

Self-assessment for XXX

Instructions

Read through the requirement and examples. Fill in to the empty column by answering these questions:

1. How is this requirement currently fulfilled?
2. What is currently missing in order to meet this requirement? Make notes of the findings:
 - Is there an administrative issue keeping the organization from meeting the criteria?
 - Are there resourcing issues that prevent the organization from meeting the criteria?
 - Maybe there is an acknowledged residual risk that makes the criteria obsolete?
 - Are there technical reasons or measures that full fill the criteria via other means?

Administrative requirements

1.1	Documentation	
Existence of necessary documents	<ul style="list-style-type: none"> • Business continuity plan exists • Disaster recovery plan exists and includes this service • Recovery time objective is defined for this service • Recovery point objective is defined for this services • Risk analysis exists and is regularly updated • Infrastructure and service documentation is written and has a process for frequent updates 	
Reference	2.2, 2.3, 3.1, 3.1.1, 3.1, 3.2.2, 3.2.3, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 4.3	
Examples	<ul style="list-style-type: none"> • Business continuity and disaster recovery plans are written and updated as needed, and they include this service. • Recovery time objective is defined for this service. A defined RTO aims at ensuring that the service level is met by the provider and ensures the service quality can be monitored. • Recover point objective is defined for this service. A defined RPO aims at ensuring that the service level is met by the provider and ensures the service quality can be monitored. • A comprehensive risk analysis is written and it includes threats for this service. A comprehensive risk analysis should take into account for example: <ul style="list-style-type: none"> ◦ The chosen cloud type and deployment model are recognized and the threats they imply are verified. ◦ Possible threats derived from e.g. multi-tenancy, responsibilities and geographical location are recognized and analyzed. • There exists for documents that for example describe the service's architecture, data locations, data flows and interfaces. This documentation is up-to-date. • The necessary documentation is up-to-date and there exists a process to 	

	continuously update these. Also, the documentation should also include the cloud provider's aspect.	
--	---	--

1.2	SLA	
Service level agreement documents	<ul style="list-style-type: none"> • SLA contracts exist with some or all service providers • SLA meets the needs of the service or services 	
Reference	3.10.2	
Examples	<ul style="list-style-type: none"> • SLA contracts are done with all necessary cloud providers • The documents are signed by all involved parties • The SLA requirement follows the needs specified in the service descriptions • The SLA documents ensure quality, reliability, security and scalability of the service 	

1.3	Transferability	
Technologies and contracts enable fast transfer of the service and data	<ul style="list-style-type: none"> • The service uses common standards • The service uses common protocols • The policies do not prevent data transfer 	
Reference	3.2.4	
Examples	<ul style="list-style-type: none"> • The programming languages and data formats to name a few are common and not e.g. proprietary. • The protocols used in the service and related services are common and not e.g. proprietary. • There exists e.g. another service provider to whose infrastructure the service could be transferred. • There are no contractual limitation to transfer the service or the limitations are recognized and there is a plan to overcome them. 	

1.4	Regulative requirements	
Requirements set by regulations	<ul style="list-style-type: none"> • Necessary documents exist to depict the regulations each party and service has to commit into • Procedures exist to audit and update the documentation and procedures regularly 	

Reference	3.2.2, 3.2.3	
Examples	<ul style="list-style-type: none"> • The implemented regulations by the service are documented • Procedures exist to audit the compliance regularly • Procedures exist to follow changes in the regulations 	

1.5	Personnel	
Personnel: roles and training	<ul style="list-style-type: none"> • Key roles are recognized • The personnel is trained to recognize and act upon any attacks 	
Reference	3.10.4	
Examples	<ul style="list-style-type: none"> • Key roles, like manager roles, are recognized and named • All personnel is trained to recognize malicious deeds • All personnel is trained to follow defined procedures upon a malicious deed • There is a document verifying training • There is a documented procedure to to keep the training up-to-date 	

1.6	Incident response	
Incident response and definitions of responsibilities	<ul style="list-style-type: none"> • Ensure that the responsibilities are defined between the customer and provider • Ensure the service provider and the customer have sufficient strategy for incidents • Ensure the service provider and the customer have the ability to properly handle incidents • Ensure that proper technology to identify potential attacks exist and operate properly, these can be for example intrusion detection or prevention systems and proper logging infrastructure • Ensure that dedicated personnel exists to handle the incidents, the incident response team should have the ability to analyze, respond, escalate and to report any incidents 	
Reference	3.2.6	

Examples	•	
----------	---	--

Physical requirements

2.1	Physical security and continuity	
Physical security and continuity	<ul style="list-style-type: none"> • Verify the cloud provider's documentation about physical security • Verify that physical security fulfills the requirements 	
Reference	2.1	
Examples	<ul style="list-style-type: none"> • Verify that documentation exists about the cloud provider's physical security • Verify that the documentation is up-to-date and the provider applies the procedures with e.g. interviewing the provider or using 3rd party audit reports • Verify that there is internal documentation about physical security requirements for this service or the company in general • Compare the provider's document against company's internal requirements 	

