# Self-assessment for Organization Y

## 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 | Notes |
|---|---|---|
| Existence of necessary documents | • Business continuity plan exists<br>• Disaster recovery plan exists and includes this service<br>• Recovery time objective is defined for this service<br>• Recovery point objective is defined for this services<br>• Risk analysis exists and is regularly updated<br>• 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 | • Business continuity and disaster recovery plans are written and updated as needed, and they include this service.<br>• 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.<br>• 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.<br>• A comprehensive risk analysis is written and it includes threats for this service. A comprehensive risk analysis should take into account for example:<br>  ○ The chosen cloud type and deployment model are recognized and the threats they imply are verified.<br>  ○ Possible threats derived from e.g. multi-tenancy, responsibilities and geographical location are recognized and analyzed.<br>• There exists for documents that for example describe the service's architecture, data locations, data flows and interfaces. This documentation is up-to-date.<br>• 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** | **Notes** |
|---|---|---|
| Service level agreement documents | • SLA contracts exist with some or all service providers<br>• SLA meets the needs of the service or services | |
| Reference | 3.10.2 | |
| Examples | • SLA contracts are done with all necessary cloud providers.<br>• The documents are signed by all involved parties.<br>• The SLA requirement follows the needs specified in the service descriptions.<br>• The SLA documents ensure quality, reliability, security and scalability of the service. | |

| **1.3** | **Transferability** | **Notes** |
|---|---|---|
| Technologies and contracts enable fast transfer of the service and data | • The service uses common standards<br>• The service uses common protocols<br>• The policies do not prevent data transfer | |
| Reference | 3.2.4 | |
| Examples | • The programming languages and data formats to name a few are common and not e.g. proprietary.<br>• The protocols used in the service and related services are common and not e.g. proprietary.<br>• There exists e.g. another service provider to whose infrastructure the service could be transferred.<br>• 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 | Notes |
|---|---|---|
| Requirements set by regulations | • Necessary documents exist to depict the regulations each party and service has to commit into<br>• Procedures exist to audit and update the documentation and procedures regularly | |
| Reference | 3.2.2, 3.2.3 | |
| Examples | • The implemented regulations by the service are documented.<br>• Procedures exist to audit the compliance regularly.<br>• Procedures exist to follow changes in the regulations. | |

| 1.5 | Personnel | Notes |
|---|---|---|
| Personnel: roles and training | • Key roles are recognized<br>• The personnel is trained to recognize and act upon any attacks | |
| Reference | 3.10.4 | |
| Examples | • Key roles, like manager roles, are recognized and named.<br>• All personnel is trained to recognize malicious deeds.<br>• All personnel is trained to follow defined procedures upon a malicious deed.<br>• There is a document verifying training.<br>• There is a documented procedure to to keep the training up-to-date. | |

| 1.6 | Incident response | Notes |
|---|---|---|
| Incident response and definitions of responsibilities | • Ensure that the responsibilities are defined between the customer and provider<br>• Ensure the service provider and the customer have sufficient strategy for incidents<br>• Ensure the service provider and the customer have the ability to properly handle incidents<br>• 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 | • The customer and provider both have a detailed and documented incident handling workflow.<br>• There is an up-to-date incident response team in all parties and shared communication channels during incident escalation.<br>• Technologies exist to recognize incidents, for example: SIEM, IDS, detailed information about the normal state including protocols, devices and IPs to name a few.<br>• Incident handling process is tested frequently and the personnel are trained. | |

# Physical requirements

| 2.1 | Physical security and continuity | Notes |
|---|---|---|
| Physical security and continuity: physical security fulfilling the requirements | • Verify the cloud provider's documentation about physical security<br>• Verify that physical security fulfills the requirements | |
| Reference | 2.1 | |
| Examples | • Documentation exists about the cloud provider's physical security.<br>• The documentation is up-to-date and the provider applies the procedures with e.g. interviewing the provider or using 3rd party audit reports.<br>• There is internal documentation about physical security requirements for this service or the company in general.<br>• Compare the provider's document against company's internal requirements. | |

| 2.2 | Supply chain security and continuity | Notes |
|---|---|---|
| Supply chain security and continuity | • Verify there are contracts, controls, policies and monitoring which ensure availability and security of new hardware, software and installation | |
| Reference | 3.10.3 | |
| Examples | • Verify that support contracts secure and fast enough delivery of replacement hardware, software and installation.<br>• Verify that proper hardware and software updates are taken care of by the contract.<br>• Ensure that the delivery chain is trustworthy.<br>• 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 | Notes |
|---|---|---|
| Defense-in-depth: segmentation | • There are multiple layers of defenses<br>• Segments requiring more security are separated from those requiring less security<br>• There are protective measures between different segments<br>• The connectivity towards cloud is robust and redundant from both ends | |
| Reference | 3.12.4 | |
| Examples | • Based on architecture diagrams there are different segments separated from others, when required security measures differ between devices and services.<br>• The built system follows the aforementioned documentation.<br>• There are technologies like firewalls, VPNs and intrusion detection systems between segments.<br>• Individual systems are protected with additional measures like host IDS, host firewalls and malware detection software.<br>• Dual homed connectivity via different Internet Service Providers. | |

