MPS
March 2025

Compliance Mapping Tables for MPS Cloud Reference Architecture v10

[Undertittel]

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, including CSA-CCM, NSM Grunnprinsipper, and NIS2.

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

CSRA Requirement	NIST CSF 2.0	ISO 27001:2022	ISO 27002:2022	NSM Grunnprinsipper for IKT-sikkerhet 2.1	CSA CCM V4.0.12
A.1 Purpose	• GV.OC Organizational Contex (GV.OC-01, 02, 04, 05,)	• 4.1 Understanding the organization and its context • 4.2 Understanding the needs and expectations of interested parties • 6.2 Information security objectives and planning to achieve them			

A.2 Purpose	• GV.OV Oversight (GV.OV-01, 02, 03) • GV.PO Policies, Processes, and Procedures (GV.PO-01) • GV.RM Risk Management Strategy (GV.RM-01, 02, 03, 04, 06, 07) • GV.RA Risk Assessment (ID.RA-05, 06, 07)	• 6.1.1 General		• 1.1 Identify management structures, delliverables and supporting systems (1.1.2, 1.1.3, 1.1.4, 1.1.5) • 2.1 Include security during procurement and development processes (2.1.4, 2.1.9) • 2.2 Establish a secure ICT architecture (2.2.7) • 2.3 Maintain a secure configuration (2.3.10)	• GRC Governance, Risk and Compliance (GRC-02, GRC-04) • TVM Threat & Vulnerability Management (TVM-01) • CCC Change Control and Configuration Management (CCC-03) • CEK Cryptography, Encryption & Key Management (CEK-07) • STA Supply Chain Management, Transparency, and Accountability (STA-08) • BCR Business Continuity Management and Operational Resilience (BCR-02)

A.3 Compliance	• OV.OC Organizational Context (GV.OC-03)	• 8.1 Operational Planning and Control	• 5.4 Management Responsibilities • 5.10 Acceptable use of information and other associated assets • 5.31 Legal, statutory, regulatory, and contractual requirements	• 3.2 Establish security monitoring (3.2.2)	• A&A Audit & Assurance (A&A-04)
A.4 Compliance	• GV.OC Organizational Context (GV-OC-03) • GV.PO Policies, Processes, and Procedure (GV.PO-01)	• 4.3 Determining the scope of the information security management system • 4.4 Information security management system	• 5.31 Legal, statutory, regulatory, and contractual requirements • 5.36 Compliance with policies, rules and standards for information security	• 2.1 Include security during procurement and development processes (2.1.3)	• GRC Governance, Risk and Compliance (GRC-05, GRC-07)
A.5 Documentation		• 7.5 Documented information	• 5.37 Documented operating procedure		• BCR Business Continuity Management and Operational

			• 6.8 Information security event reporting		Resilience (BCR-05)
A.6 Notification			• 6.8 Information security event reporting	• 1.3 Identify users and access requirements (1.3.3) • 4.1 Prepare the organisation for incidents (4.1.5) • 4.2 Assess and categorize incidents (4.2.3) • 4.3 Control and manage incidents (4.3.5)	
A.7 Audit	• ID.IM Improvement (ID.IM-02)	• 9.2.2 Internal audit program	• 5.35 Independent review of information security • 8.34 Protection of information systems during audit testing		• A&A Audit & Assurance (A&A-01, A&A-04, A&A-05) • STA Supply Chain Management, Transparency, and Accountability (STA-11) • SEF Security Incident Management, E-Discovery &

					Cloud Forensics (SEF-08)
A.8 Governance	• GV.RR Roles, Responsibilities, and Authorities (GV.RR-01, 02) • GV.RM Risk Management Strategy (GV.RM-05) • GV.SC Cybersecurity Supply Chain Risk Management (GV.SC-02)	• 5.1 Leadership and Commitment • 5.3 Organizational roles, responsibilities and authorities • 7.1 Resources	• 5.2 Information security roles and responsibilities • 5.3 Segregation of duties	• 1.3 Identify users and access requirements (1.3.3) • 4.1 Prepare the organisation for incidents (4.1.3)	• GRC Governance, Risk and Compliance (GRC-06)

