

MPS

August 2025

# Compliance Mapping Tables for MPS Cloud Reference Architecture v1.1

# 1. Compliance Mapping Tables

This section is intended to provide guidance for the Customer(s) and Supplier(s) in mapping the principal and basic information security requirements to established standards and frameworks for compliance purposes. The compliance mapping tables will be extended with additional standards and frameworks in future versions, such as NIS2 and NIS2 Implementing Regulations.

Note that the mapping table is intended as guidance only based on the included standards. Such a mapping exercise will always be a subjective assessment, and the mapping tables are therefore not to be considered complete (i.e., all mappings are not necessarily provided) or authoritative (i.e., other interpretations are valid).

## 1.1 Principal Security Requirements Mapping Table

CRA Requirement	NIST CSF 2.0	ISO 27001:2022	ISO 27002:2022	NSM Grunnprinsipper for IKT-sikkerhet 2.1	CSA CCM V4.0.12	BSI C5:2020 (Cloud Computing Compliance Criteria Catalogue)
A.1 Purpose	<ul style="list-style-type: none"> <li>GV.OC Organizational Context (GV.OC-01, 02, 04, 05, )</li> </ul>	<ul style="list-style-type: none"> <li>4.1 Understanding the organization and its context</li> <li>4.2 Understanding the needs and expectations of interested parties</li> </ul>				

		<ul style="list-style-type: none"> <li>6.2 Information security objectives and planning to achieve them</li> </ul>				
A.2 Purpose	<ul style="list-style-type: none"> <li>GV.OV Oversight (GV.OV-01, 02, 03)</li> <li>GV.PO Policies, Processes, and Procedures (GV.PO-01)</li> <li>GV.RM Risk Management Strategy (GV.RM-01, 02, 03, 04, 06, 07)</li> <li>GV.RA Risk Assessment (ID.RA-05, 06, 07)</li> </ul>	<ul style="list-style-type: none"> <li>6.1.1 General</li> </ul>		<ul style="list-style-type: none"> <li>1.1 Identify management structures, deliverables and supporting systems (1.1.2, 1.1.3, 1.1.4, 1.1.5)</li> <li>2.1 Include security during procurement and development processes (2.1.4, 2.1.9)</li> <li>2.2 Establish a secure ICT architecture (2.2.7)</li> <li>2.3 Maintain a secure configuration (2.3.10)</li> </ul>	<ul style="list-style-type: none"> <li>GRC Governance, Risk and Compliance (GRC-02, GRC-04)</li> <li>TVM Threat &amp; Vulnerability Management (TVM-01)</li> <li>CCC Change Control and Configuration Management (CCC-03)</li> <li>CEK Cryptography , Encryption &amp; Key Management (CEK-07)</li> <li>STA Supply Chain Management, Transparency , and</li> </ul>	<ul style="list-style-type: none"> <li>OIS-06 Risk management policy</li> <li>OIS-07 Application of the risk management policy</li> </ul>

					Accountability (STA-08) <ul style="list-style-type: none"> <li>BCR Business Continuity Management and Operational Resilience (BCR-02)</li> </ul>	
A.3 Compliance	<ul style="list-style-type: none"> <li>OV.OC Organizational Context (GV.OC-03)</li> </ul>	<ul style="list-style-type: none"> <li>8.1 Operational Planning and Control</li> </ul>	<ul style="list-style-type: none"> <li>5.4 Management Responsibilities</li> <li>5.10 Acceptable use of information and other associated assets</li> <li>5.31 Legal, statutory, regulatory, and contractual requirements</li> </ul>	<ul style="list-style-type: none"> <li>3.2 Establish security monitoring (3.2.2)</li> </ul>	<ul style="list-style-type: none"> <li>A&amp;A Audit &amp; Assurance (A&amp;A-04)</li> </ul>	<ul style="list-style-type: none"> <li>AM-02 Acceptable Use and Safe Handling of Assets Policy</li> <li>AM-06 Asset Classification and Labelling</li> <li>PI-02 Contractual agreements for the provision of data</li> <li>COM-01 Identification of applicable legal, regulatory, self-imposed or contractual requirements</li> </ul>

						<ul style="list-style-type: none"> <li>PSS-12 Locations of Data Processing and Storage</li> </ul>
A.4 Compliance	<ul style="list-style-type: none"> <li>GV.OC Organization al Context (GV-OC-03)</li> <li>GV.PO Policies, Processes, and Procedure (GV.PO-01)</li> </ul>	<ul style="list-style-type: none"> <li>4.3 Determining the scope of the information security management system</li> <li>4.4 Information security management system</li> </ul>	<ul style="list-style-type: none"> <li>5.31 Legal, statutory, regulatory, and contractual requirements</li> <li>5.36 Compliance with policies, rules and standards for information security</li> </ul>	<ul style="list-style-type: none"> <li>2.1 Include security during procurement and development processes (2.1.3)</li> </ul>	<ul style="list-style-type: none"> <li>GRC Governance, Risk and Compliance (GRC-05, GRC-07)</li> </ul>	<ul style="list-style-type: none"> <li>COM-01 Identification of applicable legal, regulatory, self-imposed or contractual requirements</li> <li>COM-03 Internal audits of the information security management system</li> </ul>
A.5 Documentation		<ul style="list-style-type: none"> <li>7.5 Documented information</li> </ul>	<ul style="list-style-type: none"> <li>5.37 Documented operating procedure</li> <li>6.8 Information security event reporting</li> </ul>		<ul style="list-style-type: none"> <li>BCR Business Continuity Management and Operational Resilience (BCR-05)</li> </ul>	<ul style="list-style-type: none"> <li>SP-01 Documentation, communication and provision of policies and instructions</li> <li>DEV-08 Version Control</li> </ul>

A.6 Notification			<ul style="list-style-type: none"> <li>6.8 Information security event reporting</li> </ul>	<ul style="list-style-type: none"> <li>1.3 Identify users and access requirements (1.3.3)</li> <li>4.1 Prepare the organisation for incidents (4.1.5)</li> <li>4.2 Assess and categorize incidents (4.2.3)</li> <li>4.3 Control and manage incidents (4.3.5)</li> </ul>		<ul style="list-style-type: none"> <li>SIM-01 Policy for security incident management</li> <li>SIM-04 Duty of the users to report security incidents to a central body</li> <li>SIM-05 Evaluation and learning process</li> <li>INQ-02 Informing Cloud Customers about Investigation Requests</li> </ul>
A.7 Audit	<ul style="list-style-type: none"> <li>ID.IM Improvement (ID.IM-02)</li> </ul>	<ul style="list-style-type: none"> <li>9.2.2 Internal audit program</li> </ul>	<ul style="list-style-type: none"> <li>5.35 Independent review of information security</li> <li>8.34 Protection of information systems during audit testing</li> </ul>		<ul style="list-style-type: none"> <li>A&amp;A Audit &amp; Assurance (A&amp;A-01, A&amp;A-04, A&amp;A-05)</li> <li>STA Supply Chain Management, Transparency, and Accountability (STA-11)</li> </ul>	<ul style="list-style-type: none"> <li>PI-02 Contractual agreements for the provision of data</li> <li>COM-02 Policy for planning and conducting audits</li> </ul>

					<ul style="list-style-type: none"><li>• SEF Security Incident Management, E-Discovery &amp; Cloud Forensics (SEF-08)</li></ul>	<ul style="list-style-type: none"><li>• COM-03 Internal audits of the information security management system</li><li>• INQ-01 Legal Assessment of Investigative Inquiries</li><li>• INQ-02 Informing Cloud Customers about Investigation Requests</li><li>• INQ-03 Conditions for Access to or Disclosure of Investigation Requests</li><li>• INQ-04 Limiting Access to or Disclosure of Data in Investigation Requests</li></ul>
--	--	--	--	--	--	---

A.8 Governance	<ul style="list-style-type: none"> <li>GV.RR Roles, Responsibilities, and Authorities (GV.RR-01, 02)</li> <li>GV.RM Risk Management Strategy (GV.RM-05)</li> <li>GV.SC Cybersecurity Supply Chain Risk Management (GV.SC-02)</li> </ul>	<ul style="list-style-type: none"> <li>5.1 Leadership and Commitment</li> <li>5.3 Organizational roles, responsibilities and authorities</li> <li>7.1 Resources</li> </ul>	<ul style="list-style-type: none"> <li>5.2 Information security roles and responsibilities</li> <li>5.3 Segregation of duties</li> </ul>	<ul style="list-style-type: none"> <li>1.3 Identify users and access requirements (1.3.3)</li> <li>4.1 Prepare the organisation for incidents (4.1.3)</li> </ul>	<ul style="list-style-type: none"> <li>GRC Governance, Risk and Compliance (GRC-06)</li> </ul>	<ul style="list-style-type: none"> <li>OIS-04 Segregation of Duties</li> <li>SP-01 Documentation, communication and provision of policies and instructions</li> <li>SP-02 Review and Approval of Policies and Instructions</li> <li>SP-03 Exceptions from Existing Policies and Instructions</li> <li>SSO-03 Directory of service providers and suppliers</li> </ul>
----------------	---	--	--	--	--	--

