SINTEF

A27131- Unrestricted

Report

Cloud Security Requirements

A checklist with security and privacy requirements for public cloud services

Author(s)
Karin Bernsmed
Per Håkon Meland
Martin Gilje Jaatun

SINTEF ICT
Software Engineering, Safety and Security
2015-08-25

SINTEF IKT
SINTEF ICT

Address:
Postboks 4760 Sluppen
NO-7465 Trondheim
NORWAY

Telephone:+47
Telefax:+47 73594302

Enterprise /VAT No:
NO 948 007 029 MVA

KEYWORDS:
Cloud computing
Security
Privacy

Report

Cloud Security Requirements

A checklist with security and privacy requirements for public cloud services

VERSION
2.0

DATE
2015-08-25

AUTHOR(S)
Karin Bernsmed
Per Håkon Meland
Martin Gilje Jaatun

PROJECT NO.
102002334

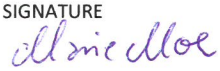
NUMBER OF PAGES/APPENDICES:
13

ABSTRACT
This document contains a checklist that can be used to develop or evaluate security and privacy requirements for Cloud computing services. The content has been gathered from established industry standards and best practices, supplemented with requirements from European data protection legislation, and taking into account security issues identified in recent research on Cloud security. The document is intended to be used by potential cloud customers that need to assess the security of a cloud service they are considering, by cloud providers to evaluate the security of their offers, or by anyone else who is in need of supporting material for cloud security and privacy.

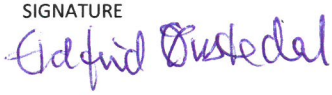
MAIN AUTHOR
Karin Bernsmed

SIGNATURE


QUALITY ASSUROR
Marie Moe

SIGNATURE


PROJECT RESPONSIBLE
Eldfrid Øvstedal

SIGNATURE


REPORT NO.	ISBN	CLASSIFICATION	CLASSIFICATION THIS PAGE
A27131	978-82-14-05908-3	Unrestricted	Unrestricted

1 Introduction

This document contains a checklist that can be used to develop or evaluate security and privacy requirements for Cloud computing services. The content has been gathered from established industry standards and best practices, supplemented with requirements from European data protection legislation, and taking into account security issues identified in recent research on Cloud security. The requirements in the document have been organized in terms of whether they are related to Data Storage, Data Processing, Data Transfer, Access Control, Security Procedures, Incident Management, Privacy or Layered Services.

This document is intended to be used by potential cloud customers that need to assess the security of a cloud service they are considering, by cloud providers to evaluate the security of their offers, or by anyone else who is in need of supporting material for cloud security and privacy. The authors have used it extensively for extracting relevant risks and vulnerabilities in public cloud services, applications and infrastructures, and we have decided to make this work openly accessible to benefit everyone interested in this domain.

To be applicable to all different types of cloud services, regardless of whether it is a storage service hosted by one of the big cloud providers or an application developed by a small company, all the requirements have been organized in tables, where each requirement has been specified in terms of security controls (the "security control" column). We recommend that for each control there should be a record stating the responsible actor for implementing this control and whether the control has been sufficiently implemented. We have found this way of organizing the requirements particularly useful during risk assessments.

The requirements in this report stem from an updated version of the Cloud Security Checklist Framework [1], which has been commissioned by Telenor Research. The work with this report has been partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317631 (OPTET).

2 Data Storage Requirements

ID	Category	Description	Security controls
S1	**Back-up**	*Ensure backup is properly done*	
			S1.1: Back-ups are performed at specific time intervals
			S1.2: Restoration of back-ups are tested at specific time intervals
			S1.3: Time to restore back-ups is guaranteed
			S1.4: Back-ups are stored in another availability zone/geographic location
			S1.5: Production data are not replicated or used in non-production environments
S2	**Encryption**	*Ensure data are never persistently stored in clear text*	
			S2.1: All data are encrypted when at rest
			S2.2: It is allowed to store encrypted data
			S2.3: Each customer has a unique encryption key
			S2.4: The encryption keys will be generated by a specified party (provider/customer/3rd party)
			S2.5: The encryption keys will be stored by a specified party (provider/customer/3rd party)
			S2.6: Encryption keys are protected against unauthorized access or accidental loss.
S3	**Location**	*Ensure data will be stored in a specific geographic location*	
			S3.1: All data will be stored in a specified country
			S3.2: All data will be stored in a country under a particular jurisdiction
S4	**Isolation**	*Ensure the data are isolated from other customers' data*	
			S4.1: All data will be segregated from other data maintained by the provider
			S4.2: All data will be stored on dedicated servers
			S4.3: All data will be stored on segregated infrastructure
			S4.4: All data will be stored in multi-instance databases
S5	**Ownership**	*Ensure customer retains ownership of the data*	
			S5.1: All data stored in the Cloud remain the sole property of the customer
			S5.2: All data generated by user interactions remain the sole property of the customer
			S5.3: All applications remain the sole property of the customer