1.2 Basic 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
B.IS.1 Security Governance – Compliance with standards and frameworks	• GV.OC Organizational Context (GV.OC-03) • GV.PO Policies, Processes, and Procedure (GV.PO-01)	• 8.1 Operational planning and control	• 5.31 Legal, statutory and contractual requirements	• 1.1 Identify management structures, deliverables and supporting systems (1.1.1)	• GRC Governance, Risk and Compliance (GRC-05, GRC-07)

B.IS.2 Security Governance – Information security management system	• GV.PO Policies, Proocesses, and Procedures (GV.PO-01, 02)	• 4.3 Determining the scope of the information security management system • 4.4 Information security management system	• 5.36 Compliance with policies, rules, and standards for information security	• 1.1 Identify management structures, deliverables and supporting systems (1.1.2, 1.1.3)	• GRC Governance, Risk and Compliance (GRC-01, GRC-03, GRC-04, GRC-05, GRC-07)
B.IS.3 Security governance – Assurance			• GV.PO Policies, Processes, and Procedure (GV.PO-01)	• 2.1 Include security during procurement and development processes (2.1.3, 2.1.10)	• GRC Governance, Risk and Compliance (GRC-07) • A&A Audit & Assurance (A&A-02, A&A-03)
B.IS.4 Security Governance – Security audit and testing obligations – regular security audits and testing	• ID.IM Improvement (ID.IM-01, 02, 03, 04)	• 9.2.2 Internal audit program • 9.2.1 Internal audit general	• 5.35 Independent review of information security • 8.34 Protection of information systems during audit testing		• Audit & Assurance (A&A-02, A&A-03, A&A-05) • STA Supply Chain Management, Transparency, and Accountability (STA-11)

B.IS.5 Security governance – security audit and testing obligations – documentation and remediation	• ID.IM Improvement (ID.IM-02, 03)	• 9.2.2 Internal audit program • 10.2 Noncomformity and corrective action • 10.1 Continual improvement	• 5.35 Independent review of information security • 8.34 Protection of information systems during audit testing		• A&A Audit & Assurance (A&A-06)
B.IS.6 Security governance – Access to security documents		• 5.2 Policy • 7.5 Documented information	• 5.1 Policies for information security • 5.37 Documented operating procedures		• BCR Busiuness Continuity Management and Operational Resilience (BCR-05)
B.IS.7 Security governance – Third party security management – security requirements	• ID.IM Improvement (ID.IM-02) • GV.SC Cybersecurity supply chain risk management (GV.SC-01 to 10)	•	• 8.26 Application security requirements • 5.19 Information security in supplier relationships • 5.21 Managing information security in the ICT supply chain • 5.20 Addressing information security within	• 2.1 Include security during procurement and development processes (2.1.2, 2.1.3, 2.1.4, 2.1.9, 2.1.10,) • 4.1 Prepare the organisation for incidents (4.1.4)	• STA Supply Chain Management, Transparency, and Accountability (STA-01 to STA-12) • UEM Universal ENdpoint Management (UEM-14)

			supplier agreements • 5.21 Managing information secuity in the ICT supply chain • 5.20 Addressing information security within supplier agreements • 6.6 Confidentiality or non-disclosure agreements • 8.30 Outsourced development		
B.IS.8 Security governance – Third party security management ownership and operations of data centres and infrastructure			• 5.22 Monitoring, review and change management of supplier services		• DCS Datacenter Security (DCS-02)
B.IS.9 Cooperation rgarding	• GV.RR Roles, Responsibilities, and Authorities	• 5.1 Leadership and commitment	• 5.2 Information security roles and responsibilities	• 1.3 Identify users and access requirements (1.3.3)	• GRC Governance, Risk and Compliance (GRC-06)