## 1.2 Basic Security Requirements Mapping Table

CRA Requirement	NIST CSF 2.0	ISO 27001:2022	ISO 27002:2022	NSM Grunnprinsipper for IKT-sikkerhet 2.1	CSA CCM V4.0.12	BSI C5:2020 (Cloud Computing Compliance Criteria Catalogue)
-----------------	--------------	----------------	----------------	---	-----------------	---



B.IS.1 Security Governance – Compliance with standards and frameworks	<ul style="list-style-type: none"> <li>GV.OC Organization al Context (GV.OC-03)</li> <li>GV.PO Policies, Processes, and Procedure (GV.PO-01)</li> </ul>	<ul style="list-style-type: none"> <li>8.1 Operationa l planning and control</li> </ul>	<ul style="list-style-type: none"> <li>5.31 Legal, statutory and contractual requirements</li> </ul>	<ul style="list-style-type: none"> <li>1.1 Identify management structures, deliverables and supporting systems (1.1.1)</li> </ul>	<ul style="list-style-type: none"> <li>GRC Governance, Risk and Compliance (GRC-05, GRC-07)</li> </ul>	<ul style="list-style-type: none"> <li>COM-01 Identification of applicable legal, regulator, self-imposed or contractual requirements</li> </ul>
B.IS.2 Security Governance – Information security managemen t system	<ul style="list-style-type: none"> <li>GV.PO Policies, Processes, and Procedures (GV.PO-01, 02)</li> </ul>	<ul style="list-style-type: none"> <li>4.3 Determinin g the scope of the informatio n security managemen t system</li> <li>4.4 Informatio n security managemen t system</li> </ul>	<ul style="list-style-type: none"> <li>5.36 Compliance with policies, rules, and standards for information security</li> </ul>	<ul style="list-style-type: none"> <li>1.1 Identify management structures, deliverables and supporting systems (1.1.2, 1.1.3)</li> </ul>	<ul style="list-style-type: none"> <li>GRC Governance, Risk and Compliance (GRC-01, GRC-03, GRC-04, GRC-05, GRC-07)</li> </ul>	<ul style="list-style-type: none"> <li>OIS-01 Information Security Management System (ISMS)</li> <li>OIS-02 Information Security Policy</li> <li>OIS-03 Interfaces and Dependencies</li> <li>OIS-06 Risk Management Policy</li> <li>OIS-07 Application of the Risk Management Policy</li> <li>COM-04 Information on information security</li> </ul>

						performance and management assessment of the ISMS •
B.IS.3 Security governance – Assurance			<ul style="list-style-type: none"> <li>GV.PO Policies, Processes, and Procedure (GV.PO-01)</li> </ul>	<ul style="list-style-type: none"> <li>2.1 Include security during procurement and development processes (2.1.3, 2.1.10)</li> </ul>	<ul style="list-style-type: none"> <li>GRC Governance, Risk and Compliance (GRC-07)</li> <li>A&amp;A Audit &amp; Assurance (A&amp;A-02, A&amp;A-03)</li> </ul>	<ul style="list-style-type: none"> <li>COM-03 Internal audits of the information security management system</li> <li>•</li> </ul>
B.IS.4 Security Governance – Security audit and testing obligations – regular security audits and testing	<ul style="list-style-type: none"> <li>ID.IM Improvement (ID.IM-01, 02, 03, 04)</li> </ul>	<ul style="list-style-type: none"> <li>9.2.2 Internal audit program</li> <li>9.2.1 Internal audit general</li> </ul>	<ul style="list-style-type: none"> <li>5.35 Independent review of information security</li> <li>8.34 Protection of information systems during audit testing</li> </ul>		<ul style="list-style-type: none"> <li>Audit &amp; Assurance (A&amp;A-02, A&amp;A-03, A&amp;A-05)</li> <li>STA Supply Chain Management, Transparency, and Accountability (STA-11)</li> </ul>	<ul style="list-style-type: none"> <li>COM-02 Policy for planning and conducting audits</li> <li>COM-03 Internal audits of the information security management system</li> </ul>
B.IS.5 Security governance – security audit and testing obligations –	<ul style="list-style-type: none"> <li>ID.IM Improvement (ID.IM-02, 03)</li> </ul>	<ul style="list-style-type: none"> <li>9.2.2 Internal audit program</li> <li>10.2 non-conformity and</li> </ul>	<ul style="list-style-type: none"> <li>5.35 Independent review of information security</li> <li>8.34 Protection of</li> </ul>		<ul style="list-style-type: none"> <li>A&amp;A Audit &amp; Assurance (A&amp;A-06)</li> </ul>	<ul style="list-style-type: none"> <li>COM-02 Policy for planning and conducting audits</li> <li>COM-03 Internal audits of the information</li> </ul>

documentation and remediation		<ul style="list-style-type: none"> <li>corrective action</li> <li>10.1 Continual improvement</li> </ul>	information systems during audit testing			security management system
B.IS.6 Security governance – Access to security documents		<ul style="list-style-type: none"> <li>5.2 Policy</li> <li>7.5 Documented information</li> </ul>	<ul style="list-style-type: none"> <li>5.1 Policies for information security</li> <li>5.37 Documented operating procedures</li> </ul>		<ul style="list-style-type: none"> <li>BCR Business Continuity Management and Operational Resilience (BCR-05)</li> </ul>	<ul style="list-style-type: none"> <li>OIS-02 Information Security Policy</li> <li>SP-02 Review and Approval of Policies and Instructions</li> <li>SP-03 Exceptions from Existing Policies and Instructions</li> </ul>
B.IS.7 Security governance – Third party security management – security requirements	<ul style="list-style-type: none"> <li>ID.IM Improvement (ID.IM-02)</li> <li>GV.SC Cybersecurity supply chain risk management (GV.SC-01 to 10)</li> </ul>		<ul style="list-style-type: none"> <li>8.26 Application security requirements</li> <li>5.19 Information security in supplier relationships</li> <li>5.21 Managing information security in the ICT supply chain</li> </ul>	<ul style="list-style-type: none"> <li>2.1 Include security during procurement and development processes (2.1.2, 2.1.3, 2.1.4, 2.1.9, 2.1.10,)</li> <li>4.1 Prepare the organisation for incidents (4.1.4)</li> </ul>	<ul style="list-style-type: none"> <li>STA Supply Chain Management, Transparency, and Accountability (STA-01 to STA-12)</li> <li>UEM Universal Endpoint Management (UEM-14)</li> </ul>	<ul style="list-style-type: none"> <li>HR-06 Confidentiality agreements</li> <li>DEV-01 Policies for the development / procurement of information systems</li> <li>DEV-02 Outsourcing of the development</li> <li>SSO-01 Policies and instructions for controlling</li> </ul>

			<ul style="list-style-type: none"> <li>• 5.20 Addressing information security within supplier agreements</li> <li>• 5.21 Managing information security in the ICT supply chain</li> <li>• 5.20 Addressing information security within supplier agreements</li> <li>• 6.6 Confidentiality or non-disclosure agreements</li> <li>• 8.30 Outsourced development</li> </ul>			<p>and monitoring third parties</p> <ul style="list-style-type: none"> <li>• SSO-02 Risk assessment of service providers and suppliers</li> <li>• SSO-03 Directory of service providers and suppliers</li> </ul>
B.IS.8 Security governance – Third party security			<ul style="list-style-type: none"> <li>• 5.22 Monitoring, review and change management</li> </ul>		<ul style="list-style-type: none"> <li>• DCS Data Center Security (DCS-02)</li> </ul>	<ul style="list-style-type: none"> <li>• SSO-04 Monitoring of compliance with requirements</li> </ul>

management ownership and operations of data centres and infrastructure			of supplier services			<ul style="list-style-type: none"> <li>PSS-12 Locations of Data Processing and Storage</li> </ul>
B.IS.9 Cooperation regarding information security – information security responsible	<ul style="list-style-type: none"> <li>GV.RR Roles, Responsibilities, and Authorities (GV.RR-01, 02, 03, 05)</li> </ul>	<ul style="list-style-type: none"> <li>5.1 Leadership and commitment</li> <li>5.3 Organizational roles, responsibilities, and authorities</li> <li>7.1 Resources</li> </ul>	<ul style="list-style-type: none"> <li>5.2 Information security roles and responsibilities</li> <li>5.3 Segregation of duties</li> </ul>	<ul style="list-style-type: none"> <li>1.3 Identify users and access requirements (1.3.3)</li> <li>4.1 Prepare the organisation for incidents (4.1.3)</li> </ul>	<ul style="list-style-type: none"> <li>GRC Governance, Risk and Compliance (GRC-06)</li> <li>SEF Security Incident Management, E-Discovery &amp; Cloud Forensics (SEF-08)</li> </ul>	
B.IS.10 Cooperation regarding information security - information security responsible – summoning meetings	<ul style="list-style-type: none"> <li>GV.RM Risk management strategy (GV.RM-05)</li> </ul>					

