Direktoratet for forvaltning og økonomistyring

DFØ
Mars 2026

MPS Cloud Reference Architecture v1.3

Information Security, Data Protection and Responsible AI Requirements for Cloud Contracts

Change Log

Version	Date	Description
0.9	27.08.2024	• First published version
1.0	01.04.2025	• Revised requirements based on feedback from reference group, users of the contract, and suppliers • Added data protection requirements • Added mapping table to ISO 27001, NIST CSF 2.0, NSM Grunnprinsipper for IKT-sikkerhet 2.1, and CSA CCM V4.0.12
1.0.1	09.04.2025	• Minor corrections
1.1	22.08.2025	• Added BSI C5:2020 (Cloud Computing Compliance Criteria Catalogue) to the standards mapping table
1.2	10.12.2025	• Added NIS2 Implementing Regulations to the standards mapping table
1.3	30.03.2026	• Added Basic Requirements for Responsible AI. These requirements will be updated as we test these in the market.

1 Preface

As the public sector adopts cloud computing as a key enabler for its digital transformation, information security and data protection represent critical risk areas. At the same time, cybersecurity risks are highlighted as a strategic area by national security authorities, with nation-state threat actors and advanced cybercrime organizations targeting vulnerabilities in digital services and infrastructure.

This document presents the Norwegian Public Sector Cloud Marketplace (MPS) Cloud Reference Architecture: Information Security and Data Protection Requirements for Cloud Contracts. Its primary purpose is to strengthen information security and data protection in the Norwegian public sector, through verifying the security of cloud services ("security of the cloud") and enabling secure adoption of cloud services ("security in the cloud").

We use the term "MPS Cloud Reference Architecture: Information Security and Data Protection Requirements for Cloud Contracts" as a concept to describe the overall principles, methodology, and requirements for information security and data protection developed for cloud services by MPS. This document represents a key part of the reference architecture – the information security and data protection requirements.

The document is based on international and national laws, standards, and frameworks, and example cloud agreements. It is developed in cooperation with public sector entities, cloud vendors, and relevant authorities, and it is tested in framework agreement procurement processes at MPS.

The document is intended to be used for cloud services in the public sector, both the public sector (customers) and cloud service providers (suppliers). It should be noted that the requirements outlined are intended to be used as a reference, and that not all requirements apply in all cases. Users should review and select applicable parts of the document, and add additional requirements as needed.

The document will be continuously updated through user feedback, with new additions. This version – v1.3 includes a new set of Basic AI Governance requirements (Part B), incorporates support for the NIS2 Directive and its Implementing Regulations into the compliance mapping tables.

We hope this comes to good use!

Content

Innhold

2 Introduction

This document contains the first version of the MPS Cloud Reference Architecture Information Security and Data Protection Requirements for Cloud Contracts, developed and published by the Norwegian Public Sector Cloud Marketplace (MPS) at the Norwegian Agency for Public and Financial Management (DFØ).

The purpose of the document is to strengthen information security and data protection in the Norwegian public sector through making available a set of information security and data protection requirements, enabling the public sector to set requirements and verify the security and privacy of cloud services ("security of the cloud"), but also to succeed with managing risks in their cloud adoption ("security in the cloud").

We use the term "MPS Reference Architecture" as a concept to describe the overall principles, methodology, and requirements for information security and data protection developed for cloud services by MPS. The "MPS Cloud Reference Architecture" will be developed over time and is intended to include information security and data protection requirements (this document) with a mapping to relevant legal / regulatory requirements and security standards / frameworks, vendor input and evaluation forms, as well as the vendors' responses to the requirements, including the vendors' security architectures.

It is important to stress that public sector buyers should make a thorough assessment of each requirement in the particular context of their intended use of the cloud services, following a risk-based approach. As a starting point, requirements that limit or skew competition in a public procurement process should not be used unless this is based on legitimate needs and requirements, e.g., regulatory requirements.

2.1 Audience

The document and the outlined requirements are written for the Norwegian public sector and vendors of cloud services and are intended to be used as a reference for procurement, contract management, and vendor management related to cloud services in the public sector.

The document is written in English as the cloud services market is international. A Norwegian translation is available as part of the guidance provided by the Norwegian[1] Public Sector Cloud Marketplace.

2.2 Structure and Methodology

The Cloud Security Reference Architecture Information Security Requirements for principal, basic and optional security requirements in Cloud Contracts, is developed during the period 2022-24 in dialogue with users in the Norwegian public sector (government, counties and municipalities), vendors and relevant authorities.

[1] markedsplassen.anskaffelser.no

The requirements are based on international standards and frameworks (including ISO 27001 and NIST Cyber Security Framework 2.0, also referred to as NIST CSF, and the BSI C5:2020 (Cloud Computing Compliance Criteria Catalogue)), Norwegian standards and frameworks (including NSM ICT Security Principles and "Normen"), legal frameworks (including GDPR, NIS2, the Norwegian Security Act, and the Norwegian Digital Security Act), and a comprehensive assessment of information security and data protection requirements from both national (government and municipalities) and international example contracts. A comprehensive overview of referenced standards and frameworks is included as an appendix, and a mapping table with relevant laws, standards, and frameworks will be provided at a later stage.

The requirements are further tested in procurement processes and market assessments at the Norwegian Public Sector Cloud Marketplace, where the vendors have had the opportunity to ask questions and to give input to the requirements.

