CLOUD ACCOUNTABILITY PROJECT

A Data Protection Impact Assessment Methodology for Cloud

Rehab Alnemr (HP), Erdal Cayirci (UiS), Lorenzo Dalla Corte(TiU), Alexandr Garaga(SAP), Ronald Leenes(TiU), Rodney Mhungu(TiU), Siani Pearson(HP), Chris Reed(QMUL), Anderson Santana de Oliveira (SAP), Dimitra Stefanatou(TiU), Katerina Tetrimida(TiU) and Asma Vranaki(QMUL)

Annual Privacy Forum 2015

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-201(TiU)) under grant agreement no: (TiU)17(QMUL)(QMUL)0 (A(SAP)CLO

CLOUD ACCOUNTABILITY PROJECT

Cloud Accountability Project (A4Cloud)

Framework 7 Integrated Project
A4Cloud "Accountability for Cloud and Other Future Internet Services"

Duration: 42 Months (Oct '12 to Mar '16)
13 Partners - Coordinator & Scientific Lead Hewlett Packard (HP)

Industry

Community

Research

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

Data Protection Impact Assessment

- Accountability mechanism demonstrating awareness about privacy and DP risks
- Need to identify risks to the rights of data subjects concerning their personal data
- Select and document measures to mitigate threats

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-201(TiU)) under grant agreement no: (TiU)17(QMUL)(QMUL)0 (A(SAP)CL

CLOUD ACCOUNTABILITY PROJECT

Why?

- Key topic for data protection governance in Europe
- Increased Data protection requirements on both data controllers and data processors
- Mandatory according to the proposed General Data Protection Regulation (GDPR)
- Pressure to make DPIAs part of overall organizational risk management practices
- Emergence of cloud as the natural choice for most IT departments of very diverse types of organisations
- SMEs need a tool to help them assess risks in regards to data protection

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-201(TiU)) under grant agreement no: (TiU)17(QMUL)(QMUL)0 (A(SAP)CL

CLOUD ACCOUNTABILITY PROJECT

Contributions

Data Protection Privacy Impact Assessment Tool for Cloud

- Comprehensive methodology targeting SMEs and lay users
- Considers up-to-date information sources for privacy and cloud related risks
- DPIA questionnaire follows latest recommendations and standards
- Built on the expertise of a multi-disciplinary team of researchers

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-201(TiU)) under grant agreement no: (TiU)17(QMUL)(QMUL)0 (A(SAP)CL

CLOUD ACCOUNTABILITY PROJECT

Agenda

1. Methodology and principles used to design it
2. Phases and assessment of the results
3. Related work
4. Cloud Adoption Risk Model
5. Tool demo and output report
6. Concluding remarks

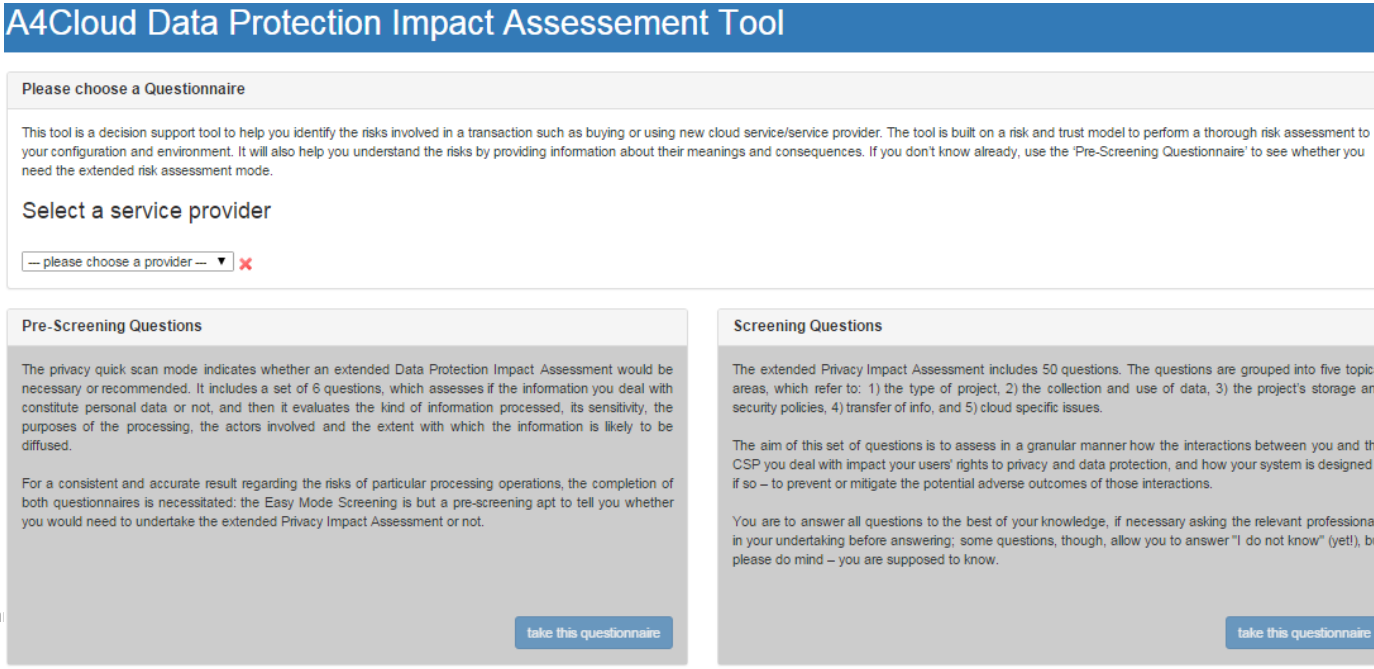
This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-201(TiU)) under grant agreement no: (TiU)17(QMUL)(QMUL)0 (A(SAP)CL

