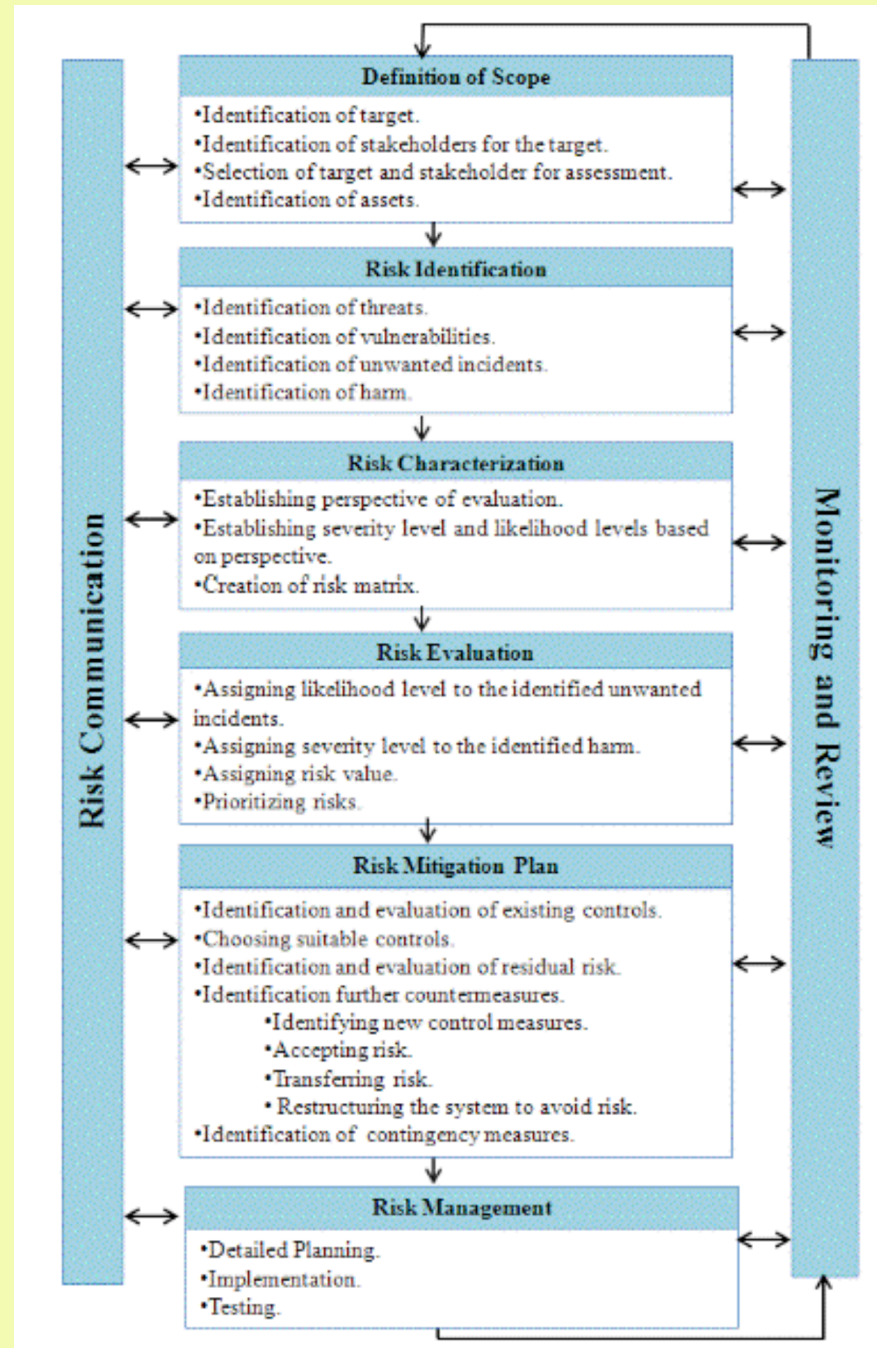
(Threat) Risk Assessment

ISO 2700x
NIST 800-30
BSI 100-x
etc.

Yesudas & Clarke

<http://www.rogerclarke.com/EC/SG-FRA.html>

Copyright
2013-14



Technology Assessment

"A scientific, interactive and communicative process,
which aims to contribute to
the formation of public and political opinion
on societal aspects of science and technology"

European Parliamentary Technology Assessment (EPTA) network

<http://www.eptanetwork.org/>

The Key Scoping Factors:

- The **Technologies** Considered
- The **Perspectives** Reflected
- The **Values** Impinged Upon

Social Impact Assessment

- Rights IA UDHR, ICCPR, ICESCR
- Ethical IA Ethical Issues, Participative Design
- Surveillance IA Many Values & Ind'ls / Groups / Society
- Privacy IA All Dimensions of Privacy
- Data Privacy IA Only the Data Privacy Dimension