The requirements are structured in 3 sections, as follows:

A. **Principal requirements:** High-level information security and data protection requirements intended to be included in the main contract of cloud services agreements.
B. **Basic information security and data protection requirements:** A comprehensive set of information security requirements intended to be included as a security annex in cloud services agreements. As a general rule, this section defines requirements for the Supplier and the Service(s) provided, i.e., "security of the cloud".
C. **Optional information security and data protection requirements:** A set of optional information security requirements intended to support the Norwegian public sector with a secure and compliant cloud adoption, i.e., "security in the cloud", supported by the vendor's reference architecture, specific national requirements, and other security related services.

It should be noted that the requirements are intended to be used as a reference, and that all requirements do not apply in all cases. Users of the Cloud Security Reference Architecture should review and select applicable requirements, and add additional requirements as required. This evaluation should include whether the requirements are mandatory requirements, evaluation requirement, optional requirements, or documentation requirements. To determine the applicable requirements for each environment, it is advisable to adopt a risk-based approach, guided by recognized frameworks such as those previously mentioned.

The following key terms are used in the document:

- Contract: The cloud service agreement between Customer and Supplier
- Service: The cloud services in question (i.e., IaaS, PaaS and/ or SaaS[2])
- Customer: The entity buying or consuming cloud services
- Supplier: The cloud service provider
- Personal Data: Any information relating to an identified or identifiable natural person (cf. the GDPR art. 4 no. 1)

[2] Infrastructure-as-a-Service, Platform-as-a-Service, Software-as-a-Service

The term “such as” is used in the requirements to provide examples, such as relevant laws, standards, technologies, and products. Such examples are not to be considered complete (i.e., the lists are not exhaustive) or mandatory (i.e., the Supplier(s) are not required to support all examples provided.)

3 Principal Security Requirements

This chapter contains high level information security and data protection requirements intended to be included in the main contract of cloud services agreements. The purpose of this chapter is to define high level requirements for the Supplier and the Service(s) in scope (i.e., "security of the cloud".)

Number	Category	Requirement
A.1	Purpose	The Supplier acknowledges that information security is of critical importance to the Norwegian government and the Customer under this Agreement.
A.2	Purpose	The Supplier shall ensure that all security risks are managed in a vigilant manner and take all necessary measures to protect the offered Services from all levels of internal and external threats, including, but not limited to, nation state targeted network and intelligence operations.
A.3	Compliance	The Supplier (and any person or entity acting on its behalf, including Subcontractors, and any Affiliate) shall; A) comply with all Laws applicable to the Supplier in general, including those concerning security, bribery, corruption, and fraud; B) offer Services that are in accordance with applicable Laws and that will enable the Customers to comply with applicable Laws relevant for the Services, including the Regulation (EU) 2016/679 (GDPR) (where applicable) and the Norwegian Act no 38 of 15 June 2018 relating to the Processing of Personal Data (Personal Data Act); and C) comply with the highest standards of business ethics, i.e., establish and maintain robust processes and controls to ensure ethical compliance for itself and throughout its supply chain.
A.4	Compliance	The Supplier shall comply with international standards and frameworks for information security. The Supplier shall achieve and maintain information security and data protection compliance in accordance with international standards and frameworks, such as ISO/IEC 27001:2022, NIST Cybersecurity Framework v.2.0, or other substantially equivalent standard(s) for

Number	Category	Requirement
		information security management and any updates to such standards.
A.5	Documentation	The Supplier shall, within 30 (thirty) days after a written request from the Customer, provide reasonable documentation to verify compliance of any security or data protection provisions in the Contract.
A.6	Notification	In the event of a serious security incident or significantly increased threat to the information security relating to the provisioning of the Services, the Supplier shall provide an initial notification in writing or by phone directly to the Customer within 24 hours and a report of the incident within 72 hours. This equally applies to compromises of personal information.
A.7	Audit	The Customer shall, by itself or by use of a third party, have the right to carry out audits of the Supplier in order to: A) verify that the Supplier is complying with this Agreement; B) carry out general IT security risk audits/reviews; C) carry out data security and data protection audits/reviews; or D) accommodate requests from Norwegian security authorities and for compliance with Laws, hereunder the Norwegian Act no 24 of 1 June 2018 relating to national security (the Security Act).
A.8	Governance	The Supplier shall appoint a security responsible at an executive level as a counterpart to the Customer, who is responsible for strategic security meeting places, reporting, and follow-up of material risks, incidents, and vulnerabilities.

4 Basic Information Security and Data Protection Requirements

This section contains a comprehensive set of information security and data protection requirements intended to be included as a security annex in cloud services agreements. The purpose of this chapter is to define basic requirements for the Supplier and the Service(s) in scope (i.e., “security of the cloud”.)

It is recommended that the requirements are reviewed for the scope in question and adjusted accordingly, including adding new or removing unnecessary requirements.

Please note that there is an intended redundancy between some of the principal requirements (level A) and the basic information security and data protection requirements (level B). This is to support more complex contract structures, such as framework agreements, and it is indicated through cross-references (footnotes). This can be simplified by removing redundant requirements in level A or B respectively.