information security – information security responsible	(GV.RR-01, 02, 03, 05)	• 5.3 Organizational roles, responsibilities, and authorities • 7.1 Resources	• 5.3 Segration of duties	• 4.1 Prepare the organisation for incidents (4.1.3)	• SEF Security Incident Management, E-Discovery & Cloud Forensics (SEF-08)
B.IS.10 Cooperation regarding information security - information security responsible – summoning meetings	• GV.RM Risk management strategy (GV.RM-05)				
B.IS.11 Incident, Asset and Vulnerability Management – Security incident management and threat intelligence – processes	• GV.RA Risk Assessment Strategy (GV.RM-05) • ID.RA Risk Assessment (ID.RA-04, 05) • ID.AE Adverse Event Analysis (DE.AE-02, 03, 04, 06, 08) • RS.MA Incident Management		• 5.7 Threat intelligence • 5.24 Information security incident management planning and preparation • 5.25 Assessment and decision on information security events • 5.26 Response to information security incidents	• 1.1 Identify management structures, deliverables and supporting systems (1.1.3) • 2.1 Include security during procurement and development processes (2.1.10) • 3.3 Analyse data from security	• SEF Security Incident Management, E-Discovery & Cloud Forensics (SEF-01 to SEF-07)

	(RS.MA-01, 02, 03, 04, 05) • RS.AN Incident Analysis (RS.AN-03, 06, 07, 08) • RS.MI Incident Mitigation (RS.MI-01, 02) • RC.RP Incident Recovery Plan Execution (RC.RP-01 to 06)			monitoring (3.3.6) • 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) • 4.2 Assess and categorize incidents (4.2.1, 4.2.2, 4.2.3) • 4.3 Control and manage incidents (4.3.1, 4.3.2, 4.3.3, 4.3.5, 4.3.6) • 4.4 Evaluate and learn from incidents (4.4.1, 4.4.2, 4.4.3, 4.4.4)	
B.IS.12 Incident, Asset and Vulnerability Management – Security incident management and threat	• DE.AE Adverse Event Analysis (DE.AE-04, 08) • RC.CO Incident Recovery Communication (RC.CO-04)		• 5.24 Information security incident management planning and preparation • 5.28 Collection of evidence	• 1.3 Identify users and access requirements (1.3.3) • 3.3 Analyse data from security monitoring (3.3.6)	• SEF Security Incident Management, E-Discovery & Cloud Forensics (SEF-07)

intelligence – notification and doumentation			• 6.8 Information security event reporting	• 4.1 Prepare the organisation for incidents (4.1.5) • 4.2 Assess and categorise incidents (4.2.1, 4.2.2, 4.2.3, 4.3.5)	
B.IS.13 Incident, Asset and Vulnerability Management – Security incident management and threat intelligence – Cooperation	• DE.AE Adverse Event Analysis (DE.AE-03, 06, 08) • GV.SC Cybersecurity Supply Chain Risk Management (GV.SC-08) • RS.MA Incident management (RS.MA-01) • RS.CO Incident Response Reporting and Communication (RS.CO-02, 03, 08)			• 1.3 Identify users and access requirements (1.3.3) • 2.1 Include security during procurement and development processes (2.1.10) • 3.3 Analyse data from security monitoring (3.3.6) • 4.1 Prepare the organisation for incidents (4.1.4, 4.1.4) • 4.2 Assess and categorize incidents (4.2.3)	

				• Control and manage incidents (4.3.5)	
B.IS.14 Incident, Asset and Vulnerability Management – Security incident management and threat intelligence – Access to security logs	• PR.PS Platform security (PR.PS-04)		8.15 Logging	• 3.2 Establish security monitoring (3.2.4) • 4.2 Assess and categorize incidents (4.2.1) • 4.3 Control and manage incidents (4.3.3)	
B.IS.15 Incident, Asset and Vulnerability Management - Security incident management and threat intelligence - Threat Intelligence	• ID.RA Risk Assessment (ID.RA-02, 03) • DE.AE Adverse Event Analysis (DE.AE-07)		8.7 Protection against malware	• 3.1 Detect and remove known vulnerabilities and threats (3.1.2, 3.1.3) • 3.3 Analyse data from security monitoring (3.3.4)	
B.IS.16 Incident, Asset and	• ID.RA Risk Assessment (ID.RA-09)		8.7 Protection against malware	• 2.1 Include security during	• TVM Threat & Vulnerability