<p>B.IS.11 Incident, Asset and Vulnerability Management – Security incident management and threat intelligence – processes</p>	<ul style="list-style-type: none"> <li>• GV.RA Risk Assessment Strategy (GV.RM-05)</li> <li>• ID.RA Risk Assessment (ID.RA-04, 05)</li> <li>• ID.AE Adverse Event Analysis (DE.AE-02, 03, 04, 06, 08)</li> <li>• RS.MA Incident Management (RS.MA-01, 02, 03, 04, 05)</li> <li>• RS.AN Incident Analysis (RS.AN-03, 06, 07, 08)</li> <li>• RS.MI Incident Mitigation (RS.MI-01, 02)</li> <li>• RC.RP Incident</li> </ul>		<ul style="list-style-type: none"> <li>• 5.7 Threat intelligence</li> <li>• 5.24 Information security incident management planning and preparation</li> <li>• 5.25 Assessment and decision on information security events</li> <li>• 5.26 Response to information security incidents</li> </ul>	<ul style="list-style-type: none"> <li>• 1.1 Identify management structures, deliverables and supporting systems (1.1.3)</li> <li>• 2.1 Include security during procurement and development processes (2.1.10)</li> <li>• 3.3 Analyse data from security monitoring (3.3.6)</li> <li>• 4.1 Prepare the organisation for incidents (4.1.1, 4.1.2, 4.1.3, 4.1.4, 4.1.5, 4.1.6)</li> <li>• 4.2 Assess and categorize incidents</li> </ul>	<ul style="list-style-type: none"> <li>• SEF Security Incident Management, E-Discovery &amp; Cloud Forensics (SEF-01 to SEF-07)</li> </ul>	<ul style="list-style-type: none"> <li>• OPS-13 Logging and Monitoring – Identification of Events</li> <li>• SIM-01 Policy for security incident management</li> <li>• SIM-02 Processing of security incidents</li> <li>• SIM-03 Documentation and reporting of security incidents</li> <li>• SIM-05 Evaluation and learning process</li> </ul>
--	--	--	---	--	--	---

	Recovery Plan Execution (RC.RP-01 to 06)			<ul style="list-style-type: none"> <li>(4.2.1, 4.2.2, 4.2.3)</li> <li>• 4.3 Control and manage incidents (4.3.1, 4.3.2, 4.3.3, 4.3.5, 4.3.6)</li> <li>• 4.4 Evaluate and learn from incidents (4.4.1, 4.4.2, 4.4.3, 4.4.4)</li> </ul>		
B.IS.12 Incident, Asset and Vulnerability Management – Security incident management and threat intelligence – notification and documentation	<ul style="list-style-type: none"> <li>• DE.AE Adverse Event Analysis (DE.AE-04, 08)</li> <li>• RC.CO Incident Recovery Communication (RC.CO-04)</li> </ul>		<ul style="list-style-type: none"> <li>• 5.24 Information security incident management planning and preparation</li> <li>• 5.28 Collection of evidence</li> <li>• 6.8 Information security event reporting</li> </ul>	<ul style="list-style-type: none"> <li>• 1.3 Identify users and access requirements (1.3.3)</li> <li>• 3.3 Analyse data from security monitoring (3.3.6)</li> <li>• 4.1 Prepare the organisation for incidents (4.1.5)</li> <li>• 4.2 Assess and categorise incidents</li> </ul>	<ul style="list-style-type: none"> <li>• SEF Security Incident Management, E-Discovery &amp; Cloud Forensics (SEF-07)</li> </ul>	<ul style="list-style-type: none"> <li>• OPS-21 Involvement of Cloud customers in the event of incidents</li> <li>• SIM-01 Policy for security incident management</li> <li>• SIM-02 Processing of security incidents</li> <li>• SOM-03 Documentation and reporting of security incidents</li> <li>• SIM-04 Duty of the users to</li> </ul>

				(4.2.1, 4.2.2, 4.2.3, 4.3.5)		report security incidents to a central body <ul style="list-style-type: none"> <li>• INQ-02 Informing Cloud Customers about Investigation Requests</li> </ul>
B.IS.13 Incident, Asset and Vulnerability Management – Security incident management and threat intelligence – Cooperation	<ul style="list-style-type: none"> <li>• DE.AE Adverse Event Analysis (DE.AE-03, 06, 08)</li> <li>• GV.SC Cybersecurity Supply Chain Risk Management (GV.SC-08)</li> <li>• RS.MA Incident management (RS.MA-01)</li> <li>• RS.CO Incident Response Reporting and Communication (RS.CO-02, 03, 08)</li> </ul>			<ul style="list-style-type: none"> <li>• 1.3 Identify users and access requirements (1.3.3)</li> <li>• 2.1 Include security during procurement and development processes (2.1.10)</li> <li>• 3.3 Analyse data from security monitoring (3.3.6)</li> <li>• 4.1 Prepare the organisation for incidents (4.1.4, 4.1.4)</li> </ul>		



				<ul style="list-style-type: none"> <li>• 4.2 Assess and categorize incidents (4.2.3)</li> <li>• Control and manage incidents (4.3.5)</li> </ul>		
B.IS.14 Incident, Asset and Vulnerability Management – Security incident management and threat intelligence – Access to security logs	<ul style="list-style-type: none"> <li>• PR.PS Platform security (PR.PS-04)</li> </ul>		8.15 Logging	<ul style="list-style-type: none"> <li>• 3.2 Establish security monitoring (3.2.4)</li> <li>• 4.2 Assess and categorize incidents (4.2.1)</li> <li>• 4.3 Control and manage incidents (4.3.3)</li> </ul>		<ul style="list-style-type: none"> <li>• OPS-10 Logging and Monitoring – Concept</li> <li>• OPS-11 Logging and Monitoring – Metadata Management Concept</li> <li>• OPS-12 Logging and Monitoring – Access, Storage and Deletion</li> <li>• OPS-14 Logging and Monitoring – Storage of the Logging Data</li> <li>• OPS-15 Logging and Monitoring – Accountability</li> <li>• OPS-16 Logging and Monitoring – Configuration</li> <li>• PSS-01 Guidelines and</li> </ul>

						Recommendations for Cloud Customers
B.IS.15 Incident, Asset and Vulnerability Management - Security incident management and threat intelligence - Threat Intelligence	<ul style="list-style-type: none"> <li>ID.RA Risk Assessment (ID.RA-02, 03)</li> <li>DE.AE Adverse Event Analysis (DE.AE-07)</li> </ul>		8.7 Protection against malware	<ul style="list-style-type: none"> <li>3.1 Detect and remove known vulnerabilities and threats (3.1.2, 3.1.3)</li> <li>3.3 Analyse data from security monitoring (3.3.4)</li> </ul>		<ul style="list-style-type: none"> <li>OPS-04 Protection Against Malware – Concept</li> <li>OPS-05 Protection Against Malware - Implementation</li> </ul>
B.IS.16 Incident, Asset and Vulnerability Management - Security incident management and threat intelligence - Malicious Software	<ul style="list-style-type: none"> <li>ID.RA Risk Assessment (ID.RA-09)</li> </ul>		8.7 Protection against malware	<ul style="list-style-type: none"> <li>2.1 Include security during procurement and development processes (2.1.2, 2.1.3, 2.1.4)</li> <li>2.8 Protect email clients and browsers</li> </ul>	<ul style="list-style-type: none"> <li>TVM Threat &amp; Vulnerability Management (TVM-02)</li> </ul>	OPS-05 Protection Against Malware - Implementation

				<ul style="list-style-type: none"> <li>(2.8.3, 2.8.4)</li> <li>3.1 Detect and remove known vulnerabilities and threats (3.1.3)</li> </ul>		
B.IS-17 Incident, Asset and Vulnerability Management - Asset and Vulnerability Management – Asset Management	<ul style="list-style-type: none"> <li>ID.AM Asset Management (ID.AM-1,2,4,5, 7,8)</li> <li>PR.PS Platform Security (PR.PS-05)</li> <li>ID.RA Risk Assessment (ID.RA-09)</li> </ul>		<ul style="list-style-type: none"> <li>5.11 Return of assets</li> <li>7.9 Security of assets off-premises</li> <li>7.10 Storage media</li> <li>7.14 Secure disposal or re-use of equipment</li> <li>5.9 Inventory of informati</li> </ul>	<ul style="list-style-type: none"> <li>1.1 Identify management structures, deliverables and supporting systems (1.1.3)</li> <li>1.2 Identify devices and software (1.2.1, 1.2.2, 1.2.3, 1.2.4)</li> <li>Include security</li> </ul>	<ul style="list-style-type: none"> <li>HRS Human Resources (HRS-02, HRS-05)</li> <li>CCC Change Control and Configuration Management (CCC-04)</li> <li>DCS Data Center Security (DCS-01, DCS-04, DCS-05, DCS-06)</li> </ul>	<ul style="list-style-type: none"> <li>AM-01 Asset Inventory</li> <li>AM-02 Acceptable Use and Safe Handling of Assets Policy</li> <li>AM-03 Commissioning of Hardware</li> <li>AM-04 Decommissioning of Hardware</li> <li>AM-05 Commitment to Permissible Use, Safe Handling</li> </ul>