			S5.4: The customer retains ownership of all data after the service contract has terminated.
S6	**Portability**	*Ensure portability of customer data*	
			S6.1: Data can be exported according to a specified standard
			S6.2: There is an interface for migration of customer data
S7	**Integrity**	*Ensure accuracy and consistency of customer data*	
			S7.1: Data integrity is being maintained for all data that are stored in the cloud
S8	**Deletion**	*Ensure proper disposal of customer data*	
			S8.1: All data replications will be deleted by a specific time after it has been requested
			S8.2: Data will be disposed by a specific method (overwriting/degaussing/media destruction)

3 Data Processing Requirements

ID	Category	Description	Security controls
P1	**Isolation**	*Ensure the data are isolated from other customers' data*	
			P1.1: All customer data in RAM will be isolated from other customers' data
			P1.2: Provider implements mechanisms to ensure that VMs do not interfere with each other
			P1.3: Each customer's applications will run on segregated infrastructure
			P1.4: Data sent to the service related to a specific request will not be visible to or used by any other users of the service
P2	**Monitoring**	*Ensures that breaches of acceptable use agreements will be detected*	
			P2.1: The behavior of running VMs/applications will be continuously monitored
P3	**Location**	*Ensure data will be processed in a specific geographic location*	
			P3.1: All data will be processed in a specific country
			P3.2: All data will be processed in a country under a

			particular jurisdiction
P4	**Migration**	*Ensure a secure transfer of VMs between different physical machines*	
			P4.1: All VM data will be encrypted during VM migration
P5	**Encryption**	*Ensures that data will never be processed in clear text*	
			P5.1: Computations can be performed on encrypted data ("homomorphic encryption")

4 Data Transfer Requirements

ID	Category	Description	Security controls
T1	**Encryption**	*Ensure data are never transferred in clear text*	
			T1.1: The upload / download of customer data is encrypted
			T1.2: All customer data will be encrypted in transit within the Cloud service
T2	**Integrity**	*Ensure accuracy and consistence of customer data*	
			T2.1: All customer data will be digitally signed when uploaded /downloaded to the Cloud
			T2.2: All customer data will be digitally signed when in transit within the Cloud service
			T2.3. The customer is able to digitally sign data that are being sent out from the Cloud
T3	**Non-repudiation**	*Ensures recipient of data cannot be denied*	
			T3.1: The customer is able to confirm reception of data that have been uploaded to the Cloud
			T3.2: The customer is able to confirm reception of data that have been sent out from the Cloud
T4	**Isolation**	*Ensure data are isolated from other customers' data*	
			T4.1: The provider offers network isolation between tenants
			T4.2: The customer is able to specify that data will only be sent over defined network sections
T5	**Location**	*Ensure data will never be transferred through specific geographic locations*	
			T5.1: Data in transit will only be routed through specified

			countries
T6	**Monitoring**	*Ensures that breaches of acceptable use agreements will be detected*	
			T6.1: The network between VMs in private subnets is monitored by networked-based intrusion detection and prevention systems

5 Access Control Requirements

ID	Category	Description	Security controls
AC1	**Management access control**	*Ensure secure access to the Cloud management interface (dashboard)*	
			AC1.1: Provider enforces a recognized password policy
			AC 1.2: Provider supports multi-factor authentication
			AC 1.3: Provider supports 3rd party authentication (SAML/OpenID) single sign on
			AC 1.4: Provider must have written approval from the customer to process any of the customer's files
AC2	**User access control**	*Ensure secure access for Cloud service users*	
			AC2.1: There is a system is place to create, update, suspend and delete user accounts, to remove access from employees when they leave the organization or to reset forgotten, lost or stolen credentials
			AC2.2: All cloud users each have their own user account
			AC2.3: There is a system in place to limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants
AC3	**Physical access control**	*Ensure that the datacenters are properly protected*	
			AC 3.1: The data centers are protected by physical security perimeters (fences/ guards/surveillance/locks)
			AC 3.2: Secure areas are monitored and access is restricted to authorized personnel
			AC 3.3: The provider's employees who have access to customer data have been subject to background checks
			AC 3.4: Access to application, program or object source code is restricted to authorized personnel on a need to know basis

