Logging Deep Dive - V1.0

ID	Requirements	Reference
Logging_01	The policies and procedures for ICT operations shall cover information on controls and monitoring of ICT systems, including details on protocols for audit trails and system log information.	RTS risk management
Logging_02	Develop, document, and implement a logging procedure, including logging protocols and tools as part of the ICT security procedures.	
The logging procedure shall require		
Logging_03	the specification of events to be logged, the retention period, and measures to secure and handle log data, considering the purpose of log creation. Retention periods shall be set based on business and security objectives, the reason for recording the event, and the results of the ICT risk assessment	
Logging_04	the logging of events related to physical access control.	
Logging_05	the logging of events related to logical access control, as well as identity management	
Logging_06	the logging of events related to capacity management.	
Logging_07	the logging of events related to change management.	
Logging_08	the logging of events related to ICT operations, including ICT system activities.	
Logging_09	the logging of events related to network traffic activities, including ICT network performance.	
Logging_10	the synchronization of ICT system clocks with a documented reliable reference time source, in accordance with applicable regulatory requirements.	
The logging procedures shall include measures		
Logging_11	to protect logging systems and log information against tampering, deletion, and unauthorized access at rest, in transit, and, where relevant, in use.	
Logging_12	to detect failures in logging systems.	
Logging_13	The logging procedures, protocols, and tools shall ensure that the level of detail in logs is aligned with their purpose and usage to effectively detect anomalous activities.	
Logging_14	Ensure logging of the granting, reviewing, and revoking of access rights, and define retention periods for the log files based on business and information security objectives, the purpose of recording the events, and the results of the ICT risk assessment.	
Logging_15	Implement procedures to identify and log authorized individuals accessing premises, data centers, and sensitive areas, with the level of logging aligned to the importance of these locations and the criticality of the operations or ICT systems housed within.	
Logging_16	Collect, monitor, and analyse the logs collected to promptly detect anomalous activities, including ICT network performance issues and ICT-related incidents.	