4.1 Basic Information Security Requirements

Number	Category	Title	Requirement
B.IS.1[3]	Security Governance	Compliance with standards and frameworks	The Supplier shall achieve and maintain information security and data protection compliance in accordance with: a) ISO 27001:2022, NIST Cybersecurity Framework 2.0 or other substantially equivalent standard(s) for information security management and any updates to such standards; b) cloud specific frameworks, such as ISO 27017, CCM-CSA, C5 and FedRAMP or other equivalent standards.
B.IS.2	Security Governance	Information security management system	The Supplier shall establish and maintain an effective information security management system that considers all information security risks, including both external threats and insider risks. The Services shall comply with requirements set forth in ISO/IEC 27001:2022, or equivalent standards.

[3] See also requirement A.4

Number	Category	Title	Requirement
B.IS.3	Security Governance	Assurance	The Supplier shall, either on-line or upon request, provide documentation that verifies independent assurance of the Supplier's information security management system through ISO/IEC 27001:2022 certifications, SOC2 Type 2 reports, C5, FedRAMP or equivalent evidence. The Supplier shall maintain the assurance at an equivalent or higher level throughout the duration of the Contract.
B.IS.4	Security Governance	Security audit and security testing obligations – Regular Security Audits and Testing	The Supplier shall ensure the security of the Service(s) through regular external and internal security audits and security testing. If evidence from the Supplier´s security audits indicate the need for sharing more detailed information with the customer, the Supplier shall provide specifications of the type, scope, and frequency of the testing.
B.IS.5	Security Governance	Security audit and security testing obligations – Documentation and Remediation	The Supplier shall address issues identified in security audits or security tests that are relevant to the Service(s) without undue delay and provide the Customer with a copy of the security audit or testing report upon request. In the event that the document contains Supplier Confidential information, then either a redacted version will be supplied or alternative evidence that the issue has been satisfactorily rectified.
B.IS.6	Security Governance	Access to Security Documents	The Supplier shall, either on-line or upon request, make available to the Customer relevant documents necessary to demonstrate compliance with the obligations laid down in the Contract.
B.IS.7	Security Governance	Third Party Security Management – Security Requirements	The Supplier shall ensure that third parties (e.g., vendors, services, subcontractors, and software providers) used in providing the Services to the Customer under the Contract fulfil the security requirements, or substantially equivalent security requirements, set out in this Contract.

Number	Category	Title	Requirement
B.IS.8	Security Governance	Third Party Security Management – Ownership and Operations of Data Centres and Infrastructure	The Supplier shall notify the Customer, for the purpose of assessing foreign ownership risks, in advance of any planned changes to the ownership or operation of the data centres or infrastructure used to deliver the Service(s). Such notice shall include the identity of the new third-party owner or operator, if applicable, and any potential impact on the provision of the Services. This requirement is limited to data centres and infrastructure used to provision the Service(s) in the EU/EEA.
B.IS.9[4]	Cooperation regarding Information Security	Information security roles and responsibilities – point of contact	The Supplier shall appoint an information security manager role or other point of contact under the Contract as a counterpart to the Customer, who is responsible for updating the Customer on the Suppliers security strategy and roadmaps, security products and services, risks, incidents, and vulnerabilities. The Customer shall be entitled to escalate any security issues at an executive level.
B.IS.10	Cooperation regarding information security	Information security roles and responsibilities – Summoning meetings	Both Parties can summon a meeting with 7 (seven) days' written notice.
B.IS.11	Incident, Asset and Vulnerability Management	Security incident management and threat intelligence - Processes	The Supplier shall establish and maintain processes for security incident management and threat intelligence. This includes actively detect, identify and respond to threats and security incidents, including those arising from third parties or third-party components in the Service(s).
B.IS.12[5]	Incident, Asset and Vulnerability Management	Security incident management and threat intelligence -	In the event of a serious security incident or significantly increased threat to the information security relating to the provisioning of the Services, the Supplier shall, through the Suppliers established

[4] See also requirement A.8
[5] See also requirement A.6

Number	Category	Title	Requirement
		Notifications and Documentation	processes, provide an initial notification directly to the Customer within 24 hours and a report of the incident within 72 hours. This equally applies to compromises of personal information. The report shall include information about the systems, services and information affected, along with an assessment of the impact on the Customer and a remediation plan.
B.IS.13	Incident, Asset and Vulnerability Management	Security incident management and threat intelligence - Cooperation	In the event of a serious security incident, the Supplier shall cooperate with relevant vendors appointed by the Customer, such as ICT outsourcing partners, cloud vendors and managed security services providers appointed by the Customer, to ensure the operational information security of the Customer's systems.
B.IS.14	Incident, Asset and Vulnerability Management	Security incident management and threat intelligence - Access to Security Logs	In the event of security breaches in the Services, the Supplier shall maintain and on either on-line or on request from the Customer provide access to a security log of all incidents concerning Customer Data, including log data and relevant indicators of compromise, for Customer incident analysis and digital forensic purposes.
B.IS.15	Incident, Asset and Vulnerability Management	Security incident management and threat intelligence - Threat Intelligence	The Supplier shall perform threat intelligence for the Service(s) in scope and continuously, or at least daily, update indicators of compromise (IoCs) and malware definitions.
B.IS.16	Incident, Asset and Vulnerability Management	Security incident management and threat intelligence - Malicious Software	The Supplier shall, while performing under the Contract, ensure that all software and storage media used in the provisioning of the Service(s) is free of any known malicious software.