6 Security Procedure Requirements

ID	Category	Description	Security controls
M1	**Auditing**	*Ensures that the Cloud services can be audited*	
			M1.1: The customer has a means to self-audit accesses
			M1.2: The customer has on-site audit rights to the provider's security program
			M1.3: The customer can require an independent assessment of the security of the cloud service
			M1.4: The assessment includes the physical, technical and organizational security measures in place and is appropriate for the particular cloud service.
			M1.5: In the case of layered cloud services, this assessment should include appropriate assurances that the security of each sub-processor likely to be involved in the processing of cloud customer's data will comply with security requirements set out by the cloud provider
			M1.6: The provider is able to provide the cloud customer with regular updates showing that appropriate security measures continue to be in place (and are kept up to date where necessary).
M2	**Classification**	*Ensures that the Cloud service fulfills a particular classification*	
			M2.1: The provider has a 3rd party certification (ISO 27001 / CCSP/ SafeHarbour, etc)
			M2.2: The provider will conduct regular risk assessments associated with data governance requirements
			M2.3: The customer can select a security level for the environment in which the application will be running
M3	**Countermeasures**	*Ensures that the Cloud service implements defense mechanisms*	
			M3.1: Firewalls have been set and configured
			M3.2: DoS/DDoS protection/mitigation mechanisms have been set up and configured
			M3.3: Data loss prevention mechanisms have been implemented
			M3.4: All software is kept up-to-date with the latest security patches
			M3.5: Redundant provisioning of the service has been set up

M4	**Testing**	*Ensures that the security of a Cloud service can be tested*	
			M4.1: The customer is allowed to do penetration testing
			M4.2: The provider performs regular vulnerability scans
M5	**Detection**	*Ensures that attacks and intrusions will be detected*	
			M5.1: An IDS has been set up and is correctly configured
			M5.2: Disks, memory and network are regularly scanned for malware
			M5.3: There are established procedures for monitoring and regular reviewing of logs
M6	**Notification**	*Ensures that the customers will receive information about security related changes*	
			M6.1: Provider will inform customers of open vulnerabilities
			M6.2: Provider will provide information on patches and controls in place
			M6.3: Anything which affects customer certification requirements will be reported to the customer
			M6.4: Provider will report any significant changes related to encryption procedures (change of key lengths, algorithms or key management procedures, etc.)
			M6.5: The provider will report any changes to the geographic location of services
			M6.6: The provider will respond to extraordinary requests for information regarding the use of the customer's system, within a certain timeframe
M7	**Recovery**	*Ensures that the Cloud service can recover from an attack*	
			M7.1: The provider maintains periodic checkpoints of VM state
			M7.2: The provider guarantees that if the system is compromised it will be running securely again within a certain amount of time
			M7.3: The provider performs tests of the recovery of

			data from backups at regular time intervals
M8	**Key management**	*Ensures the correct management of cryptographic keys*	
			M8.1: Recognized methods are used to generate, exchange, store, safeguard, use and replace cryptographic keys
			M8.2: There is a key escrow system in place
M9	**Transparency**	*Ensures transparency of the cloud service and its security mechanisms*	
			M9.1: The cloud provider has documented the design of the service and its security mechanisms
			M9.2: The cloud provider cannot change its security architecture unless the customer has been informed in writing and approved the changes.

7 Incident Management Requirements

ID	Category	Description	Security controls
IR1	**Response**	*Ensures that there is a system in place to respond to security incidents*	
			IR1.1: Provider implements mechanisms to monitor and quantify the types, volumes and costs of incidents
			IR1.2: Incident severity is classified according to a well-defined scheme
			IR1.3: Provider will implement a remedial response, given a specific severity class, within a specified time
			IR1.4: The provider employs a recognized method for dealing with security incidents (such as NIST SP 800-61 or ISO 27035)
IR2	**Logging**	*Ensures that the provider will log security incidents*	
			IR2.1: The provider will retain audit logs recording privileged user access activities, authorized and unauthorized access attempts, system exceptions, and information security events
			IR2.2: The provider will make relevant log information

			available to the customer
IR3	**Reporting**	*Ensures that the provider will report security incidents to the customer*	
			IR3.1: Provider will report security incidents to the customer within a specified time frame
			IR3.2: Provider will report on incidents through a pre-defined communication channel
			IR3.3: Provider will report incident data only to the affected party
			IR3.4: Provider will only report incident data to 3rd parties after consulting the customer
			IR3.5: Provider will report on the recovery process at given time intervals
			IR3.6: Provider will report the expected time to recover at given time intervals
IR4	**Forensics**	*Ensures that the provider facilitates forensic procedures*	
			IR4.1: In case of a security incident that requires legal action, the provider will collect and deliver supporting evidence
			IR4.2: The provider complies with jurisdictional requirements for handling incident data and evidence according to specified chain of custody
			IR4.3: The provider guarantees financial penalties in case of a security breach