Vulnerability Management - Security incident management and threat intelligence - Malicious Software				procurement and development processes (2.1.2, 2.1.3, 2.1.4) • 2.8 Protect email clients and browsers (2.8.3, 2.8.4) • 3.1 Detect and remove known vulnerabilities and threats (3.1.3)	Management (TVM-02)
B.IS-17 Incident, Asset and Vulnerability Management - Asset and Vulnerability Management – Asset Management	• ID.AM Asset Management (ID.AM-1,2,4,5, 7,8) • PR.PS Platform Security (PR.PS-05) • ID.RA Risk Assessment (ID.RA-09)		• 5.11 Return of assets • 7.9 Security of assets off-premises • 7.10 Storage media • 7.14 Secure disposal or re-use of equipment • 5.9 Inventory of information and other	• 1.1 Identify management structures, deliverables and supporting systems (1.1.3) • 1.2 Identify devices and software (1.2.1, 1.2.2, 1.2.3, 1.2.4) • Include security	• HRS Human Resources (HRS-02, HRS-05) • CCC Change Control and Confiruation Management (CCC-04) • DCS Datacenter Security (DCS-01, DCS-04, DCS-05, DCS-06)

			associated assets • 5.10 Acceptable use of information and other associated assets	during procurement and development processes (2.1.1, 2.1.2, 2.1.3) • 2.2 Establish a secure ICT architecture (2.2.6) • 2.3 Maintain a secure configuration (2.3.10)	• UEM Universal Endpoint Management (UEM-01, UEM-02, UEM-04) • DSP Data Security and Privacy Lifecycle Management (DSP-02 to DSP-06)
B.IS.18 Incident, Asset and Vulnerability Management - Asset and Vulnerability Management – Vulnerability Management	• ID.RA Risk Assessment (ID.RA-01, 08)	•	• 8.8 Management of technical vulnerabilities	• 2.3 Maintain a secure configuration (2.3.1 to 2.3.10) • 2.5 Control data flow (2.5.4) • 2.8 Protect email clients and browsers (2.8.3, 2.8.4) • 3.1 Detect and remove known vulnerabilitie	• TVM Threat & Vulnerability Management (TVM-01, TVM-03, TVM-03, TVM-07, TVM-08, TVM-10) • AIS Application & Interface Security (AIS-07)

				s and threats (3.1.1)	
B.IS.19 Incident, Asset and Vulnerability Management - Asset and Vulnerability Management – third-party vulnerabilities	• ID.RA Risk Assessment (ID.RA-05)	•	• 8.16 Monitoring activities • 8.30 Outsourced development	• 3.1 Detect and remove known vulnerabilities and threats (3.1.2)	• TVM Threat & Vulnerability Management (TVM-01, TVM-05, TVM-10)
B.IS.20 Incident, Asset and Vulnerability Management - Asset and Vulnerability Management – Vulnerability Identification and Scoring					• TVM Threat & Vulnerability Management (TVM-01, TVM-09)
B.IS.21 Incident, Asset and Vulnerability Management - Asset and Vulnerability Management – Vulnerability Notification	• ID.RA Risk Assessment (ID.RA-05)				• TVM Threat & Vulnerability Management (TVM-01, TVM-09)
B.IS.22 Incident, Asset and Vulnerability Management - Suspension of	•			• 4.3 Control and manage incidents (4.3.2)	• TVM Threat & Vulnerability Management (TVM-01)

