4. Organisation of Information Security

4.1. OIS-01 Information Security Management System

4.1.1 Objective

The CSP operates an Information Security Management System (ISMS). The scope of the ISMS covers the CSP's organisational units, locations and processes for providing the cloud service.

4.1.2. Requirements

Basic	**The CSP shall document the scope of the cloud service that is under the CSP's control and the boundaries.**	OIS-01.1B
	The CSP shall have an information security management system (ISMS), covering at least the operational units, locations, people and processes for providing the cloud service.	OIS-01.2B
	The CSP shall provide documented information about the ISMS as applied to the cloud service, covering what is applicable to the cloud service regarding: • **Scope and boundaries of the ISMS;** • **The context of the CSP;** • **Description of how the cloud service is covered by activities in the ISMS; and** • **How the security of the cloud service is maintained and improved**	OIS-01.3B
Substantial	The CSP shall document the scope of the cloud service that is under the CSP's control and the boundaries.	OIS-01.1S
	The CSP shall have an information security management system (ISMS), covering at least the operational units, locations, people and processes for providing the cloud service.	OIS-01.2S
	The CSP shall provide documented information about the ISMS as applied to the cloud service, covering what is applicable to the cloud service regarding: • Scope and boundaries of the ISMS; • The context of the CSP; • Description of how the cloud service is covered by activities in the ISMS; and • How the security of the cloud service is maintained and improved	OIS-01.3S
High	The CSP shall document the scope of the cloud service that is under the CSP's control and the boundaries.	OIS-01.1H
	The CSP shall have an information security management system (ISMS), covering at least the operational units, locations, people and processes for providing the cloud service.	OIS-01.2H

106

	The CSP shall provide documented information about the ISMS as applied to the cloud service, covering what is applicable to the cloud service regarding: • Scope and boundaries of the ISMS; • The context of the CSP; • Description of how the cloud service is covered by activities in the ISMS; and • How the security of the cloud service is maintained and improved.	OIS-01.3H

1153

4.2. OIS-02 Segregation of Duties

4.2.1 Objective

Conflicting tasks and responsibilities are separated based on an RM-01 risk assessment to reduce the risk of unauthorised or unintended changes or misuse of CSC data in use, in motion or at rest in the cloud service.

4.2.2 Requirements

Basic	**The CSP shall perform a risk assessment as defined in RM-01 about the accumulation of responsibilities or tasks on roles or individuals, regarding the provision of the CSC, covering at least the following areas, insofar as these are applicable to the provision of the cloud service and are in the area of responsibility of the cloud service:** • **Administration of rights profiles, approval and assignment of access and access authorisations (cf. IAM-01);** • **Development, testing and release of changes (cf. DEV-01, CCM-01); and** • **Operation of the system components.**	OIS-02.1B
	The CSP shall implement the mitigating measures defined in the risk treatment plan, prioritising separation of duties.	OIS-02.2B
	If implementation is impossible for organisational or technical reasons, the measures shall include the monitoring of activities in order to detect unauthorised or unintended changes as well as misuse and the subsequent appropriate actions.	OIS-02.3B
Substantial	The CSP shall perform a risk assessment as defined in RM-01 about the accumulation of responsibilities or tasks on roles or individuals, regarding the provision of the cloud service, covering at least the following areas, insofar as these are applicable to the provision of the cloud service and are in the area of responsibility of the cloud service:	OIS-02.1S

107

	• Administration of rights profiles, approval and assignment of access and access authorisations (cf. IAM-01); • Development, testing and release of changes (cf. DEV-01, CCM-01); and • Operation of the system components.	
	The CSP shall implement the mitigating measures defined in the risk treatment plan, prioritising separation of duties.	OIS-02.2S
	If implementation is impossible for organisational or technical reasons, the measures shall include the monitoring of activities in order to detect unauthorised or unintended changes as well as misuse and the subsequent appropriate actions.	OIS-02.3S
	The CSP shall: • **Introduce and maintain an inventory of conflicting roles including resolving measures;**	OIS-02.4S
	• **Enforce the segregation of duties during the assignment or modification of roles as part of the role management process.**	OIS-02.5S
High	The CSP shall perform a risk assessment as defined in RM-01 about the accumulation of responsibilities or tasks on roles or individuals, regarding the provision of the cloud service, covering at least the following areas, insofar as these are applicable to the provision of the cloud service and are in the area of responsibility of the cloud service: • Administration of rights profiles, approval and assignment of access and access authorisations (cf. IAM-01); • Development, testing and release of changes (cf. DEV-01, CCM-01); and • Operation of the system components.	OIS-02.1H
	The CSP shall implement the mitigating measures defined in the risk treatment plan, prioritising separation of duties.	OIS-02.2H
	If implementation is impossible for organisational or technical reasons, the measures shall include the monitoring of activities in order to detect unauthorised or unintended changes as well as misuse and the subsequent appropriate actions.	OIS-02.3H
	The CSP shall: • Introduce and maintain an inventory of conflicting roles including resolving measures;	OIS-02.4H
	• Enforce the segregation of duties during the assignment or modification of roles as part of the role management process.	OIS-02.5H
	The CSP shall monitor and enforce measures related to segregation of duties to resolve conflicting roles.	OIS-02.6H