CLOUD ACCOUNTABILITY PROJECT

Methodology and principles

Questionnaire:

- Designed with lay users in mind (SMEs and individuals)
- Multiple sources (regulatory, academic, industry)
- Considers both the risks relating to the DS and the DC's potential compliance issues
- Aims at being future-proof

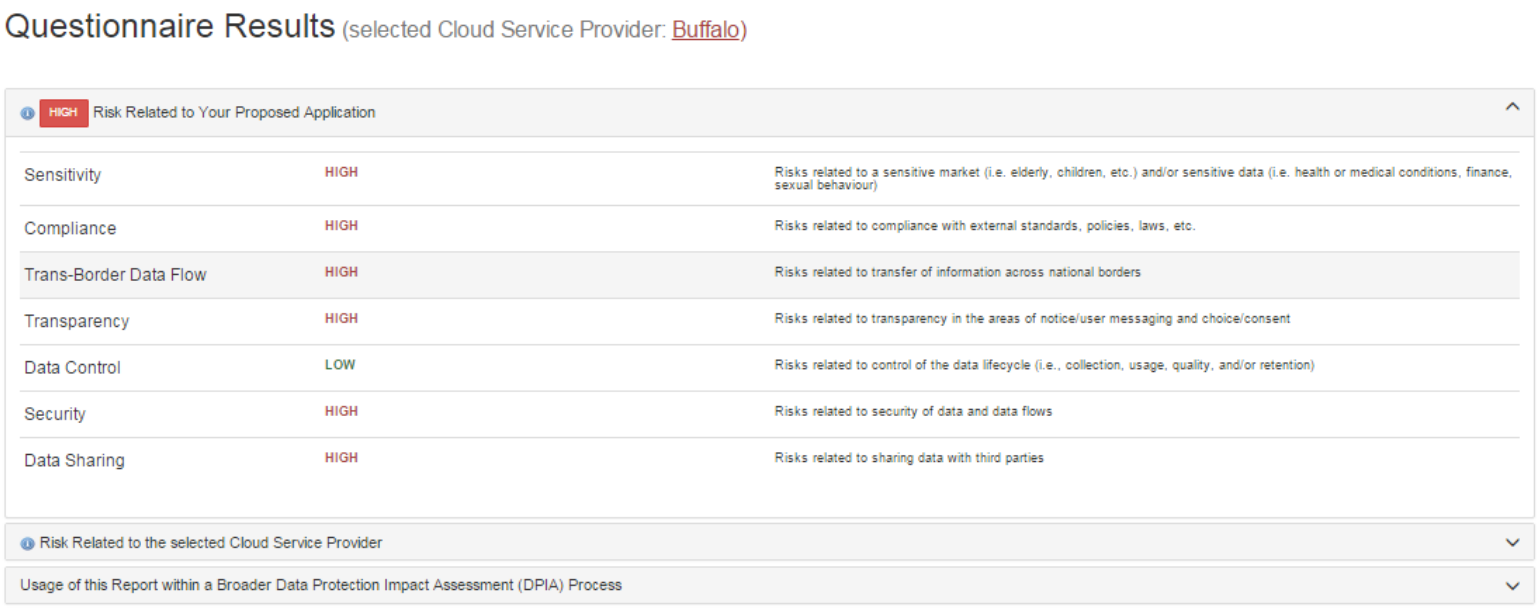


This project is partly funded from the European Com

CLOUD ACCOUNTABILITY PROJECT

Methodology and principles

- Tries to infer potential risks from the user's answers
- 50 questions divided into thematic areas (project type, information collection and use, storage and security, data transfers, cloud-specific issues)
- Different levels of granularity
- Preliminary step meant to introduce a broader PIA/DPIA process



Questionnaire Results (selected Cloud Service Provider: Buffalo)

HIGH Risk Related to Your Proposed Application

Sensitivity	HIGH	Risks related to a sensitive market (i.e. elderly, children, etc.) and/or sensitive data (i.e. health or medical conditions, finance, sexual behaviour)
Compliance	HIGH	Risks related to compliance with external standards, policies, laws, etc.
Trans-Border Data Flow	HIGH	Risks related to transfer of information across national borders
Transparency	HIGH	Risks related to transparency in the areas of notice/user messaging and choice/consent
Data Control	LOW	Risks related to control of the data lifecycle (i.e., collection, usage, quality, and/or retention)
Security	HIGH	Risks related to security of data and data flows
Data Sharing	HIGH	Risks related to sharing data with third parties