			<ul style="list-style-type: none"> <li>on and other associated assets</li> <li>5.10 Acceptable use of information and other associated assets</li> </ul>	<ul style="list-style-type: none"> <li>during procurement and development processes (2.1.1, 2.1.2, 2.1.3)</li> <li>2.2 Establish a secure ICT architecture (2.2.6)</li> <li>2.3 Maintain a secure configuration (2.3.10)</li> </ul>	<ul style="list-style-type: none"> <li>UEM Universal Endpoint Management (UEM-01, UEM-02, UEM-04)</li> <li>DSP Data Security and Privacy Lifecycle Management (DSP-02 to DSP-06)</li> </ul>	<ul style="list-style-type: none"> <li>and Return of Assets</li> <li>AM-06 Asset Classification and Labelling</li> <li>PI-03 Secure deletion of data</li> </ul>
B.IS.18 Incident, Asset and Vulnerability Management - Asset and Vulnerability Management – Vulnerability	<ul style="list-style-type: none"> <li>ID.RA Risk Assessment (ID.RA-01, 08)</li> </ul>		<ul style="list-style-type: none"> <li>8.8 Management of technical vulnerabilities</li> </ul>	<ul style="list-style-type: none"> <li>2.3 Maintain a secure configuration (2.3.1 to 2.3.10)</li> <li>2.5 Control data flow (2.5.4)</li> </ul>	<ul style="list-style-type: none"> <li>TVM Threat &amp; Vulnerability Management (TVM-01, TVM-03, TVM-07,</li> </ul>	<ul style="list-style-type: none"> <li>OPS-18 Managing Vulnerabilities, Malfunctions and Errors – Measurements, Analyses and Assessments</li> </ul>

Managemen t				<ul style="list-style-type: none"> <li>2.8 Protect email clients and browsers (2.8.3, 2.8.4)</li> <li>3.1 Detect and remove known vulnerabilities and threats (3.1.1)</li> </ul>	<ul style="list-style-type: none"> <li>TVM-08, TVM-10)</li> <li>AIS Application &amp; Interface Security (AIS-07)</li> </ul>	<ul style="list-style-type: none"> <li>of Procedures</li> <li>OPS-22 Testing and Documentation of known Vulnerabilities</li> <li>PSS-02 Identification of Vulnerabilities of the Cloud Service</li> </ul>
B.IS.19 Incident, Asset and Vulnerability Management - Asset and Vulnerability Management – third-party vulnerabilities	<ul style="list-style-type: none"> <li>ID.RA Risk Assessment (ID.RA-05)</li> </ul>	<ul style="list-style-type: none"> <li></li> </ul>	<ul style="list-style-type: none"> <li>8.16 Monitoring activities</li> <li>8.30 Outsourced development</li> </ul>	<ul style="list-style-type: none"> <li>3.1 Detect and remove known vulnerabilities and threats (3.1.2)</li> </ul>	<ul style="list-style-type: none"> <li>TVM Threat &amp; Vulnerability Management (TVM-01, TVM-05, TVM-10)</li> </ul>	
B.IS.20 Incident, Asset and Vulnerability					<ul style="list-style-type: none"> <li>TVM Threat &amp; Vulnerability Management</li> </ul>	<ul style="list-style-type: none"> <li>OPS-18 Managing Vulnerabilities, Malfunctions</li> </ul>

Managemen t - Asset and Vulnerability Managemen t – Vulnerability Identificatio n and Scoring					(TVM-01, TVM-09)	<p>and Errors – Concepts</p> <ul style="list-style-type: none"> <li>• OPS-20 Managing Vulnerabilities, Malfunctions and Errors – Measurements, Analyses and Assessments of Procedures</li> <li>• DEV-02 Outsourcing of the development</li> <li>• PSS-02 Identification of Vulnerabilities of the Cloud Service</li> <li>• PSS—03 Online Register of Known Vulnerabilities</li> </ul>
B.IS.21 Incident, Asset and Vulnerability Managemen t - Asset and Vulnerability Managemen t –	<ul style="list-style-type: none"> <li>• ID.RA Risk Assessment (ID.RA-05)</li> </ul>				<ul style="list-style-type: none"> <li>• TVM Threat &amp; Vulnerability Management (TVM-01, TVM-09)</li> </ul>	<ul style="list-style-type: none"> <li>• OPS-18 Managing Vulnerabilities, Malfunctions and Errors – Concepts</li> <li>• OPS-20 Managing Vulnerabilities, Malfunctions</li> </ul>

Vulnerability Notification						and Errors – Measurements, Analyses and Assessments of Procedures <ul style="list-style-type: none"> <li>• PSS-01 Guidelines and Recommendations for Cloud Customers</li> <li>• PSS-02 Identification of Vulnerabilities of the Cloud Service</li> <li>• PSS-03 Online Register of Known Vulnerabilities</li> </ul>
B.IS.22 Incident, Asset and Vulnerability Management - Suspension of service due to security incidents and vulnerabilities	<ul style="list-style-type: none"> <li>•</li> </ul>			<ul style="list-style-type: none"> <li>• 4.3 Control and manage incidents (4.3.2)</li> </ul>	<ul style="list-style-type: none"> <li>• TVM Threat &amp; Vulnerability Management (TVM-01)</li> </ul>	<ul style="list-style-type: none"> <li>• OPS-19 Managing Vulnerabilities, Malfunctions and Errors – Concept</li> <li>• OPS-20 Managing Vulnerabilities, Malfunctions and Errors – Measurements, Analyses and</li> </ul>

						Assessments of Procedures
B.IS.23 Incident, Asset and Vulnerability Management - Penetration testing rights	<ul style="list-style-type: none"> <li>ID.IM Improvement (ID.IM-02)</li> </ul>			<ul style="list-style-type: none"> <li>3.4 Perform penetration tests (3.4.1 to 3.4.6)</li> </ul>	<ul style="list-style-type: none"> <li>TVM Threat &amp; Vulnerability Management (TVM-06)</li> </ul>	
B.IS.24 Access Control and Customer Data – Security Access Management	<ul style="list-style-type: none"> <li>PR.AA Identity Management, Authentication, and Access Control (PR.AA-01, 02, 03, 04, 05)</li> <li>PR.IR Technology Infrastructure Resilience (PR.IR-01)</li> </ul>		<ul style="list-style-type: none"> <li>8.3 Information access restriction</li> <li>5.15 Access control</li> <li>5.17 Authentication information</li> <li>5.18 Access rights</li> <li>8.5 Secure authentication</li> <li>8.2 Privileged access rights</li> </ul>	<ul style="list-style-type: none"> <li>1.3 Identify users and access requirements (1.3.1 to 1.3.3)</li> <li>2.2 Establish a secure ICT architecture (2.2.6)</li> <li>2.3 Maintain a secure configuration (2.3.7, 2.3.10)</li> <li>2.4 Protect the organisation's networks (2.4.1, 2.4.2)</li> <li>2.6 Control identities and access rights (2.6.1 to 2.6.7)</li> </ul>	<ul style="list-style-type: none"> <li>IAM Identity &amp; Access Management (IAM-01 to IAM-07, IAM-09, IAM-10, IAM-13 to IAM-16)</li> <li>DCS Datacenter Security (DCS-08)</li> </ul>	<ul style="list-style-type: none"> <li>PS-04 Physical site access control</li> <li>OPS-06 Data Protection and Recovery</li> <li>OPS-12 Logging and Monitoring – Access, Storage and Deletion</li> <li>IDM-01 Policy for user accounts and access rights</li> <li>IDM-02 Granting and change of user accounts and access rights</li> <li>IDM-03 Locking and withdrawal of user accounts in the event of inactivity or</li> </ul>



						<ul style="list-style-type: none"><li>multiple failed loggings</li><li>• IDM-04 Withdraw or adjust access rights as the task area changes</li><li>• IDM-06 Privileged access rights</li><li>• IDM-08 Confidentiality of authentication information</li><li>• IDM-09 Authentication mechanisms</li><li>• PSS-01 Guidelines and Recommendations for Cloud Customers</li><li>• PSS-05 Authentication Mechanisms</li><li>• PSS-08 Roles and Rights Concept</li><li>• PSS-09 Authorisation Mechanisms</li></ul>
--	--	--	--	--	--	--