| 3.2 | Segregation of duties | Notes |
|---|---|---|
| Segregation of duties: avoiding dangerous work combinations and tracking changes | • Segregation of duties is done by both the provider and customer<br>• It is ensured that a single person can not execute a full path of actions<br>• Changes are tracked | |
| Reference | 3.2.5 | |
| Examples | • Critical processes that require multiple actors are defined.<br>• All parties' policies, abilities and strategy are ensuring segregation of duties.<br>• There are technical and process oriented measures to ensure segregation.<br>• There is sufficient tracking for all critical actions. | |

| | | |
|---|---|---|
| | • A single person can not modify tracking logs. | |

| **3.3** | **Encryption and key management** | **Notes** |
|---|---|---|
| Encryption: securing data and keys | • Data stores and flows are documented<br>• Data is encrypted during storage and transfer when required<br>• The encryption algorithms used are sufficient and fulfill legislative requirements<br>• The encryption keys are sufficient and stored so that their secrecy and availability are ensured<br>• Backups to cloud are encrypted | |
| Reference | 3.11.1, 3.11.4 | |
| Examples | • All data locations whether moving or in rest are documented.<br>• The data is encrypted or protected with other acceptable methods like hiding all the time.<br>• The encryption algorithms satisfy the requirements of legislation, policies and current recommendations.<br>• The encryption devices, software and configuration are according to legislation, policies and recommendations.<br>• The encryption keys are of required length and complexity, the keys are changed on required intervals.<br>• The keys are stored securely and separated from data, the keys are stored so that they can not be lost.<br>• Process exist to verify that the encryption and keys are updated as needed.<br>• Process exist to audit that data and communication are encrypted when needed.<br>• Backups are encrypted using keys not shared with the service provider. | |

| **3.4** | **Backups** | **Notes** |
|---|---|---|
| Backups and restoration | • Regular backups are taken of all the relevant data<br>• Backups are stored regularly to an offsite location(s)<br>• Full backup (if applicable) is taken regularly enough for restore time to meet the RTO<br>• Backup mediums are being refreshed so that when new backup systems become available, old backups are still readable for restores<br>• Expired backup mediums are destroyed according to standard or overwritten by new backups<br>• Restore functionality is tested regularly | |
| Reference | 3.12.1 | |
| Examples | • All relevant data is identified and backups are configured.<br>• Tape/disk library in a separate location.<br>• Full backup (if applicable) is taken regularly enough for restores to be fluent.<br>• Backup mediums are refreshed as new LTO generations are being introduced.<br>• Mediums are destroyed using a standard compliant mechanism once they are at the end of their lifecycle.<br>• Restore functionality is tested regularly by using scripts and status is being monitored. | |

| **3.5** | **Authentication** | **Notes** |
|---|---|---|
| Secure authentication throughout the infrastructure | • Users, devices and services are authenticated throughout the service<br>• Authentication methods follow recommendations<br>• Authentication data is protected | |
| Reference | 5.3.5 | |
| Examples | • All data and process access requires authentication and authorization.<br>• When possible, two-factor authentication is used.<br>• Authentication is constructed using at least one of the following: something the user knows, has or is unique to each user.<br>• Logon ID does not consist of e.g. | |

| | | |
|---|---|---|
| | person’s name or other easily accessible data.<br>• Authentication data is properly protected.<br>• The authentication requirements are fulfilled all over the service, including also the platform and other dependencies. | |

| **3.6** | **Lifecycle management** | **Notes** |
|---|---|---|
| Managing services throughout their lifetime | • Different stages of service lifecycle are identified and record of services is kept<br>• There is a regular procedure to update the service catalog<br>• There is a clearly defined decommissioning procedure for services | |
| Reference | 3.10.5 | |
| Examples | • Specs, discovery, negotiation, composition, consumption and decommissioning are identified.<br>• Automated mechanism in-place to detect new hosts and services.<br>• Decommissioning planning is part of the initial specification. | |

| **3.7** | **Hardening** | **Notes** |
|---|---|---|
| Minimized installations | • Used disk images are hardened to contain the desired settings and patches | |
| Reference | 5.3.7 | |
| Examples | • The disk images used in services are acquired from a defined source.<br>• The images are minimized to contain only the needed software and correct configuration.<br>• The images are updated frequently.<br>• The image installation and update processes are monitored.<br>• Other requirements by the customer concerning the operating system and dependencies are fulfilled. | |

| **3.8** | **Vulnerability and patch management** | **Notes** |
|---|---|---|
| Vulnerability and patch management: keeping software up-to-date | • Updating and patching of devices and services are applied in a managed manner by both the customer and provider<br>• Security scans are used to ensure proper update and patch procedures | |
| Reference | 5.3.8, 3.12.6 | |
| Examples | • Both the customer and provider have a process to recognize and analyze any vulnerabilities in the systems.<br>• Updates and patches are applied frequently in a controlled manner.<br>• Vulnerability scans or equivalent methods are used to verify that all devices and services are up-to-date.<br>• Patching, updating and scanning are applied to different parts of the infrastructure. | |

| **3.9** | **Log management** | **Notes** |
|---|---|---|
| Log management: securing and gathering logs for tracing and alarms | • Logging is configured<br>• There is a log filtering and alarming configured<br>• There is a mechanism in-place to detect and prevent tampering with the log entries<br>• Logging is done to a remote system<br>• Custom applications (if applicable) implement their logging according to an applicable standard | |
| Reference | 3.12.7 | |
| Examples | • Logging is configured and not left on defaults.<br>• SIEM system or similar log filtering and analysis tool is deployed.<br>• Logging is configured to send logs to a remote log server.<br>• Logging is part of the specification of the custom application. | |