2.2	Supply chain security and continuity	
Supply chain security and continuity	<ul style="list-style-type: none"> • Verify there are contracts, controls, policies and monitoring which ensure availability and security of new hardware, software and installation 	
Reference	3.10.3	
Examples	<ul style="list-style-type: none"> • Verify that support contracts secure and fast enough delivery of replacement hardware, software and installation • Verify that proper hardware and software updates are taken care of by the contract • Ensure that the delivery chain is trustworthy • Ensure that there are written procedures to verify that the deliveries are received in proper state, e.g. seals are untouched, installations are done by designated persons 	

Technical requirements

3.1	Defence-in-depth	
Defence-in-depth: segmentation	<ul style="list-style-type: none">• There are multiple layers of defences• Segments requiring more security are separated from those requiring less• There are protective measures between different segments	
Reference	3.12.4	
Examples	<ul style="list-style-type: none">• Based on architecture diagrams there are different segments separated from others, when required security measures differ between devices and services• The built system follows the aforementioned documentation• There are technologies like firewalls, VPNs and intrusion detection systems between segments• Individual systems are protected with additional measures like host IDS, host firewalls and malware detection software	

3.2	Segregation of duties	
Segregation of duties	<ul style="list-style-type: none">• Segregation of duties is done by both the provider and customer• Ensure that a single person can not execute a full path of actions• Changes are tracked	
Reference	3.2.5	
Examples	<ul style="list-style-type: none">• Critical processes that require multiple actors are defined• All parties' policies, abilities and strategy are ensuring segregation of duties• There are technical and process oriented measures to ensure segregation• There is sufficient tracking for all critical actions• A single person can not modify tracking logs	

3.3	Encryption and key management	
------------	--------------------------------------	--

Encryption: securing data and keys	<ul style="list-style-type: none"> • Data stores and flows are documented • Data is encrypted during storage and transfer when required • The encryption algorithms used are sufficient and fulfill legislative requirements • The encryption keys are sufficient and stored so that their secrecy and availability are ensured 	
Reference	3.11.1, 3.11.4	
Examples	<ul style="list-style-type: none"> • All data locations whether moving or in rest are documented • The data is encrypted or protected with other acceptable methods like hiding all the time • The encryption algorithms satisfy the requirements of legislation, policies and current recommendations • The encryption devices, software and configuration are according to legislation, policies and recommendations • The encryption keys are of required length and complexity, the keys are changed on required intervals • The keys are stored securely and separated from data, the keys are stored so that they can not be lost • Process exist to verify that the encryption and keys are updated as needed • Process exist to audit that data and communication are encrypted when needed 	

3.4	Backups	
	<ul style="list-style-type: none"> • Regular backups are taken of all the relevant data • Backups are stored regularly to a offsite location(s) • Full backup (if applicable) is taken regularly enough for restore time to meet the RTO • Backup mediums are being refreshed so that when new backup systems become available, old backups are still readable for restores • Expired backup mediums are destroyed according to standard, or overwritten by 	

	new backups <ul style="list-style-type: none"> • Restore functionality is tested regularly 	
Reference	3.12.1	
Examples	<ul style="list-style-type: none"> • All relevant data is identified and backups are configured • Tape/disk library in a separate location • Full backup (if applicable) is taken regularly enough for restores to be fluent • Backup mediums are refreshed as new LTO generations are being introduced • Mediums are destroyed using standard compliant mechanism once they are at the end of their life-cycle • Restore functionality is tested regularly by using scripts and status is being monitored 	

3.5	Authentication	
	<ul style="list-style-type: none"> • 	
Reference		
Examples	<ul style="list-style-type: none"> • 	

3.6	Lifecycle management	
	<ul style="list-style-type: none"> • Different stages of service life-cycle are identified and record of services is kept • There is a regular procedure to update the service catalog • There is a clearly defined decommissioning procedure for services 	
Reference	3.10.5	
Examples	<ul style="list-style-type: none"> • Specs, discovery, negotiation, composition, consumption and decommissioning are identified • Automated mechanism in-place to detect new hosts and services • Decommissioning planning is part of the initial specification 	

3.7	Hardening	
	<ul style="list-style-type: none"> • 	
Reference		
Examples	<ul style="list-style-type: none"> • 	

3.8	Vulnerability and patch management	
	•	
Reference		
Examples	•	

3.9	Log management	
	<ul style="list-style-type: none"> • Logging is configured • There is a log filtering and alarming configured • There is a mechanism in-place to detect and prevent tampering with the log entries • Logging is done to a remote system • Custom applications (if applicable) implement their logging according to standard 	
Reference	3.12.7	
Examples	<ul style="list-style-type: none"> • Syslog is configured, not left on defaults • SIEM system or similar log filtering and analysis tool is deployed • Syslog is configured to sent the logs to remote syslog server • Logging is part of the specification of custom application 	