service due to security incidents and vulnerabilities					
B.IS.23 Incident, Asset and Vulnerability Management - Penetration testing rights	• ID.IM Improvement (ID.IM-02)			• 3.4 Perform penetration tests (3.4.1 to 3.4.6)	• TVM Threat & Vulnerability Management (TVM-06)
B.IS.24 Access Control and Customer Data – Security Access Management	• PR.AA Identity Management, Authentication, and Access Control (PR.AA-01, 02, 03, 04, 05) • PR.IR Technology Infrastructure Resilience (PR.IR-01)		• 8.3 Information access restriction • 5.15 Access control • 5.17 Authentication information • 5.18 Access rights • 8.5 Secure authentication • 8.2 Privileged access rights	• 1.3 Identify users and access requirements (1.3.1 to 1.3.3) • 2.2 Establish a secure ICT architecture (2.2.6) • 2.3 Maintain a secure configuration (2.3.7, 2.3.10) • 2.4 Protect the organisation's networks (2.4.1, 2.4.2) • 2.6 Control identities and access rights (2.6.1 to 2.6.7)	• IAM Identity & Access Management (IAM-01 to IAM-07, IAM-09, IAM-10, IAM-13 to IAM-16) • DCS Datacenter Security (DCS-08)
B.IS.25 Access Control and				• 2.6 Control identities and	• IAM Identity & Access

Customer Data – Secureity Access Management – Regular Access Reviews				access rights (2.6.1) •	Management (IAM-01, IAM-08)
B.IS.26 Access Control and Customer Data - Flexible and fine-grained identity and access management – Customer Identity and Access Management	• PR.AA Identity Management, Authentication, and Access Control (PR.AA-01 to 04)		• 5.18 Access Rights • 8.2 Privileged access rights	• 1.3 Identify users and access requirements (1.3.1)	• IAM Identity & Access Management (IAM-01 to IAM-07, IAM-09 to IAM-11, IAM-13 to IAM-16) • DCS Datacenter Security (DCS-08)
B.IS.27 Access Control and Customer Data - Flexible and fine-grained identity and access management – Standards for Cross-domain Identity Management (DELETED)			• 5.23 Information security for use of cloud services • 5.18 Use of privileged utility programs • 8.20 Networks security • 8.24 Use of cryptography • 5.17 Authentication information • 8.5 Secure authentication		• IAM Identity & Access Management (IAM-01, IAM-04)

			• 8.20 Networks security		
B.IS.28 Access Control and Customer Data – Secure Remote Access	• DE.CM Continuous Monitoring (DE.CM-01, 03, 06, 09)	• 9.1 Monitoring, measurement, analysis and evaluation	• 5.17 Authentication information • 8.5 Secure authentication • 6.7 Remote working • 8.20 Networks security • 8.21 Security of network services •	• 2.3 Maintain a secure configuration (2.3.10) • 2.4 Protect the organisation's networks (2.4.1, 2.4.2, 2.4.4) • 2.5 Control data flow (2.5.2, 2.5.5, 2.5.7)	• HRS Human Resources (HRS-04) • IVS Infrastructure & Virtualization Security (IVS-03, IVS-07, IVS-09)
B.IS.29 Access Control and Customer Data - Separation of Customer Data	• PR.DS Data Security (PR.DS-05, 09)	•	• 8.12 Data leakage prevention • 8.22 Segregation of Networks	• 1.1 Identify management structures, deliverables and supporting systems (1.1.6) • 2.1 Include security during procurement and development of processes (2.1.10) • 2.2 Establish a secure ICT architecture (2.2.3) • 2.3 Maintain a secure	• DSP Data Security and Privacy Lifecycle Management (DSP-01) • AIS Application & Interface Security (AIS-01, AIS-03) • IVS Infrastructure & Virtualization Security (IVS-06)

