



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 (FP7/2007-2013) under grant agreement no: (TIU)17(QMUL)(QMUL)0 (A(SAP)CLO



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



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

- 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

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

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

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

A4Cloud Data Protection Impact Assessment Tool

Please choose a Questionnaire

This tool is a decision support tool to help you identify the risks involved in a transaction such as buying or using new cloud service/service provider. The tool is built on a risk and trust model to perform a thorough risk assessment to your configuration and environment. It will also help you understand the risks by providing information about their meanings and consequences. If you don't know already, use the 'Pre-Screening Questionnaire' to see whether you need the extended risk assessment mode.

Select a service provider

--- please choose a provider --- ✖

Pre-Screening Questions

The privacy quick scan mode indicates whether an extended Data Protection Impact Assessment would be necessary or recommended. It includes a set of 6 questions, which assesses if the information you deal with constitute personal data or not, and then it evaluates the kind of information processed, its sensitivity, the purposes of the processing, the actors involved and the extent with which the information is likely to be diffused.

For a consistent and accurate result regarding the risks of particular processing operations, the completion of both questionnaires is necessitated: the Easy Mode Screening is but a pre-screening apt to tell you whether you would need to undertake the extended Privacy Impact Assessment or not.

[take this questionnaire](#)

Screening Questions

The extended Privacy Impact Assessment includes 50 questions. The questions are grouped into five topic areas, which refer to: 1) the type of project, 2) the collection and use of data, 3) the project's storage and security policies, 4) transfer of info, and 5) cloud specific issues.

The aim of this set of questions is to assess in a granular manner how the interactions between you and the CSP you deal with impact your users' rights to privacy and data protection, and how your system is designed if so – to prevent or mitigate the potential adverse outcomes of those interactions.

You are to answer all questions to the best of your knowledge, if necessary asking the relevant professional in your undertaking before answering; some questions, though, allow you to answer "I do not know" (yet!), but please do mind – you are supposed to know.

[take this questionnaire](#)

- 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		

-  **ico.** launched a PIA process and handbook
Information Commissioner's Office



Guidelines on Security and Privacy in Public Cloud Computing

-  **OECD** Guidelines Concerning the Protection of Privacy and Transborder Flows of Personal Data

-  **CNIL** guides and recommendations
Commission Nationale de l'Informatique et des Libertés



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

- 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

GDPR Alignment

identifying to what extent the customer complies with the GDPR

Guidance

educating the users about relevant risks

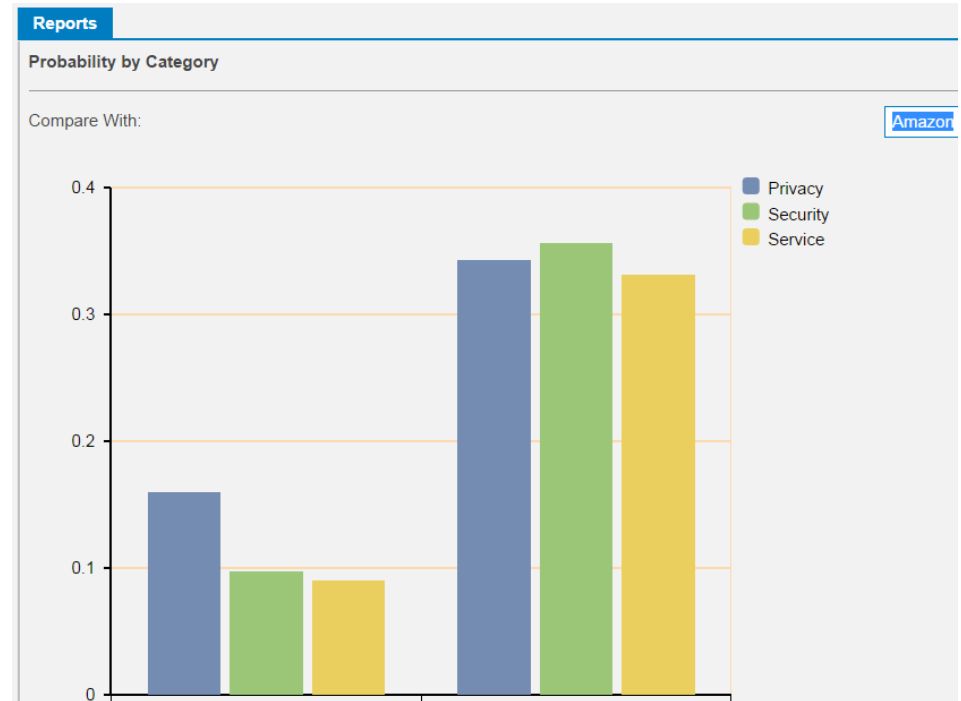


Risk Management

reducing the risks of selecting a service provider

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





CLOUD
ACCOUNTABILITY
PROJECT

Demo



- 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