Number	Category	Title	Requirement
B.IS.17	Incident, Asset and Vulnerability Management	Asset and Vulnerability Management – Asset Management	The Supplier shall establish and maintain processes for management and control of enterprise and software assets used in provisioning the Service(s). This includes keeping updated asset inventories with asset ownership, detecting and managing unauthorized assets, and managing relevant controls.
B.IS.18	Incident, Asset and Vulnerability Management	Asset and Vulnerability Management – Vulnerability Management	The Supplier shall establish and maintain processes for managing vulnerabilities in the Services. This includes performing security patching and implementing other compensating measures.
B.IS.19	Incident, Asset and Vulnerability Management	Asset and Vulnerability Management – third-party vulnerabilities	The Supplier shall monitor third-party vulnerability notifications and other relevant security vulnerability advisories.
B.IS.20	Incident, Asset and Vulnerability Management	Asset and Vulnerability Management – Vulnerability Identification and Scoring	Each vulnerability identified in the Service(s) shall be assigned a unique Common Vulnerability and Exposures (“CVE”) identifier and a Common Vulnerability Scoring System (“CVSS”) score. The Supplier shall maintain a record of all identified vulnerabilities.
B.IS.21	Incident, Asset and Vulnerability Management	Asset and Vulnerability Management – Vulnerability Notification	The Supplier shall, either through established notification channels or in writing, notify the Customer without undue delay of any vulnerabilities identified in the Services, including vulnerabilities from 3rd party vendors used to produce the Service, with a CVSS score of 9.0 to 10.0 (Critical) or 7.0 to 8.9 (High). The notification shall include information about the systems and information affected, along with an assessment of the impact on the Customer, and a remediation plan. The Supplier shall provide necessary support and information to the Customer and take appropriate actions to manage and mitigate risks associated with such vulnerabilities.

Number	Category	Title	Requirement
B.IS.22	Incident, Asset and Vulnerability Management	Suspension of service due to security incidents or vulnerabilities	In the event of a serious security incident or vulnerability affecting the provisioning of the Services, the Supplier shall offer to suspend the Services until the situation has been resolved or the Supplier has remedied the issue to the Customer's satisfaction. The Supplier shall assist the Customer with suspending the Services upon request.
B.IS.23	Incident, Asset and Vulnerability Management	Penetration testing rights	The Customer, shall, by itself or by use of a third party, have the right to perform penetration testing of the Service(s) according to procedures defined and maintained by the Supplier, to identify and analyse potential security vulnerabilities and risks.
B.IS.24	Access Control and Customer Data	Security Access Management	The Supplier shall implement and maintain strict access control policies and procedures to ensure that only identified and authorised employees and third parties have access to the Service(s) and their management system. The policies must, at minimum, address privileged access management, password management, authentication, authorisation, provisioning, change of role or work tasks and revocation of terminated users, separation of duties, approval workflows, and just-enough and just-in-time administration.
B.IS.25	Access Control and Customer Data	Security Access Management – Regular Access Reviews	The Supplier shall conduct regular access review to ensure compliance with the established access control policies and procedures.
B.IS.26	Access Control and Customer Data	Flexible and fine-grained identity and access management – Customer Identity and Access Management	The Supplier shall provide the Customer with flexible and fine-grained mechanisms for identity and access management. This includes supporting integration with the Customer's existing identity and access management systems, such as user directories.

Number	Category	Title	Requirement
B.IS.27	Access Control and Customer Data	Flexible and fine-grained identity and access management – Standards for Cross-domain Identity Management	The Supplier shall support relevant standards such as SCIM 2.0 or IETF RFC 7643 for cross-domain identity management.
B.IS.28	Access Control and Customer Data	Secure Remote Access	The Supplier shall ensure that any remote access to the Service(s) by its employees and third parties is secured with effective encryption and phishing resistant authentication measures in accordance with best industry practices, and that security gateways (enabling security policy enforcement, security monitoring, etc.) are used to control access between the Internet and the Supplier's Service(s).
B.IS.29	Access Control and Customer Data	Separation of Customer Data	The Supplier shall keep all Customer Data logically separate from the data of any third parties in order to eliminate the risk of compromising data and/ or unauthorised access to data. Logically separate means the implementation and maintenance of necessary and technical measures to secure data against undesired change or access. Undesired changes or access shall include access by the Supplier's personnel or others who do not need access to the information in their work for Customer.
B.IS.30	Access Control and Customer Data	Encryption of Customer Data – Protection of Customer Data	The Supplier shall ensure protection of Customer Data in transit and at rest, both internally within the Service(s) and for inbound/outbound traffic, including web access, APIs and administrative accesses.
B.IS.31	Access Control and Customer Data	Encryption of Customer Data – State of the Art Encryption	To achieve this protection, the Supplier shall implement measures such as state of the art encryption in transit and at rest and phishing resistant authentication. State of the art shall