				configuration (2.3.10) • 2.5 Control data flow (2.5.1)	
B.IS.30 Access Control and Customer Data - Encryption of Customer Data – Protection of Customer Data	• ID.AM Asset Management (ID.AM-3) • PR.DS Data Security (PR.DS-01, 02, 05)	•	• 5.33 Protection of records • 5.34 Privacy and protection of PII • 8.24 Use of cryptography • 8.18 Use of privileged utility programs • 8.20 Networks security	• 2.5 Control data flow (2.5.6) • 2.7 Protect data at rest and in transit (2.7.1 to 2.7.5) • 2.9 Establish capability to restore data (2.9.4)	• CEK Cryptography, Encryption & Key Management (CEK-03) • DCS Datacenter Security (DCS-02) • UEM Universal Endpoint Management (UEM-08, UEM-11) • DSP Data Security and Privacy Lifecycle Management (DSP-01, DSP-10, DSP-17)
B.IS.31 Encryption of Customer Data – State of the Art Encryption			• 8.20 Networks security • 8.24 Use of cryptography • 5.17 Authentication information • 8.5 Secure authentication	• 2.4 Protect the organisation's networks (2.4.2) • 2.7 Protect data at rest and in transit (2.7.1 to 2.7.4)	• CEK Cryptography, Encryption & Key Management (CEK-01 to CEK-21) • LOG Logging and Monitoring

					(LOG-10, LOG-11)
B.IS.32 Access Control and Customer Data - Encryption of Customer Data – Quantum Resistant Cryptographic Algorithms			• 8.24 Use of cryptography		• CEK Cryptography, Encryption & Key Management (CEK-07)
B .IS.33 Access Control and Customer Data - Logging of access to Customer Data	PR.PS Platform Security (PR.PS-04)		• 8.5 Secure authentication • 8.15 Logging	• 3.2 Establish security monitoring (3.2.1 to 3.2.7)	• LOG Logging and monitoring (LOG-01 to LOG-05, LOG-07 to LOG-09, LOG-12, LOG-13) • IAM Identity & Access Management (IAM-12) • DSP Data Security and Privacy Lifecycle Management (DSP-01)
B.IS.34 Access Control and Customer Data - Logging of access to Customer Data – Retention Period			• 8.10 Information deletion • 8.15 Logging	• 3.2 Establish security monitoring (3.2.2)	

B.IS.35 Access Control and Customer Data - Notification of relocation of Customer Data			• 5.14 Information transfer		• DCS Datacenter security (DCS-02) • DSP Data Security and Privacy Lifecycle Management (DSP-01)
B.IS.36 Change Management and Security by Design – Change Management			• 8.32 Change Management	• 2.3 Maintain a secure configuration (2.3.5) • 2.10 Include security in the change management process (2.10.1 to 2.10.4) •	• CCC Change Control and Configuration Management (CCC-01 to CCC-05, CCC-07 to CCC-09) • CEK Cryptography, Encryption & Key Management (CEK-05) • Universal Endpoint Management (UEM-02, UEM-07) • IVS Infrastructure & Virtualization Security (IVS-05) • AIS Application & Interface

					Security (AIS, 04, AIS-06)
B.IS.37 Change Management and Security by Design – Change Management – Advance Notice			• 8.32 Change Management • 6.3 Planning of Changes		• CCC Change Control and Configuration Management (CCC-02)
B.IS.38 Change Management and Security by Design – Security by Design	ID.RA Risk Assessment (ID.RA-09)		• 8.9 Configuration management • 8.26 Application security requirements • 8.27 Secure system architecture and engineering principles • 8.25 Secure development life cycle • 5.8 Information security in project management	• 2.1 Include security during procurement and development processes (2.1.5, 2.1.6, 2.1.8) • 2.3 Maintain a secure configuration (2.3.1 to 2.3.10) • 2.8 Protect email clients and browsers (2.8.1 to 2.8.4)	• UEM Universal Endpoint Management (UEM-02, UEM-03, UEM-05, UEM-06, UEM-08 to UEM-13) • CCC Change Control and Configuration Management (CCC-06) • IVS Infrastructure & Virtualization Security (IVS-04) • AIS Application & Interface Security (AIS-02) • LOG Logging and Monitoring (LOG-06)