8 Privacy Requirements

ID	Category	Description	Security controls
PR1	**Non-disclosure**	*Ensures that customer data will be kept private*	
			PR1.1: There is a clear policy in place to specify the circumstances in which the cloud provider may access its customers' data
			PR1.2: The provider will not disclose any of the customer' data to any 3rd party
			PR1.3: The provider will only disclose customer data to 3rd party providers on a need-to-know basis
PR2	**Anonymity**	*Ensures that the customer will remain*	

		anonymous	
			PR2.1: Provider will not disclose any details about the customer to any unrelated third party
			PR2.2: Provider will not provide common logs to any other customer
PR3	**Data minimization**	*Ensures that no unnecessary data will be collected*	
			PR3.1: Provider will only require the minimal set of data necessary to perform the service
PR4	**Data Processing Agreement (DPA)**	*Ensures that personal data are properly protected*	
			PR4.1: The DPA states that the processor will only act upon instructions from the controller
			PR4.2: The DPA states that the data processor will comply with security obligations equivalent to those imposed on the data controller itself
			PR4.3: The provider is not able to change the terms of data processing operations during the lifetime of the contract without the customer's knowledge and agreement
			PR4.4: The cloud customer must ensure that a move to a cloud service still allows data subjects to exercise their rights.

9 Layered Services Requirements

ID	Category	Description	Security controls
LS1	**Outsourcing**	*Requirements regarding 3rd party service providers*	
			LS 1.1: The provider will not outsource the service to any 3rd party provider
			LS 1.2: All infrastructure for the service will be delivered by the same provider
			LS 1.3: Provider will not outsource the service to any company from a particular country
LS2	**Surveillability**	*Ensure the customer's ability to inspect how the service is assembled*	
			LS 2.1: The customer is able to inspect the composition of the service
			LS 2.2: The customer will be notified when the composition of the service changes
LS3	**Binding of**	*Two or more*	

	duties	*given services must be delivered by the same party*	
			LS 3.1: Roles in a specification defines which tasks must be performed by the same actor.
LS4	**Separation of duties**	*Two or more given services cannot be delivered by the same party*	
			LS 4.1: Roles in a specification defines which tasks cannot be performed by the same actor.

10 Bibliography

[1] Martin Gilje Jaatun, Per Håkon Meland, Karin Bernsmed, Humberto Castejón, and Astrid Undheim. "Cloud Security Whitepaper. A Briefing on Cloud Security Challenges and Opportunities." Technical report, October 2013. Available at http://www.telenor.com/media/articles/2013/safe-in-the-cloud/ (last accessed 2015-08-20).

[2] Wayne Jansen and Timothy Grance. "Guidelines on Security and Privacy in Public Cloud Computing". NIST SP 800-144, December 2011. Available at http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf (last accessed 2015-08-20).

[3] The Cloud Security Alliance Cloud Controls Matrix (CCM), version 3.0.1. Available at https://cloudsecurityalliance.org/research/ccm/ (last accessed 2015-08-20).

[4] The FedRAMP Security Controls. Available at https://www.fedramp.gov/resources/documents/ (last accessed 2015-08-20).

[5] Procure Secure - A guide to monitoring of security service levels in cloud contracts. ENISA, 2012. Available at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/ (last accessed 2015-08-20).

[6] Karin Bernsmed, Martin Gilje Jaatun and Astrid Undheim**.** "Security in Service Level Agreements for Cloud Computing". In Proceedings of the 1st International Conference on Cloud Computing and Services Science (CLOSER 2011), Noordwijkerhout, The Netherlands, 7-9 May 2011.

[7] Aniketos Security Property Elicitation (internal report), http://www.aniketos.eu/

[8] Ernst & Young's 2011 Global Information Security Survey: "Into the cloud, out of the fog", November 2011

[9] Jay Heiser and David W. Cearley. "Hype Cycle for Cloud Security, 2011". Gartner report, 28 July, 2011.

[10] Peter Mell and Timothy Grance. "The NIST Definition of Cloud Computing". NIST SP 800-145, September 2011. Available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (last accessed 2015-08-20).

[11] Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf. "NIST Cloud Computing Reference Architecture". NIST SP 500-292, September 2011. Available at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505 (last accessed 2015-08-20).

Technology for a better society

www.sintef.no