Number	Category	Title	Requirement
			be interpreted as industry best practice with regards to choice of cryptographic protocols and algorithms.
B.IS.32	Access Control and Customer Data	Encryption of Customer Data – Quantum Resistant Cryptographic Algorithms	The Supplier should document its roadmap to ensure that cryptographic algorithms used in the Service(s) are quantum resistant, in accordance with, e.g., CNSA 2.0 ("Commercial National Security Algorithm Suite 2.0"), NIST standards for post-quantum cryptography, “NSMs veileder for kvantemigrering”, “NSMs kryptografiske anbefalinger (utkast 2024)”, or similar.
B.IS.33	Access Control and Customer Data	Logging of access to Customer Data	The Supplier shall maintain logs of all access to Customer Data by its own employees and any of its third parties and shall make such logs available to the Customer upon request.
B.IS.34	Access Control and Customer Data	Logging of access to Customer Data – Retention Period	The logs shall be retained for a defined retention period defined and maintained by the Supplier, taking into account applicable Laws and regulations, as well as any applicable recommendations from Norwegian authorities.
B.IS.35	Access Control and Customer Data	Notification of relocation of Customer Data	The Supplier shall notify the Customer in writing in advance of any planned relocation or transfer of Customer Data, including backups, to a new region or data center. This requirement is limited to data centres and infrastructure used to provision the Service(s) in the EU/EEA.
B.IS.36	Change Management and Security by Design	Change Management	The Supplier shall establish and maintain strict procedures for technology change management and deviation handling in the Service(s).
B.IS.37	Change Management and Security by Design	Change Management – Advance Notice	The Supplier shall provide advance notice to the Customer of any changes to the Service(s) that may negatively impact information security with sufficient time for the Customer to object.
B.IS.38	Change Management	Security by Design	The Supplier shall implement and adhere to security by design principles in the provision

Number	Category	Title	Requirement
	and Security by Design		of the Service(s) and ensure that software hardening best practices are implemented with secure configuration set as default.
B.IS.39	Change Management and Security by Design	Security by Design – Testing	The Supplier shall conduct testing to ensure that the Service(s) maintain a high level of integrity and quality, with no backdoors or known vulnerabilities.
B.IS.40	Change Management and Security by Design	Security by Design – Standards and Best Practices	The Supplier shall follow relevant industry standards and best practices to ensure security by design, such as CIS, CWE Top 25, OWASP Top 10, and OWASP ASVS.
B.IS.41	Business Continuity	Business Continuity and Disaster Recovery	The Supplier shall establish and maintain business continuity and disaster recovery plans that adhere to best industry standards, such as ISO 22313 or equivalent. The plans shall include measures to prevent or mitigate the impact of various types of disasters or disruptions, including but not limited to ransomware attacks, a distributed denial-of-service attack ("DDoS Attacks"), advanced persistent threats ("APT") attacks, unavailability of external IT resources or other external authentication sources, sabotage, fire, and natural catastrophes. The Supplier shall regularly test and rehearse these plans to ensure their effectiveness in the event of a disaster or disruption.
B.IS.42	Business Continuity	Business Continuity and Disaster Recovery – Capacity Management	The Supplier shall implement and maintain capacity management measures to ensure stable operations in both normal and disaster recovery situations.
B.IS.43	Business Continuity	Backup and Restore of the Supplier's Systems	The Supplier shall conduct regular backups, including offline backups, and restore testing to ensure the integrity and availability of its systems.
B.IS.44	Physical and Personnel Security	Physical Security	The Supplier shall implement and maintain appropriate physical security measures for its data centres, cloud infrastructure, operations environments (including remote operations),

Number	Category	Title	Requirement
			and any equipment installed on Customer premises, in accordance with relevant international standards and the Supplier's own policies.
B.IS.45	Physical and Personnel Security	Physical Security – Audits	The Supplier shall conduct annual audits of its physical security measures by an independent, qualified auditor certified to evaluate compliance with applicable standards and policies.
B.IS.46	Physical and Personnel Security	Personnel Security	The Supplier shall ensure that all personnel involved in the delivery of the Service(s), including personnel of any subcontractors and third parties, have committed themselves to confidentiality, receive appropriate training and maintain necessary expertise on security matters. This shall include training on applicable security rules, regulations and standards, including Customer-specific security rules where applicable.
B.IS.47	Physical and Personnel Security	Personnel Security – Security Screening and Clearance	The Supplier shall establish and maintain procedures for personnel security, including screening and background checks, to ensure that all personnel have the level of security clearance appropriate for their role, in accordance with applicable laws and industry best practices.
B.IS.48	Physical and Personnel Security	Personnel Security – Audits	The Supplier shall perform annual security audits on these procedures, conducted by a third-party auditor, to evaluate compliance with applicable standards and policies.

4.2 Basic Data Protection Requirements

This section contains data protection requirements intended to be included as a data protection annex. If the Supplier acts as processor, the requirements may also be incorporated into an agreement according to GDPR art. 28 (“Data Processing Agreement”).

The Customer must always consider what kind of data will be processed and the Parties’ roles under applicable data protection legislation (e.g. the GDPR and the Norwegian Data Protection Act). It is therefore recommended that the requirements are reviewed for the

scope in question and adjusted accordingly, including adding new or removing unnecessary requirements.

References to Personal Data is Personal Data as defined in this document section 2.2.

Number	Category	Requirement
B.DP.1	General	The obligations and requirements set out in annex applies when the Supplier processes Personal Data in connection with the delivery of the Services and comes in addition to the Supplier's other obligations under the Agreement.
B.DP.2	Competence, training and awareness	The Supplier shall ensure and document that authorised personnel, including any of its data processors or sub-processors, have the necessary competency and training within privacy and data protection in accordance with best industry practice, and applicable data protection legislation. The Supplier shall build and maintain a culture to ensure that all relevant personnel receive appropriate awareness training to understand their responsibilities for data protection and information security. The Supplier shall on regularly basis evaluate the competency and training of their personnel, including an assessment of the actions and measures implemented.
B.DP.3	Data processing agreement (DPA)	If the Supplier processes Personal Data on behalf of the Customer as a data processor, the Customer and the Supplier are obliged to enter into Data Processing Agreement (DPA) in accordance with GDPR art. 28 and any sector-specific data protection legislation that is relevant to the Customer's activities. A full and final Data Processing Agreement shall be signed and binding by the Customer and the Supplier prior to processing of Personal Data. If not set out elsewhere in the Contract, the DPA shall include a list of all sub-processors including name, addresses and location of processing. The Parties may use the Supplier’s standard Data Processing Agreement, provided that it fulfils the requirements of GDPR art. 28 and is not in conflict with any provisions of the Contract.
B.DP.4	Customer’s instructions and the role of the parties	If the Supplier processes Personal Data on behalf of the Customer as a data processor, the Supplier shall process Personal Data only on documented instructions from the Customer, unless required to do so by applicable EU/EEA or Member State law to which the Supplier is subject. The Customer's instructions shall be specified in the Data Processing Agreement or the Contract.