B.IS.25 Access Control and Customer Data – Security Access Management – Regular Access Reviews				<ul style="list-style-type: none"> <li>2.6 Control identities and access rights (2.6.1)</li> <li></li> </ul>	<ul style="list-style-type: none"> <li>IAM Identity &amp; Access Management (IAM-01, IAM-08)</li> </ul>	<ul style="list-style-type: none"> <li>IDM-05 Regular review of access rights?</li> </ul>
B.IS.26 Access Control and Customer Data - Flexible and fine-grained identity and access management – Customer Identity and Access Management	<ul style="list-style-type: none"> <li>PR.AA Identity Management, Authentication, and Access Control (PR.AA-01 to 04)</li> </ul>		<ul style="list-style-type: none"> <li>5.18 Access Rights</li> <li>8.2 Privileged access rights</li> </ul>	<ul style="list-style-type: none"> <li>1.3 Identify users and access requirements (1.3.1)</li> </ul>	<ul style="list-style-type: none"> <li>IAM Identity &amp; Access Management (IAM-01 to IAM-07, IAM-09 to IAM-11, IAM-13 to IAM-16)</li> <li>DCS Data Center Security (DCS-08)</li> </ul>	<ul style="list-style-type: none"> <li>IDM-02 Granting and change of user accounts and access rights</li> <li>IDM-03 Locking and withdrawal of user accounts in the event of inactivity or multiple failed logins</li> <li>IDM-04 Withdraw or adjust access rights as the task area changes</li> <li>IDM-05 Regular review of access rights</li> <li>IDM-06 Privileged access rights</li> </ul>

B.IS.27 Access Control and Customer Data - Flexible and fine-grained identity and access management – Standards for Cross-domain Identity Management			<ul style="list-style-type: none"> <li>• 5.23 Information security for use of cloud services</li> <li>• 5.18 Use of privileged utility programs</li> <li>• 8.20 Networks security</li> <li>• 8.24 Use of cryptography</li> <li>• 5.17 Authentication information</li> <li>• 8.5 Secure authentication</li> <li>• 8.20 Networks security</li> </ul>		<ul style="list-style-type: none"> <li>• IAM Identity &amp; Access Management (IAM-01, IAM-04)</li> </ul>	
B.IS.28 Access Control and Customer Data – Secure Remote Access	<ul style="list-style-type: none"> <li>• DE.CM Continuous Monitoring (DE.CM-01, 03, 06, 09)</li> </ul>	<ul style="list-style-type: none"> <li>• 9.1 Monitoring, measurement, analysis and evaluation</li> </ul>	<ul style="list-style-type: none"> <li>• 5.17 Authentication information</li> <li>• 8.5 Secure authentication</li> <li>• 6.7 Remote working</li> </ul>	<ul style="list-style-type: none"> <li>• 2.3 Maintain a secure configuration (2.3.10)</li> <li>• 2.4 Protect the organisation's networks (2.4.1, 2.4.2, 2.4.4)</li> </ul>	<ul style="list-style-type: none"> <li>• HRS Human Resources (HRS-04)</li> <li>• IVS Infrastructure &amp; Virtualization Security (IVS-03, IVS-07, IVS-09)</li> </ul>	<ul style="list-style-type: none"> <li>• IDM-08 Confidentiality of authentication information</li> <li>• IDM-09 Authentication mechanisms</li> </ul>

			<ul style="list-style-type: none"> <li>8.20 Networks security</li> <li>8.21 Security of network services</li> </ul>	<ul style="list-style-type: none"> <li>2.5 Control data flow (2.5.2, 2.5.5, 2.5.7)</li> </ul>		<ul style="list-style-type: none"> <li>COS-01 Technical safeguards</li> <li>COS-03 Monitoring of connections in the Cloud Service Provider's network</li> <li>COS-04 Cross-network access</li> <li>PSS-01 Guidelines and Recommendations for Cloud Customers</li> <li>PSS-05 Authentication Mechanisms</li> <li>PSS-07 Confidentiality of Authentication Information</li> <li>PSS-08 Roles and Rights - Concept</li> </ul>
B.IS.29 Access Control and Customer Data -	<ul style="list-style-type: none"> <li>PR.DS Data Security (PR.DS-05, 09)</li> </ul>		<ul style="list-style-type: none"> <li>8.12 Data leakage prevention</li> </ul>	<ul style="list-style-type: none"> <li>1.1 Identify management structures, deliverables and</li> </ul>	<ul style="list-style-type: none"> <li>DSP Data Security and Privacy Lifecycle</li> </ul>	<ul style="list-style-type: none"> <li>PS-04 Physical site access control</li> </ul>

Separation of Customer Data			<ul style="list-style-type: none"> <li>8.22 Segregation of Networks</li> </ul>	<p>supporting systems (1.1.6)</p> <ul style="list-style-type: none"> <li>2.1 Include security during procurement and development of processes (2.1.10)</li> <li>2.2 Establish a secure ICT architecture (2.2.3)</li> <li>2.3 Maintain a secure configuration (2.3.10)</li> <li>2.5 Control data flow (2.5.1)</li> </ul>	<p>Management (DSP-01)</p> <ul style="list-style-type: none"> <li>AIS Application &amp; Interface Security (AIS-01, AIS-03)</li> <li>IVS Infrastructure &amp; Virtualization Security (IVS-06)</li> </ul>	<ul style="list-style-type: none"> <li>OPS-15 Logging and Monitoring – Accountability</li> <li>OPS-24 Separation of Datasets in the Cloud Infrastructure</li> <li>IDM-07 Access to cloud customer data</li> <li>COS-01 Technical safeguards</li> <li>COS-02 Security requirements for connections in the Cloud Service Provider’s network</li> <li>COS-04 Cross-network access</li> <li>COS-05 Networks for administration</li> <li>COS-06 Segregation of data traffic in jointly used network environments</li> </ul>
-----------------------------	--	--	--	---	---	--

						<ul style="list-style-type: none"> <li>• COS-08 Policies for data transmission</li> </ul>
B.IS.30 Access Control and Customer Data - Encryption of Customer Data – Protection of Customer Data	<ul style="list-style-type: none"> <li>• ID.AM Asset Management (ID.AM-3)</li> <li>• PR.DS Data Security (PR.DS-01, 02, 05)</li> </ul>		<ul style="list-style-type: none"> <li>• 5.33 Protection of records</li> <li>• 5.34 Privacy and protection of PII</li> <li>• 8.24 Use of cryptography</li> <li>• 8.18 Use of privileged utility programs</li> <li>• 8.20 Networks security</li> </ul>	<ul style="list-style-type: none"> <li>• 2.5 Control data flow (2.5.6)</li> <li>• 2.7 Protect data at rest and in transit (2.7.1 to 2.7.5)</li> <li>• 2.9 Establish capability to restore data (2.9.4)</li> </ul>	<ul style="list-style-type: none"> <li>• CEK Cryptography , Encryption &amp; Key Management (CEK-03)</li> <li>• DCS Data Center Security (DCS-02)</li> <li>• UEM Universal Endpoint Management (UEM-08, UEM-11)</li> <li>• DSP Data Security and Privacy Lifecycle Management (DSP-01, DSP-10, DSP-17)</li> </ul>	<ul style="list-style-type: none"> <li>• OPS-06 Data Protection and Recovery – Concept</li> <li>• OPS-16 Logging and Monitoring – Configuration</li> <li>• IDM-07 Access to cloud customer data</li> <li>• CRY-01 Policy for the use of encryption procedures and key management</li> <li>• CRY-02 Encryption of data for transmission (transport encryption)</li> <li>• CRY-03 Encryption of sensitive data for storage</li> <li>• CRY-04 Secure key management</li> </ul>

						<ul style="list-style-type: none"> <li>• PSS-01 Guidelines and Recommendations for Cloud Customers</li> <li>• PSS-05 Authentication Mechanisms</li> <li>• PSS-07 Confidentiality of Authentication Information</li> <li>• PSS-08 Roles and Rights Concept</li> </ul>
B.IS.31 Encryption of Customer Data – State of the Art Encryption			<ul style="list-style-type: none"> <li>• 8.20 Network security</li> <li>• 8.24 Use of cryptography</li> <li>• 5.17 Authentication information</li> <li>• 8.5 Secure authentication</li> </ul>	<ul style="list-style-type: none"> <li>• 2.4 Protect the organisation's networks (2.4.2)</li> <li>• 2.7 Protect data at rest and in transit (2.7.1 to 2.7.4)</li> </ul>	<ul style="list-style-type: none"> <li>• CEK Cryptography, Encryption &amp; Key Management (CEK-01 to CEK-21)</li> <li>• LOG Logging and Monitoring (LOG-10, LOG-11)</li> </ul>	<ul style="list-style-type: none"> <li>• OPS-06 Data Protection and Recovery – Concept</li> <li>• CRY-01 Policy for the use of encryption procedures and key management</li> <li>• CRY-02 Encryption of data for transmission (transport encryption)</li> </ul>