Risk Related to the selected Cloud Service Provider

Usage of this Report within a Broader Data Protection Impact Assessment (DPIA) Process

This project is partly funded fro

CLOUD ACCOUNTABILITY PROJECT

Related work

- launched a PIA process and handbook

Guidelines on Security and Privacy in Public Cloud Computing

- Guidelines Concerning the Protection of Privacy and Transborder Flows of Person-al Data

- guides and recommendations

- Cloud Computing - Benefits, risks and recommendations for information security

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-201(TiU)) under grant agreement no: (TiU)17(QMUL)(QMUL)0 (A(SAP)CL

CLOUD ACCOUNTABILITY PROJECT

Related Work – tools

- E-learning tool for government employees in Canada
- US DHS - Privacy Threshold Analysis tool
- Prototype decision support tool developed by the PRAIS project
- HP Privacy Advisor (HP PA)
- Avepoint Privacy Impact Assessment System
- TRUSTe Assessment Manager

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-201(TiU)) under grant agreement no: (TiU)17(QMUL)(QMUL)0 (A(SAP)CL

CLOUD ACCOUNTABILITY PROJECT

DPIAT

GDPR Alignment identifying to what extent the customer complies with the GDPR

Guidance educating the users about relevant risks

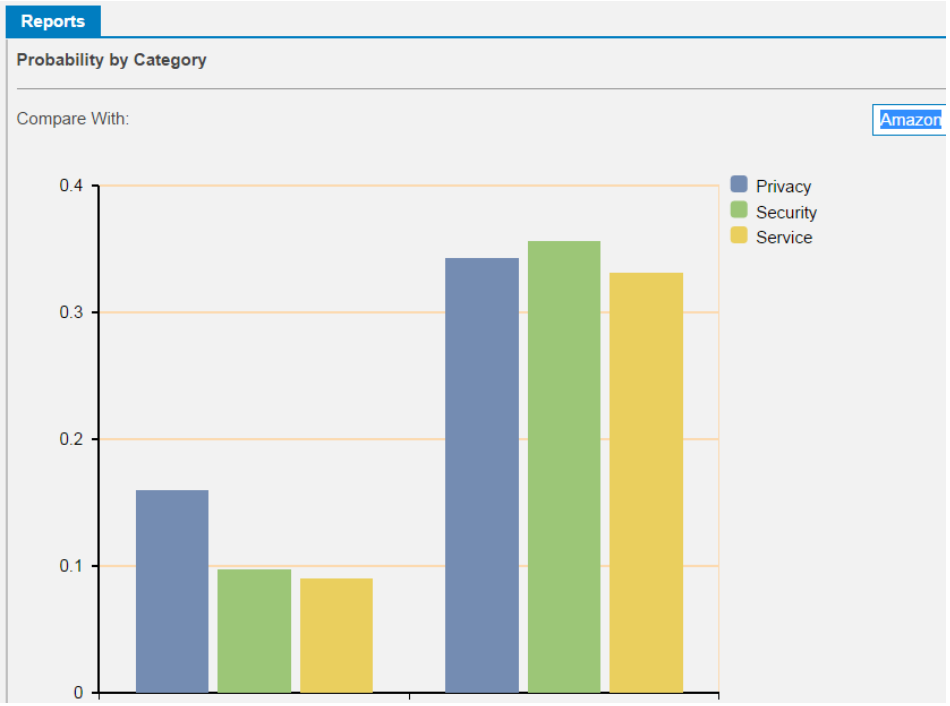
Risk Management reducing the risks of selecting a service provider

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-201(TiU)) under grant agreement no: (TiU)17(QMUL)(QMUL)0 (A(SAP)CL

CLOUD ACCOUNTABILITY PROJECT

Cloud Adoption Risk Assessment Model (CARAM)

- A guidance for cloud customers in assessing risks
- An algorithm to classify CSPs according to their security management practices
- A model to compute risk values
- A decision approach for articulating CSC preferences with relative risk analysis



This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-201(TiU)) under grant agreement no: (TiU)17(QMUL)(QMUL)0 (A(SAP)CL

CLOUD
ACCOUNTABILITY
PROJECT

Demo

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-201(TiU)) under grant agreement no: (TiU)17(QMUL)(QMUL)0 (A(SAP)CLO

CLOUD ACCOUNTABILITY PROJECT

Conclusions

- DPIAT is based on existing PIAs, legal sources and specific cloud risk scenarios
- Aims at SMEs and users with limited data protection knowledge
- Structures data protection issues and risks in an understandable way
- Presents likelihood and impact as to help the target audience to improve legal compliance
- Next steps: run additional pilots to improve the tool

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-201(TiU)) under grant agreement no: (TiU)17(QMUL)(QMUL)0 (A(SAP)CL