B.IS.39	ID.IM Improvement (ID.IM-02)		• 8.25 Secure development life cycle • 8.29 Security testing in development and acceptance • 8.33 Test information	• 2.1 Include security during procurement and development processes (2.1.6, 2.1.7)	• AIS Application & Intercace Security (AIS-05) • CCC Change Control and Configuration Management (CCC-02)
B.IS.40 Change Management and Security by Design – Standards and Best Practices			• 8.4 Access to source code • 8.27 Secure system architecture and engineering principles • 8.28 Source coding	• 2.1 Include security during procurement and development processes (2.1.4, 2.1.5, 2.1.8)	• CCC Change Control and Configuration Managment (CCC-06) • IVS Infrastructure & Virtualization Security (IVS-04) • DSP Data Security and Privacy Lifecycle Management (DSP-07, DSP-08)
B.IS.41 Business Continuity – Business Continuity and Disaster Recovery	PR.IR Technology Infrastructure Resilience (PR.IR-03)		• 8.14 Redundancy of information processing facilities • 5.29 Information security during disruption	• 4.1 Prepare the organisation for incidents (4.1.2, 4.1.6) • 4.3 Control and manage incidents (4.3.1, 4.3.2)	• BCR Business Continuity Management and Operational Resilience (BCR-01, BCR-03 to BCR-07, BCR-09, BCR-10)

			• 5.30 ICT readiness for business continuity		
B.IS.42 Business Continuity – Business Continuity and Disaster Recovery – Capacity Management	PR.IR Technology Infrastructure Resilience		• 8.6 Capacity Management	• 2.2 Establish a secure ICT architecture (2.2.7)	• IVS Infrastructure & Virtualization Security (IVS-02) • BCR Business Continuity Management and Operational Resilience (BCR-11)
B.IS.43 Business Continuity – Backup and Restore of the Supplier's Systems	• PR.DS Data Security (PR.DS-11) • RC.RP Incident Recovery Plan Execution (RC.RP-03)		• 8.13 Information backup	• 2.9 Establish capability to restore data (2.9.1 to 2.9.4)	BCR Business Continuity Management and Operational Resilience (BCR-08)
B.IS.44 Physical and Personnel Security – Physical Security	• PR.AA Identity Management, Authentication, and Access Control (PR.AA-06) • PR.IR Technology Infrastructure Resilience (PR.IR-02) • DE.CM Continuous Monitoring (DE.CM-02, 03)		• 7.13 Equipment maintenance • 8.1 User endpoint devices • 7.1 Physical security perimeters • 7.5 Protecting against physical and	• 2.1 Include security during procurement and development processes (2.1.4) • 2.4 Protect the organisation's networks (2.4.2, 2.4.3)	DCS Datacenter Security (DCS-03, DCS-07, DCS-09 to DCS-15)

			environmental threats • 7.2 Physical entry • 7.3 Securing offices, rooms and facilities • 7.6 Working in secure areas • 7.8 Equipment siting and protection • 7.11 Supporting utilities • 7.12 Cabling security • 7.4 Physical security monitoring		
B.IS.45 Physical and Personnel Security – Physical Security – Audits	• ID.IM Improvement (ID.IM-01, 02)				• A&A Audit & Assurance (A&A-02, A&A-03)
B.IS.46 Physical and Personnel Security – Personnel Security	• GV.RR Roles, Responsibilities, and Authorities (GV.RR-04) • PR.AT Awareness and Training (PR.AT-01, 02)	• 7.2 Competence • 7.3 Awareness	• 5.4 Management responsibilities • 6.3 Information security awareness, education and training		• DCS Datacenter Security (DCS-11) • HRS Human Resources (HRS-03, HRS-05 to HRS-13)