Number	Category	Requirement
		The Supplier shall not process Personal Data for any other purposes (including its own purposes) other than those set out in the Contract, the Data Processing Agreement or subsequent documented instructions from the Customer. The Supplier shall not process Personal Data to a greater extent than necessary to fulfil the aforementioned purposes. The Supplier may not itself determine what kind of processing they are authorised to do. The Supplier shall only process and store Personal Data about the Customer's administrators and end-users, including the Customer's use of the Services, when and to the extent such processing is necessary to perform the Supplier's obligations under the Contract. The Supplier shall upon request from the Customer document how only required Personal Data about such users is registered, stored and processed. If the Supplier determines the purposes and means for certain processing activities related to the delivery of the Services under the Contract, the Supplier will be regarded as a data controller for those processing activities. In such cases, the Supplier shall identify the relevant processing activities and specify the legal basis for each processing activity.
B.DP.5	Personal Data controls and measures	The Supplier shall implement and maintain a management system and/or internal control system for the processing of Personal Data in accordance with applicable data protection legislation and industry best practice, e.g. by adherence to approved codes of conduct or approved certification mechanisms as referred to in GDPR arts. 40 and 42. The internal control system shall be reviewed and updated regularly. The Supplier shall have a data protection officer when required according to GDPR art. 37. The Supplier shall upon request document the following: a) how data protection is organised, managed and controlled in its business and supply chain, including clearly defined roles and responsibilities; b) how Personal Data is processed in the Services, including the systems used, data flows and subcontractors processing, including what and why they process Personal Data; and c) the roles and responsibilities under applicable data protection legislation, including between the Customer, the Supplier and, where applicable, the Suppliers' subcontractors.
B.DP.6	Collaboration regarding	The Supplier shall collaborate with the Customer to ensure the protection and compliance of processing of Personal Data.

Number	Category	Requirement
	Personal Data	The Supplier shall notify the Customer immediately if it considers that any of the Customer's documented instructions infringe applicable data protection legislation. The Supplier shall provide all reasonable assistance to the Customer to enable the Customer to comply with applicable data protection legislation. This includes, but is not limited to upon request: a) provide the Customer with an assessment of the necessity and proportionality of the processing operations in relation to the Services; b) assist the Customer with an assessment of the risks to the rights and freedoms of Data Subjects, including, but not limited to Transfer Impact Assessment (TIA) and/or Data Protection Impact Assessment (DPIA) where applicable; and c) provide the Customer with information on measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of Personal Data. The Supplier shall notify the Customer without undue delay where: a) the Supplier becomes aware of an incident resulting in loss of the Customer's Personal Data, or an incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer's Personal Data transmitted, stored or otherwise processed; b) receiving any communication from the Norwegian Data Protection Authority ("Datatilsynet") or any other regulatory authority in connection with Personal Data processed under the Contract. The Supplier shall notify the Customer as soon as possible if it receives: a) a request made by, or on behalf of, a data subject in accordance with rights granted pursuant to the GDPR chapter III (e.g. a access request or to rectify, block or erase any Personal Data); b) a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by law; or c) any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation.
B.DP.7	Description of processing activities by Supplier and its data processors and/or sub-processors	The Supplier shall upon request provide or make available to the Customer a detailed description of the processing activities carried out by the Supplier and any of its data processors or sub-processor(s), and the purpose of the processing. This description shall include at a minimum: a) the specific processing activities in which the Supplier and data processor or sub-processor will be involved, including which Service(s) that contain Personal Data the data processor or sub-processor will have access to; b) the circumstances under which the data processor or sub-processor will have access to Personal Data for each of the processing activities, including