						<ul style="list-style-type: none"> <li>CRY-03 Encryption of sensitive data for storage</li> <li>CRY-04 Secure key management</li> </ul>
B.IS.32 Access Control and Customer Data - Encryption of Customer Data – Quantum Resistant Cryptographic Algorithms			<ul style="list-style-type: none"> <li>8.24 Use of cryptography</li> </ul>		<ul style="list-style-type: none"> <li>CEK Cryptography , Encryption &amp; Key Management (CEK-07)</li> </ul>	<ul style="list-style-type: none"> <li>OPS-06 Data Protection and Recovery – Concept</li> <li>CRY-01 Policy for the use of encryption procedures and key management</li> <li>CRY-02 Encryption of data for transmission (transport encryption)</li> <li>CRY-03 Encryption of sensitive data for storage</li> <li>CRY-04 Secure key management</li> </ul>
B .IS.33 Access Control and	PR.PS Platform Security (PR.PS-04)		<ul style="list-style-type: none"> <li>8.5 Secure authentication</li> </ul>	<ul style="list-style-type: none"> <li>3.2 Establish security</li> </ul>	<ul style="list-style-type: none"> <li>LOG Logging and monitoring</li> </ul>	<ul style="list-style-type: none"> <li>OPS-10 Logging and Monitoring – Concept</li> </ul>



Customer Data - Logging of access to Customer Data			<ul style="list-style-type: none"> <li>8.15 Logging</li> </ul>	monitoring (3.2.1 to 3.2.7)	(LOG-01 to LOG-05, LOG-07 to LOG-09, LOG-12, LOG-13) <ul style="list-style-type: none"> <li>IAM Identity &amp; Access Management (IAM-12)</li> <li>DSP Data Security and Privacy Lifecycle Management (DSP-01)</li> </ul>	<ul style="list-style-type: none"> <li>OPS-11 Logging and Monitoring – Metadata Management Concept</li> <li>OPS-12 Logging and Monitoring – Access, Storage and Deletion</li> <li>OPS-14 Logging and Monitoring – Storage of the Logging Data</li> <li>OPS-15 Logging and Monitoring – Accountability</li> <li>OPS-16 Logging and Monitoring – Configuration</li> <li>IDM-07 Access to cloud customer data</li> <li>PSS-04 Error handling and Logging Mechanisms</li> <li></li> </ul>
B.IS.34 Access Control and Customer Data - Logging of			<ul style="list-style-type: none"> <li>8.10 Information deletion</li> <li>8.15 Logging</li> </ul>	<ul style="list-style-type: none"> <li>3.2 Establish security monitoring (3.2.2)</li> </ul>		<ul style="list-style-type: none"> <li>AM-04 Decommissioning of Hardware</li> <li>OPS-10 Logging and Monitoring – Concept</li> </ul>

access to Customer Data – Retention Period						<ul style="list-style-type: none"> <li>• OPS-11 Logging and Monitoring – Metadata Management Concept</li> <li>• OPS-12 Logging and Monitoring – Access, Storage and Deletion</li> <li>• OPS-14 Logging and Monitoring – Storage of the Logging Data</li> <li>• OPS-15 Logging and Monitoring Accountability</li> <li>• OPS-16 Logging and Monitoring – Configuration</li> <li>• PI-02 Contractual agreements for the provision of data</li> </ul>
B.IS.35 Access Control and Customer Data - Notification of relocation of Customer Data			<ul style="list-style-type: none"> <li>• 5.14 Information transfer</li> </ul>		<ul style="list-style-type: none"> <li>• DCS Data Center security (DCS-02)</li> <li>• DSP Data Security and Privacy Lifecycle Management (DSP-01)</li> </ul>	<ul style="list-style-type: none"> <li>• IDM-07 Access to cloud customer data</li> <li>• COS-08 Policies for data transmission</li> <li>• PSS-12 Locations of Data Processing and Storage</li> </ul>
B.IS.36 Change Managemen			<ul style="list-style-type: none"> <li>• 8.32 Change Management</li> </ul>	<ul style="list-style-type: none"> <li>• 2.3 Maintain a secure</li> </ul>	<ul style="list-style-type: none"> <li>• CCC Change Control and Configuration</li> </ul>	<ul style="list-style-type: none"> <li>• DEV-03 Policies for changes to</li> </ul>

t and Security by Design – Change Management				<ul style="list-style-type: none"> <li>configuration (2.3.5)</li> <li>2.10 Include security in the change management process (2.10.1 to 2.10.4)</li> <li></li> </ul>	Management (CCC-01 to CCC-05, CCC-07 to CCC-09) <ul style="list-style-type: none"> <li>CEK Cryptography , Encryption &amp; Key Management (CEK-05)</li> <li>Universal Endpoint Management (UEM-02, UEM-07)</li> <li>IVS Infrastructure &amp; Virtualization Security (IVS-05)</li> <li>AIS Application &amp; Interface Security (AIS, 04, AIS-06)</li> </ul>	information systems <ul style="list-style-type: none"> <li>DEV-05 Risk assessment, categorisation and prioritisation of changes</li> <li>DEV-06 Testing changes</li> <li>DEV-07 Logging of changes</li> <li>DEV-08 Version Control</li> <li>DEV-09 Approvals of provision in the production environments</li> </ul>
B.IS.37 Change Management and Security by Design – Change			<ul style="list-style-type: none"> <li>8.32 Change Management</li> <li>6.3 Planning of Changes</li> </ul>		<ul style="list-style-type: none"> <li>CCC Change Control and Configuration Management (CCC-02)</li> </ul>	<ul style="list-style-type: none"> <li>DEV-03 Policies and changes to information systems</li> <li>DEV-05 Risk assessment, categorisation</li> </ul>

Management – Advance Notice						and prioritisation of changes <ul style="list-style-type: none"> <li>• DEV-06 Testing changes</li> <li>• DEV-07 Logging of changes</li> <li>• DEV-08 Version control</li> <li>• DEV-09 Approvals for provision in the production environment</li> </ul>
B.IS.38 Change Management and Security by Design – Security by Design	ID.RA Risk Assessment (ID.RA-09)		<ul style="list-style-type: none"> <li>• 8.9 Configuration management</li> <li>• 8.26 Application security requirements</li> <li>• 8.27 Secure system architecture and engineering principles</li> <li>• 8.25 Secure development life cycle</li> <li>• 5.8 Information security in</li> </ul>	<ul style="list-style-type: none"> <li>• 2.1 Include security during procurement and development processes (2.1.5, 2.1.6, 2.1.8)</li> <li>• 2.3 Maintain a secure configuration (2.3.1 to 2.3.10)</li> <li>• 2.8 Protect email clients and browsers (2.8.1 to 2.8.4)</li> </ul>	<ul style="list-style-type: none"> <li>• UEM Universal Endpoint Management (UEM-02, UEM-03, UEM-05, UEM-06, UEM-08 to UEM-13)</li> <li>• CCC Change Control and Configuration Management (CCC-06)</li> <li>• IVS Infrastructure &amp; Virtualization</li> </ul>	<ul style="list-style-type: none"> <li>• AM-03 Commissioning of Hardware</li> <li>• OPS-16 Logging and Monitoring – Configuration</li> <li>• OPS-23 Managing Vulnerabilities, Malfunctions and Errors – System Hardening</li> <li>• COS-03 Monitoring of connections in the Cloud Service</li> </ul>

			project management		Security (IVS-04) <ul style="list-style-type: none"> <li>• AIS Application &amp; Interface Security (AIS-02)</li> <li>• LOG Logging and Monitoring (LOG-06)</li> </ul>	Provider's network <ul style="list-style-type: none"> <li>• COS-07 Documentation of the network topology</li> <li>• PI-01 Documentation and safety of input and output interfaces</li> <li>• DEV-01 Policies for the development / procurement of information systems</li> <li>• PSS-01 Guidelines and Recommendations for Cloud Customers</li> </ul>
B.IS.39 Change Management and Security by Design – Security by Design – Testing	ID.IM Improvement (ID.IM-02)		<ul style="list-style-type: none"> <li>• 8.25 Secure development life cycle</li> <li>• 8.29 Security testing in development and acceptance</li> <li>• 8.33 Test information</li> </ul>	<ul style="list-style-type: none"> <li>• 2.1 Include security during procurement and development processes (2.1.6, 2.1.7)</li> </ul>	<ul style="list-style-type: none"> <li>• AIS Application &amp; Interface Security (AIS-05)</li> <li>• CCC Change Control and Configuration Management (CCC-02)</li> </ul>	<ul style="list-style-type: none"> <li>• DEV-01 Policies for the development / procurement of information systems</li> <li>• DEV-02 Outsourcing of the development</li> <li>• DEV-06 Testing changes</li> </ul>