The Dimensions of Privacy

- The Physical Person
- Personal Data
- Personal Communications
- Personal Behaviour
- Personal Experience

APF's Meta-Principles for Privacy Protection

1. Evaluation
2. Consultation
3. Transparency
4. Justification
5. Proportionality
6. Mitigation
7. Controls
8. Audit

Assessment Categories

Technology Focus

- Business Case Formation

Project or Proposal Focus

- Security Impact, aka
Threat Risk Assessment (TRA)

Compliance Focus

- Consistency of the T or the P
with some (quasi-)legal norm

Social Impact Focus

- Rights IA
- Ethical IA
- Surveillance IA
- Privacy IA
- Data Privacy IA

Regulatory Forms

Forms: Actors:	Formal Regulation (‘Government’)	Co-Regulation	Industry Self-Regulation	Organisational Self-Regulation (‘Governance’)
The State	Determines What and How	Negotiates What and How	Influences What	Has Limited Influence
Industry Assocn	Influences What and How	Negotiates What and How	Determines What and How	Influences What and How
Corporations	Contribute to Industry Assocn	Contribute to Industry Assocn	Contribute to Industry Assocn	Determine What and How
Other Stakeholders	May or May Not Have Some Influence	May or May Not Have Some Influence	May or May Not Have Some Influence	May or May Not Have Some Influence

Statutes,
Delegated
Legislation

Statutory Codes
& Standards

Industry Codes
& Standards

Customer
Charters

Assessment Categories

Technology Focus

- Business Case Formation

Project or Proposal Focus

- Security Impact, aka
Threat Risk Assessment (TRA)

Social Impact Focus

- Rights IA
- Ethical IA
- Surveillance IA
- Privacy IA
- Data Privacy IA

Compliance Focus

- Regulatory Compliance
 - Org'l Self-Regulation
 - Industry Self-Regulation
 - Co-Regulation
 - Formal Regulation
- Privacy Law Compliance
 - All Statutes, Delegated Legislation, Common Law
- Data Protection Law Compliance
 - An EU Directive, a Statute

Assessment Categories

Technology Focus

- Business Case Formation

Project or Proposal Focus

- Security Impact, aka
Threat Risk Assessment (TRA)

Social Impact Focus

- Rights IA
- Ethical IA
- Surveillance IA
- Privacy IA
- Data Privacy IA

Compliance Focus

- Regulatory Compliance
 - Org'l Self-Regulation
 - Industry Self-Regulation
 - Co-Regulation
 - Formal Regulation
- Privacy Law Compliance
 - All Statutes, Delegated Legislation, Common Law
- Data Protection Law Compliance
 - An EU Directive, a Statute

Organisations are under a legal obligation to do this anyway!

The EC Data Protection Impact Assessment ('DPIA')

- The Trigger (Art. 33.1, 33.2, 33.3):
'risks to the **rights and freedoms** of data subjects' ...



The EC Data Protection Impact Assessment ('DPIA')

- The Trigger (Art. 33.1, 33.2, 33.3): ✓
'risks to the **rights and freedoms** of data subjects' ...
- 'An assessment of the **impact** of the envisaged processing operations **on the protection of personal data**' (33.1). Hence:
 - **not all five dimensions, and not even data privacy**, but merely the sub-set that is subject to data protection
 - **not driven by social values**, but just the minimalist: a mere Data Protection Law Compliance Assessment

The EC Data Protection Impact Assessment ('DPIA')

- The Trigger (Art. 33.1, 33.2, 33.3): ✓
'risks to the **rights and freedoms** of data subjects' ...
- 'An assessment of the **impact** of the envisaged processing operations **on the protection of personal data**' (33.1). Hence:
 - **not all five dimensions, and not even data privacy**, but merely the sub-set that is subject to data protection
 - **not driven by social values**, but just the minimalist: a mere Data Protection Law Compliance Assessment
- Civil society's **views are to be sought, but not reflected** (33.4)
- Wide-ranging **exemption** for government agencies (33.5)
- Uncontrolled Commission power to create **exceptions** (33.6)

Approaches to Impact Assessment Agenda

1. Assessment Categories
 - Business Case Assessment
 - Risk Assessment
 - **Technology Assessment**
 - **Social Impact Assessment**
 - Compliance Assessment
2. Test Application to the EC's 'DPIA' Concept

Approaches to Impact Assessment

Roger Clarke

Xamax Consultancy, Canberra

Visiting Professor in Cyberspace Law & Policy, UNSW, Sydney

Visiting Professor in Computer Science, ANU, Canberra

<http://www.rogerclarke.com/SOS/IA-1401> {.html, .pdf}

Session on Impact Assessments

CPDP'14, Brussels – 22 January 2014