Number	Category	Requirement
		whether access is continuous or only granted periodically or upon the Supplier's instructions; and c) the categories of Personal Data that is processed by the Supplier and data processor or sub-processor for each of the processing activities.
B.DP.8	Data protection by design and default	The Supplier shall provide the Services in accordance with data protection by design and by default principles throughout the lifecycle of the service, in accordance with GDPR art. 25.
B.DP.9	Data Subject's rights	The Supplier shall have solutions that enables the Customer to, in an efficient manner, fulfil the natural persons' rights according to GDPR, including rights to access, to be informed, to rectification, to restriction, erasure, and data portability.
B.DP.10	Authorisation to engage sub-processors	If the Supplier acts as data processor, the Supplier's general or specific authorisation to engage sub-processors shall be specified in the Data Processing Agreement. A general authorisation in the Data Processing Agreement only applies to sub-processors in the EEA. The Supplier shall not engage sub-processors outside the EEA without the Customer's prior specific authorisation unless otherwise is specifically and explicitly agreed in the Contract. The Supplier shall upon request document the controls, processes, and frameworks, including risk assessments used to assess, approve, evaluate and follow up sub-processors from a data protection perspective. The Supplier shall upon request document data protection compliance of sub-processors.
B.DP.11	New sub-processors	If the Supplier, when acting as data processor, has a general authorisation from the Customer for the engagement of sub-processors, the Supplier shall notify the Customer in writing of any new sub-processors minimum 45 -forty-five- days prior to the engagement of such sub-processor. The Customer shall have the right to object to the engagement of new sub-processors in accordance with the Data Processing Agreement, EU SCC and GDPR art. 28. If the Customer does not object within 15 -fifteen- days, the sub-processor is deemed approved. If the Customer objects to the engagement of a new sub-processor, the following procedure shall be followed: a) The Supplier shall provide a written explanation as to why the processing of Personal Data by the sub-processor is in accordance with applicable laws, and how the use of the sub-processor will ensure compliance with applicable obligations under the Contract and applicable legislation. In addition, the Supplier shall address any objections raised by the Customer regarding the engagement of the sub-processor; b) If the

Number	Category	Requirement
		Customer still objects to the engagement of the new sub-processor, the Supplier shall use its best efforts to provide the Services without engaging the objected sub-processor, while ensuring that an equivalent level of information security is maintained; c) If the Supplier cannot provide the Services without engaging the objected sub-processor, then Customer shall have the right to terminate the Contract, or relevant Services under the Contract, with immediate effect without any liability.
B.DP.12	Engagement of sub-processors	If the Supplier, when acting as a data processor, engages a sub-processor for carrying out specific processing activities on behalf of the Customer, it shall do so by way of contract which imposes in substance the same data protections obligations as the ones imposed on the Supplier under the Data Processing Agreement. At the Customer's request, the Supplier shall provide a copy of such sub-processor agreement and any subsequent amendments to the Customer. To the extent necessary to protect business secret or other confidential information, including Personal Data, the Supplier may redact the text of the agreement prior to sharing the copy The Supplier shall remain fully responsible to the Customer for the performance of the sub-processor's obligations in accordance with its contract with the sub-processor. The Supplier shall notify the Customer of any failure by the sub-processor to fulfil its contractual obligations.
B.DP.13	Locations and transfer of data	Personal Data shall not be transferred outside EU/EEA unless explicitly agreed with the Customer in the Agreement or the Data Processing Agreement, if relevant, and in accordance with the procedures set out in this clause. Any transfer of Personal Data to countries outside the EU/EEA ("Third Country") shall be in accordance with GDPR chapter V (Transfers of personal data to third countries or international organisation), prior to such transfer. Transfer includes, but is not limited to: a) processing of Personal Data in data centres, etc. located in a Third Country; b) processing of Personal Data by another data processor or sub-processor in a Third Country (e.g. by remote access to Personal Data stored in EU/EEA); or c) disclosing Personal Data to a data controller or data processor (including international organisations) in a Third Country.
B.DP.14	Description of transfers to Third Countries	The Supplier shall on the Customer's request describe any transfers of Personal Data out of the EU/EEA that will be necessary for the performance of the Contract. The description shall at least include:

Number	Category	Requirement
		• A description of all transfers made by the Supplier, including the Supplier's processors or sub-processors • The legal basis for transfer in accordance with GDPR chapter V. • If the transfer is based on EU Standard Contractual Clauses for transfers to Third Countries (EU SCC), specify the data exporter and the data importer, the relevant EU SCC module, and provide information on any onward transfers • Full formal business name, address and organization number of all data importers outside the EU/EEA • Whether the Personal Data is transferred to and stored in the Third Country, or whether the transfer concerns remote access or other access to personal data stored in the EU/EEA • The purpose of the transfers • The categories of personal data being transferred • How often transfers will take place
B.DP.15	Documented assessment of transfer based on EU SCC and BCR (transfer impact assessment)	If any transfer of Personal Data is based on EU SCC or Binding Corporate Rules (BCR), the Supplier shall on the Customer's request provide a documented assessment of Third Country legislation and practices affecting the processing of Personal Data in the delivery, as well as the circumstances of the transfer, and additional measures (technical, organizational and contractual) taken by the Supplier, including its processors and sub-processors. The documented assessment shall at least contain what is required under Clause 14 (b) of the EU SCC, including documented experiences related to the disclosure of Personal Data to Third Country authorities.
B.DP.16	Data monitoring laws	The Supplier shall document and notify the Customer immediately if it has reason to believe that the laws and practices in a Third Country applicable to the processing of the Personal Data, including any requirements to disclose Personal Data or measures authorising access by public authorities, prevent the Supplier, or its data processor or sub-processors, from fulfilling its obligations under the Contract.
B.DP.17	Termination	Following termination of the Contract, the Supplier shall, at the choice of the Customer, delete all Personal Data processed on behalf of the Customer and certify to the Customer that it has done so, or, return all the Personal Data to the Customer and delete existing copies unless mandatory laws in the EU/EEA requires storage of the Personal Data. Until the data is deleted or returned, the Supplier, including its processor or sub-processors, shall continue to ensure compliance with the data protection and security requirements under the Contract.