B.IS.40 Change Management and Security by Design – Standards and Best Practices			<ul style="list-style-type: none"> <li>8.4 Access to source code</li> <li>8.27 Secure system architecture and engineering principles</li> <li>8.28 Source coding</li> </ul>	<ul style="list-style-type: none"> <li>2.1 Include security during procurement and development processes (2.1.4, 2.1.5, 2.1.8)</li> </ul>	<ul style="list-style-type: none"> <li>CCC Change Control and Configuration Management (CCC-06)</li> <li>IVS Infrastructure &amp; Virtualization Security (IVS-04)</li> <li>DSP Data Security and Privacy Lifecycle Management (DSP-07, DSP-08)</li> </ul>	<ul style="list-style-type: none"> <li>DEV-01 Policies for the development/ procurement of information systems</li> </ul>
B.IS.41 Business Continuity – Business Continuity and Disaster Recovery	<ul style="list-style-type: none"> <li>PR.IR Technology Infrastructure Resilience (PR.IR-03)</li> </ul>		<ul style="list-style-type: none"> <li>8.14 Redundancy of information processing facilities</li> <li>5.29 Information security during disruption</li> <li>5.30 ICT readiness for business continuity</li> </ul>	<ul style="list-style-type: none"> <li>4.1 Prepare the organisation for incidents (4.1.2, 4.1.6)</li> <li>4.3 Control and manage incidents (4.3.1, 4.3.2)</li> </ul>	<ul style="list-style-type: none"> <li>BCR Business Continuity Management and Operational Resilience (BCR-01, BCR-03 to BCR-07, BCR-09, BCR-10)</li> </ul>	<ul style="list-style-type: none"> <li>PS-02 Redundancy model</li> <li>OPS-06 Data Protection and Recovery – Concept</li> <li>OPS-07 Data Backup and Recovery – Monitoring</li> <li>OPS-09 Data Backup and Recovery – Storage</li> </ul>

						<ul style="list-style-type: none"> <li>• OPS-17 Logging and Monitoring – Availability of the Monitoring Software</li> <li>• BCM-01 Top management responsibility</li> <li>• BCM-02 Business impact analysis policies and instructions</li> <li>• BCM-03 Planning business continuity</li> <li>• BCM-04 Verification, updating of the business continuity</li> </ul>
B.IS.42 Business Continuity – Business Continuity and Disaster Recovery – Capacity Management	PR.IR Technology Infrastructure Resilience		<ul style="list-style-type: none"> <li>• 8.6 Capacity Management</li> </ul>	<ul style="list-style-type: none"> <li>• 2.2 Establish a secure ICT architecture (2.2.7)</li> </ul>	<ul style="list-style-type: none"> <li>• IVS Infrastructure &amp; Virtualization Security (IVS-02)</li> <li>• BCR Business Continuity Management and Operational Resilience (BCR-11)</li> </ul>	<ul style="list-style-type: none"> <li>• OPS-01 Capacity Management – Planning</li> <li>• OPS-02 Capacity Management – Monitoring</li> <li>• OPS-03 Capacity Management – Controlling and Resources</li> </ul>

B.IS.43 Business Continuity – Backup and Restore of the Supplier’s Systems	<ul style="list-style-type: none"> <li>• PR.DS Data Security (PR.DS-11)</li> <li>• RC.RP Incident Recovery Plan Execution (RC.RP-03)</li> </ul>		<ul style="list-style-type: none"> <li>• 8.13 Information backup</li> </ul>	<ul style="list-style-type: none"> <li>• 2.9 Establish capability to restore data (2.9.1 to 2.9.4)</li> </ul>	BCR Business Continuity Management and Operational Resilience (BCR-08)	<ul style="list-style-type: none"> <li>• OPS-06 Data Protection and Recovery – Concept</li> <li>• OPS-07 Data Backup and Recovery – Monitoring</li> <li>• OPS-08 Data Backup and Recovery – Regular Testing</li> <li>• OPS-09 Data Backup and Recovery - Storage</li> </ul>
B.IS.44 Physical and Personnel Security – Physical Security	<ul style="list-style-type: none"> <li>• PR.AA Identity Management , Authenticati on, and Access Control (PR.AA-06)</li> <li>• PR.IR Technology Infrastructur e Resilience (PR.IR-02)</li> <li>• DE.CM Continuous Monitoring</li> </ul>		<ul style="list-style-type: none"> <li>• 7.13 Equipment maintenance</li> <li>• 8.1 User endpoint devices</li> <li>• 7.1 Physical security perimeters</li> <li>• 7.5 Protecting against physical and environmenta l threats</li> <li>• 7.2 Physical entry</li> </ul>	<ul style="list-style-type: none"> <li>• 2.1 Include security during procurement and development processes (2.1.4)</li> <li>• 2.4 Protect the organisation’ s networks (2.4.2, 2.4.3)</li> </ul>	DCS Data Center Security (DCS-03, DCS-07, DCS-09 to DCS-15)	<ul style="list-style-type: none"> <li>• PS-01 Physical Security and Environmental Control Requirements</li> <li>• PS-03 Perimeter Protection</li> <li>• PS-04 Physical site access control</li> <li>• PS-05 Protection against threats from outside and from the environment</li> <li>• PS-06 Protection against</li> </ul>



	(DE.CM-02, 03)		<ul style="list-style-type: none"> <li>• 7.3 Securing offices, rooms and facilities</li> <li>• 7.6 Working in secure areas</li> <li>• 7.8 Equipment siting and protection</li> <li>• 7.11 Supporting utilities</li> <li>• 7.12 Cabling security</li> <li>• 7.4 Physical security monitoring</li> </ul>			interruptions caused by power failures and other such risks
B.IS.45 Physical and Personnel Security – Physical Security – Audits	<ul style="list-style-type: none"> <li>• ID.IM Improvement (ID.IM-01, 02)</li> </ul>				<ul style="list-style-type: none"> <li>• A&amp;A Audit &amp; Assurance (A&amp;A-02, A&amp;A-03)</li> </ul>	<ul style="list-style-type: none"> <li>• PS-01 Physical Security and Environmental Control Requirements</li> </ul>
B.IS.46 Physical and Personnel Security – Personnel Security	<ul style="list-style-type: none"> <li>• GV.RR Roles, Responsibilities, and Authorities (GV.RR-04)</li> <li>• PR.AT Awareness and Training</li> </ul>	<ul style="list-style-type: none"> <li>• 7.2 Competence</li> <li>• 7.3 Awareness</li> </ul>	<ul style="list-style-type: none"> <li>• 5.4 Management responsibilities</li> <li>• 6.3 Information security awareness,</li> </ul>		<ul style="list-style-type: none"> <li>• DCS Data Center Security (DCS-11)</li> <li>• HRS Human Resources (HRS-03, HRS-05 to HRS-13)</li> </ul>	<ul style="list-style-type: none"> <li>• HR-02 Employment terms and conditions</li> <li>• HR-03 Security training and awareness programme</li> </ul>

	(PR.AT-01, 02)		<ul style="list-style-type: none"> <li>education and training</li> <li>6.6 Confidentiality or non-disclosure agreements</li> <li>6.2 Terms and conditions of employment</li> <li>6.5 Responsibilities after termination or change of employment</li> <li>6.4 Disciplinary process</li> </ul>			<ul style="list-style-type: none"> <li>HR-04 Disciplinary measures</li> <li>HR-05 Responsibilities in the event of termination or change of employment</li> <li>HR-06 Confidentiality agreement</li> <li>DEV-04 Safety training and awareness programme regarding continuous software delivery and associated systems, components or tools.</li> <li>SSO-01 Policies and instructions for controlling and monitoring third parties.</li> </ul>
B.IS.47 Physical and Personnel Security – Personnel	<ul style="list-style-type: none"> <li>GV.RR Roles, Responsibilities, and Authorities (GV.RR-04)</li> </ul>		<ul style="list-style-type: none"> <li>6.1 Screening</li> </ul>		<ul style="list-style-type: none"> <li>HRS Human Resources (HRS-01)</li> </ul>	<ul style="list-style-type: none"> <li>HR-01 Verification of qualifications and trustworthiness</li> </ul>

Security – Security Screening and Clearance						
B.IS.48 Physical and Personnel Security – Personnel Security – Audits	<ul style="list-style-type: none"> <li>ID.IM Improvement (ID.IM-02)</li> </ul>				<ul style="list-style-type: none"> <li>A&amp;A Audit &amp; Assurance (A&amp;A-02, A&amp;A-03)</li> </ul>	