			• 6.6 Confidentiality or non-disclosure agreements • 6.2 Terms and conditions of employment • 6.5 Responsibilities after termination or change of employment • 6.4 Disciplinary process		
B.IS.47 Physical and Personnel Security – Personnel Security – Security Screening and Clearance	• GV.RR Roles, Responsibilities, and Authorities (GV.RR-04)		• 6.1 Screening		• HRS Human Resources (HRS-01)
B.IS.48 Physical and Personnel Security – Personnel Security – Audits	• ID.IM Improvement (ID.IM-02)		•		• A&A Audit & Assurance (A&A-02, A&A-03)

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
C.1 Security Architecture			• 8.27 Secure system architecture and engineering principles •	• 1.1 Identify management structures, deliverables and supporting systems (1.1.5, 1.1.-6) • 2.1 Include security during procurement and development processes (2.1.1, 2.1.10) • 2.2 Establish a secure ICT architecture (2.2.1 to 2.2.7) • 2.5 Control data flow (2.5.3, 2.5.8) • 3.3 Analyse data from security monitoring (3.3.1 to 3.3.7)	• IVS Infrastructure & Virtualization Security (IVS-08, IVS-09,

C.2 Secure Cloud Adoption	PR.PS Platform Security (PR.PS-01, 02, 03, 06)		• 8.9 Configuration management • 5.23 Information security for use of cloud services • 8.25 Secure development life cycle • 8.31 Separation of development, test, and production environments	• 1.1 Identify management structures, deliverables and supporting systems (1.1.5) • 2.1 Include security during procurement and development processes (2.1.1, 2.1.6) • 2.3 Maintain a secure configuration (2.3.1)	• IVS Infrastructure & Virtualization Security (IVS-01)
C.3 Governance and Compliance Dashboard		• 5.2 Policy • 7.4 Communication			
C4 Governance and Compliance Matrix – International Standards	• GV.OC Organizational Context (GV.OC-03)	• 8.1 Operational planning and control	• 5.31 Legal, statutory, regulatory and contractual requirements		• GRC Governance, Risk and Compliance (GRC-07)

and Frameworks					
C5 Governance and Compliance Matrix – National Standards and Frameworks	• GV.OC Organizational Context (GV.OC-03)	• 8.1 Operational planning and control	• 5.31 Legal, statutory, regulatory and contractual requirements		• GRC Governance, Risk and Compliance (GRC-07)
C.6 Security in multi-cloud and hybrid cloud environments			• 5.23 Information security for use of cloud services	• 1.1 Identify management structures, deliverables and supporting systems (1.1.5) • 2.2 Establish a secure ICT architecture (2.2.2)	• IPY Interoperability & Portability (IPY-01 to IPY-04)
			•		• CEK Cryptography, Encryption & Key Management (CEK-07)

C.7 Cryptography			• 8.24 Use of cryptography	• 2.7 Protect data at rest and in transit (2.7.1 to 2.7.5) • 2.9 Establish capability to restore data (2.9.5)	
C8 Legal and Regulatory – Personnel security	• GV.RR Roles, Responsibilities, and Authorities (GV.RR-04)		• 6.1 Screening		
C.9 National Location			• 8.3 Information access restriction • 5.14 Information transfer	• 3.2 Establish security monitoring (3.2.2)	• DSP Data Security and Privacy Lifecycle Management (DSP-19)
C.10 EU / EEA Location			• 8.3 Information access restriction • 5.14 Information transfer	• 3.2 Establish security monitoring (3.2.2)	• DSP Data Security and Privacy Lifecycle Management (DSP-19)
C.11 Training and Awareness	• GV.RR Roles, Responsibilities, and Awareness (GV.RR-04)		• 6.3 Information security awareness,	• 4.1 Prepare the organisation	• HRS Human Resources (HRS-11, HRS-12)

			education and training • 7.7 Clear desk and clear screen • 8.7 Protection against malware	for incidents (4.1.3)	• DCS Datacenter Security (DCS-11)
C.12 Professional Services	•		•		