InterPARES Trust

Study Name:		Ensuring Trust in Storage for Infrastructure-as-a-Service
Team & Study Number:		EU08
Research domain:		Infrastructure
Document Title:		Checklist
Status:		Final
Version:		v1.2
Date submitted:		2016/07/27
Last reviewed:		2016/08/03
Author:		InterPARES Trust
Writer(s):		Hrvoje Stancic, Faculty of Humanities and Social Sciences, University of Zagreb Edvin Bursic, Financial Agency (FINA) and GRA, Faculty of Humanities and Social Sciences, University of Zagreb Adam Al-Hariri, GRA, Faculty of Humanities and Social Sciences, University of Zagreb
Editor:		Corinne Rogers

Document Control

Version history			
Version	Date	By	Version notes
v 1.1	2016/07/27	Corinne Rogers	Adapted from EU08 Final Report
v 1.2	2016/08/03	Hrvoje Stancic	Minor improvements and edits

Checklist for Storage in IaaS

This Checklist is designed to offer guidance for individuals, businesses, government agencies or other organizations to assess the security and ongoing trustworthiness (i.e. authenticity, reliability, and accuracy) of their data when stored in an Infrastructure-as-a-Service (IaaS) platform. It is the result of a study in the international InterPARES Trust Research Project (https://interparestrust.org), Ensuring Trust in Storage in Infrastructure-as-a-Service (EU08). The goal of the study was to establish the minimum amount of information necessary to support users' trust in an IaaS provider and also position the provider as a trusted service provider.

In InterPARES Trust's terminology database the term "trust" is defined as "confidence of one party in another, based on alignment of value systems with respect to specific actions or benefits, and involving a relationship of voluntary vulnerability, dependence and reliance, based on risk assessment".[1] This means that the users of cloud services should have enough information on a particular service (e.g. in Terms of Service) in order to trust it, or the service level agreement (SLA) between users and cloud service provider (CSP) should equally protect interests of both parties involved.

To better understand the implication of issues of trust in cloud services the research team created a questionnaire. The Checklist is based on that questionnaire, which was used during the collection of data for analysis of the Croatian cloud service providers offering Infrastructure-as-a-Service (IaaS). The checklist consists of 36 questions divided into 10 categories:

1. General information (4 questions),
2. Governance (4 questions),
3. Compliance (4 questions),
4. Trust (5 questions),
5. Architecture (6 question),
6. Identity and Access Management (1 question),
7. Software Isolation (2 questions),
8. Data Protection (5 questions),
9. Availability (2 questions),
10. Incident Response (3 questions).

This checklist can be used by records managers and archivists when assessing a CSP offering IaaS as well as by CSPs as a guideline for providing online information about their service. The full report from this study can be found at https://interparestrust.org/assets/public/dissemination/EU08_20160727_EnsuringTrustStorageIaaS_FinalReport_Final.pdf.

[1] *InterPARES Trust: Trust and Digital Records in an Increasingly Networked Society*, http://interparestrust.org.

IaaS Checklist

	Question	Y*	N	?**	Answer / additional info***
1. General information					
1.	Which components are used in IaaS?				
2.	What types of services are offered in IaaS?				
3.	What technologies are being used?				
4.	What implications used technologies have on security and privacy of the system?				
2. Governance					
5.	Is it possible for a client to monitor security of computing environment and data security? How?				
6.	What kind of security assures a client that his data is not mixed with another's?				
7.	What kind of security assures a client that there is no data shared with employees of different rank or/and not created by others?				
8.	What audit mechanisms and tools are used to determine how data is stored, protected and used to validate services, and to verify policy enforcement?				
3. Compliance					
9.	Does the service comply with other countries' laws, regulations, standards and specifications for clients outside the country of service?				
10.	How is the service secured against unauthorized access, use, disclosure, disruption, modification, or destruction of data?				
11.	What technical and physical safeguards does the service assure?				

* The questions which are not simple "Yes/No" questions, i.e. require elaborated answer, have the "Y / N / ?" fields shaded.

** The "?" column indicates a situation where no information is available or the question is not applicable to your situation.

*** The "Answer / additional info" column can be used in situations where either a question is not a "Yes/No" type of question or a simple "Yes/No" answer can be supplemented with useful information.

12.	Does the service use subcontractors for any part of the used technology or offered service?				
4. Trust					
13.	Is the service secured from denial of service attack?				
14.	Does the service secure ownership rights over data?				
15.	Does the service have any certificate relevant to the service?				
16.	What kind of risk management does the organization provide?				
17.	What kind of physical and logical security is assured for the virtual servers and applications?				
5. Architecture					
18.	How is a hypervisor or virtual machine monitor secured?				
19.	How does the service secure virtual machine images from attack looking for proprietary code and data?				
20.	Does the service use image management process to govern the creation, storage, and use of virtual machine images or containers?				
21.	How does the service secure from attacks on the client side?				
22.	How does the service secure from attacks on the server side?				
23.	Is the service using encrypted network exchange?				
6. Identity and Access Management					
24.	How does the service protect ancillary data: - details about the consumers' accounts, - data about customer-related activity, - data collected to meter and charge for consumption of resources, - logs and audit trails, and other such metadata that are generated and accumulated within the environment, - data of an organization’s initiative (e.g., the activity level or projected growth of a startup company), - metadata collected by the provider?				

7. Software Isolation					
25.	How does the service prevent man-in-the-middle attacks?				
26.	Is the service secured from attacks on the server that target passwords?				
8. Data Protection					
27.	What kind of encryption does the service use to secure data stored in IaaS?				
28.	Have the service conducted deliberate attacks in order to test the system's protection?				
29.	What procedures are used for data sanitization upon termination of service, i.e. how does the service ensure that the data after deletion are not recoverable?				
30.	Where, geographically, are the data stored?				
31.	Where, geographically, is data backup stored?				
9. Availability					
32.	In a situation of a lawful raid how is the service availability assured to the users not being lawfully raided?				
33.	Is there a policy regarding user data availability in case of a bankruptcy or other facility loss and how is it defined?				
10. Incident Response					
34.	Is there an incident response plan and how is it defined?				
35.	Does the service keep track of the data using which the scope of the incident, and assets affected can be determined?				
36.	Does the service keep a forensic copy of incident data for legal proceedings or as needed by the consumer? Or, does the service give incident data to the consumers?				