### 1.3 Cloud Enablement Security Requirements Mapping Table

CSRA Requirement	NIST CSF 2.0	ISO 27001:2022	ISO 27002:2022	NSM Grunnprinsipper for IKT-sikkerhet 2.1	CSA CCM V4.0.12	BSI C5:2020 (Cloud Computing Compliance Criteria Catalogue)
C.1 Security Architecture			<ul style="list-style-type: none"> <li>8.27 Secure system architecture and engineering principles</li> </ul>	<ul style="list-style-type: none"> <li>Identify management structures, deliverables and supporting systems (1.1.5, 1.1.-6)</li> <li>2.1 Include security during procureme</li> </ul>	<ul style="list-style-type: none"> <li>IVS Infrastructure &amp; Virtualization Security (IVS-08, IVS-09,</li> </ul>	<ul style="list-style-type: none"> <li>DEV-01 Policies for the development/ procurement of information systems</li> <li>PSS-06 Session management</li> <li>PSS-10 Software-defined networking</li> <li>PSS-11 Images for Virtual</li> </ul>

				nt and developme nt processes (2.1.1, 2.1.10) <ul style="list-style-type: none"> <li>• 2.2 Establish a secure ICT architecture (2.2.1 to 2.2.7)</li> <li>• 2.5 Control data flow (2.5.3, 2.5.8)</li> <li>• 3.3 Analyse data from security monitoring (3.3.1 to 3.3.7)</li> </ul>		Machines and Containers
C.2 Secure Cloud Adoption	PR.PS Platform Security (PR.PS-01, 02, 03, 06)		<ul style="list-style-type: none"> <li>• 8.9 Configurati on manageme nt</li> <li>• 5.23 Information security for use of cloud services</li> </ul>	<ul style="list-style-type: none"> <li>• 1.1 Identify manageme nt structures, deliverable s and supporting systems (1.1.5)</li> <li>• 2.1 Include security</li> </ul>	<ul style="list-style-type: none"> <li>• IVS Infrastructur e &amp; Virtualization Security (IVS-01)</li> </ul>	<ul style="list-style-type: none"> <li>• AM-03 Commissioning of Hardware</li> <li>• AM-04 Decommissioning of Hardware</li> <li>• OPS-16 Logging and Monitoring – Configuration</li> <li>• OPS-23 Managing Vulnerabilities</li> </ul>

			<ul style="list-style-type: none"> <li>• 8.25 Secure development life cycle</li> <li>• 8.31 Separation of development, test, and production environments</li> </ul>	<p>during procurement and development processes (2.1.1, 2.1.6)</p> <ul style="list-style-type: none"> <li>• 2.3 Maintain a secure configuration (2.3.1)</li> </ul>		<p>and Errors – System Hardening</p> <ul style="list-style-type: none"> <li>• COS-03 Monitoring of connections in the Cloud Service Provider's Network</li> <li>• PI-01 Documentation and safety of input and output interfaces</li> <li>• DEV-01 Policies for the development/ procurement of information systems</li> <li>• DEV-10 Separation of environments</li> <li>• SSO-05 Exist strategy for the receipt of benefits</li> <li>• PSS-01 Guidelines and Recommendations for Cloud Customers</li> </ul>
--	--	--	---	--	--	--

C.3 Governance and Compliance Dashboard		<ul style="list-style-type: none"> <li>5.2 Policy</li> <li>7.4 Communication</li> </ul>				
C4 Governance and Compliance Matrix – International Standards and Frameworks	<ul style="list-style-type: none"> <li>GV.OC Organizational Context (GV.OC-03)</li> </ul>	<ul style="list-style-type: none"> <li>8.1 Operational planning and control</li> </ul>	<ul style="list-style-type: none"> <li>5.31 Legal, statutory, regulatory and contractual requirements</li> </ul>		<ul style="list-style-type: none"> <li>GRC Governance, Risk and Compliance (GRC-07)</li> </ul>	<ul style="list-style-type: none"> <li>COM-01 Identification of applicable legal, regulatory, self-imposed or contractual requirements</li> </ul>
C5 Governance and Compliance Matrix – National Standards and Frameworks	<ul style="list-style-type: none"> <li>GV.OC Organizational Context (GV.OC-03)</li> </ul>	<ul style="list-style-type: none"> <li>8.1 Operational planning and control</li> </ul>	<ul style="list-style-type: none"> <li>5.31 Legal, statutory, regulatory and contractual requirements</li> </ul>		<ul style="list-style-type: none"> <li>GRC Governance, Risk and Compliance (GRC-07)</li> </ul>	<ul style="list-style-type: none"> <li>COM-01 Identification of applicable legal, regulatory, self-imposed or contractual requirements</li> </ul>
C.6 Security in multi-cloud and hybrid cloud environments			<ul style="list-style-type: none"> <li>8.7 Protection against malware</li> </ul>	<ul style="list-style-type: none"> <li>1.1 Identify management structures, deliverables and supporting systems (1.1.5)</li> </ul>	<ul style="list-style-type: none"> <li>IPY Interoperability &amp; Portability (IPY-01 to IPY-04)</li> </ul>	<ul style="list-style-type: none"> <li>OPS-05 Protection Against Malware - Implementation</li> </ul>

				<ul style="list-style-type: none"> <li>2.2 Establish a secure ICT architecture (2.2.2)</li> </ul>		
C.7 Cryptography			<ul style="list-style-type: none"> <li>8.24 Use of cryptography</li> </ul>	<ul style="list-style-type: none"> <li>2.7 Protect data at rest and in transit (2.7.1 to 2.7.5)</li> <li>2.9 Establish capability to restore data (2.9.5)</li> </ul>	<ul style="list-style-type: none"> <li>CEK Cryptography, Encryption &amp; Key Management (CEK-07)</li> </ul>	<ul style="list-style-type: none"> <li>OPS-06 Data Protection and Recovery – Concept</li> <li>IDM-07 Access to cloud customer data</li> <li>CRY-01 Policy for the use of encryption procedures and key management</li> <li>CRY-02 Encryption of data for transmission (transport encryption)</li> <li>CRY-03 Encryption of sensitive data for storage</li> <li>CRY-04 Secure key management</li> </ul>
C.8 Legal and Regulatory –	<ul style="list-style-type: none"> <li>GV.RR Roles, Responsibilities, and</li> </ul>		<ul style="list-style-type: none"> <li>6.1 Screening</li> </ul>			<ul style="list-style-type: none"> <li>HR-01 Verification of qualification</li> </ul>

Personnel security	Authorities (GV.RR-04)					and trustworthiness
C.9 National Location			<ul style="list-style-type: none"> <li>• 8.3 Information access restriction</li> <li>• 5.14 Information transfer</li> </ul>	<ul style="list-style-type: none"> <li>• 3.2 Establish security monitoring (3.2.2)</li> </ul>	<ul style="list-style-type: none"> <li>• DSP Data Security and Privacy Lifecycle Management (DSP-19)</li> </ul>	<ul style="list-style-type: none"> <li>• OPS-06 Data Protection and Recovery – Concept</li> <li>• OPS-12 Logging and Monitoring – Access, Storage and Deletion</li> <li>• IDM-07 Access to cloud customer data</li> <li>• COS-08 Policies for data transmission</li> <li>• SSO-03 Directory of service providers and suppliers</li> <li>• PSS-08 Roles and Rights – Concept</li> <li>• PSS-12 Locations of Data</li> </ul>



						Processing and Storage
C.10 EU / EEA Location			<ul style="list-style-type: none"> <li>8.3 Information access restriction</li> <li>5.14 Information transfer</li> </ul>	<ul style="list-style-type: none"> <li>3.2 Establish security monitoring (3.2.2)</li> </ul>	<ul style="list-style-type: none"> <li>DSP Data Security and Privacy Lifecycle Management (DSP-19)</li> </ul>	<ul style="list-style-type: none"> <li>OPS-06 Data Protection and Recovery – Concept</li> <li>OPS-12 Logging and Monitoring – Access, Storage and Deletion</li> <li>IDM-07 Access to cloud customer data</li> <li>COS-08 Policies for data transmission</li> <li>SSO-03 Directory of service providers and suppliers</li> <li>PSS-08 Roles and Rights – Concept</li> <li>PSS-12 Locations of Data Processing and Storage</li> </ul>
C.11 Training and Awareness	<ul style="list-style-type: none"> <li>GV.RR Roles, Responsibilities, and Awareness (GV.RR-04)</li> </ul>		<ul style="list-style-type: none"> <li>6.3 Information security awareness, education and training</li> </ul>	<ul style="list-style-type: none"> <li>4.1 Prepare the organisation for incidents (4.1.3)</li> </ul>	<ul style="list-style-type: none"> <li>HRS Human Resources (HRS-11, HRS-12)</li> <li>DCS Data Center</li> </ul>	<ul style="list-style-type: none"> <li>HR-03 Security training and awareness programme</li> <li>DEV-04 Safety training and</li> </ul>

			<ul style="list-style-type: none"><li>• 7.7 Clear desk and clear screen</li><li>• 8.7 Protection against malware</li></ul>		Security (DCS-11)	awareness programme
C.12 Professional Services						