4.3 Basic Requirements Responsible AI

This section contains a set of basic requirements intended to support responsible governance, development, deployment, and operation of Artificial Intelligence (AI) Systems provided under cloud service contracts. The purpose of this section is to establish baseline Responsible AI requirements applicable to Suppliers, proportionate to the risks associated with the Intended Use(s) of AI Systems and their operational context.

The requirements are designed to complement the information security and data protection requirements set out in this document and focus on AI-specific risks and governance considerations. They address, among others, AI governance and applicability, lifecycle risk management, data and model governance, transparency and explainability, human oversight, performance and robustness, bias and harm mitigation, monitoring and continuous improvement, training and organisational readiness, and obligations related to General-Purpose AI models where applicable.

The requirements are intended to be used as a reference and shall be reviewed and selected based on a risk-based assessment of the specific Service(s) and AI System(s) in scope. Not all requirements apply in all cases. Users of the CRA should assess the applicability and proportionality of each requirement and may add additional requirements where necessary.

Relationship with the EU Artificial Intelligence Act

The Responsible AI requirements set out in this section are designed to be consistent with, and supportive of, obligations arising under Union law governing artificial intelligence, including Regulation (EU) 2024/1689 (the Artificial Intelligence Act).

The MPS Cloud Reference Architecture does not seek to replicate or restate regulatory requirements. Instead, the Responsible AI requirements adopt a risk-based, lifecycle-oriented approach that aligns with the structure and objectives of the AI Act, while remaining technology-neutral and suitable for use in public procurement and contractual contexts.

The applicability of specific obligations under the AI Act depends on factors such as the role of the Supplier (e.g. provider, deployer, importer, distributor), the Intended Use of the AI System, and the level of risk associated with the system. Users of the CRA should therefore assess, on a case-by-case basis, whether and to what extent AI Act obligations apply to a given AI System and select relevant requirements accordingly.

Definitions

AI System: A system that uses artificial intelligence techniques to generate outputs, predictions, recommendations, or decisions influencing environments or processes, for a defined purpose.

Intended Use: The specific purpose and context for which an AI System is designed and deployed, as defined by the Supplier and communicated to the Customer.

Sensitive Use: A use of an AI System that may pose heightened risks to individuals, groups, fundamental rights, safety, or other protected interests, depending on the context of deployment.

General-Purpose AI (GPAI) Model: An AI model designed to perform a wide range of tasks and capable of being adapted or integrated into multiple downstream applications.

Red Teaming: Structured testing activities aimed at identifying vulnerabilities, misuse scenarios, or failure modes of an AI System through adversarial or challenge-based approaches.

Note that these requirements will be updated during 2026.

Number	Category	Title	Requirement	Applicability
B.AI.1	Governance and Accountability	Responsible AI Governance Framework	The Supplier shall establish, maintain, and document a Responsible AI governance framework applicable to the AI System(s) provided under the Contract. The framework shall be based the EU AI Act, ISO 42001, NIST AI RMF or other globally accepted AI management standard, and shall define governance structures, internal policies, and processes for ensuring that the design, development, deployment, and operation of AI Systems are carried out in a responsible manner, proportionate to the risks associated with their Intended Use(s). The Supplier shall maintain documentation describing the Responsible AI governance framework and furnish such	All

Number	Category	Title	Requirement	Applicability
			documentation to the Customer upon request.	
B.AI.1.1	Governance and Accountability	Intended Use and Sensitive Use Definition	The Supplier shall document the Intended Use(s) of each AI System and identify any Sensitive Use(s), including uses that may affect fundamental rights, safety, or other protected interests. The documentation shall describe the operational context, user groups, and limitations of the AI System. The Supplier shall ensure that this documentation is kept up to date throughout the lifecycle of the AI System.	All
B.AI.1.2	Governance and Accountability	Scope and Applicability of Responsible AI Requirements	The Supplier shall document, for each AI System, whether the AI functionality is core to the Service(s) or constitutes an incidental component of the Service(s), and whether the Supplier has developed, customised, or fine-tuned any model used in the AI System. This documentation shall be used to determine the applicability and proportionality of the Responsible AI requirements set out in this section. The Supplier shall review and update this documentation when there are material changes to the	All

Number	Category	Title	Requirement	Applicability
			AI System or its Intended Use(s).	
B.AI.1.3	Governance and Accountability	Allocation of Roles and Responsibilities for AI Governance	The Supplier shall define clear roles and responsibilities for the governance, oversight, and management of AI Systems within its organisation. This shall include identifying the person(s) or function(s) responsible for Responsible AI governance, escalation of AI-related risks, and coordination of remediation activities.	All
B.AI.1.4	Governance and Accountability	Cooperation on AI Risk Management	The Supplier shall cooperate with the Customer, upon request, to support the identification, assessment, and mitigation of risks arising from the use of AI Systems in the context of the Service(s). Such cooperation may include providing relevant documentation, explanations of system behaviour, and information necessary to enable the Customer to fulfil its own governance and compliance obligations.	All
B.AI.2	Risk Management	AI Risk and Impact Assessment	The Supplier shall identify, assess, and document risks associated with the AI System throughout its lifecycle, taking into account the Intended Use(s), Sensitive Use(s), and	All

Number	Category	Title	Requirement	Applicability
			the operational context in which the AI System will be deployed. The Supplier shall maintain documentation of the risk or impact assessment(s) performed and furnish documentary evidence to the Customer upon request.	
B.AI.2.1	Risk Management	Review and Update of Risk and Impact Assessments	The Supplier shall ensure that any AI risk or impact assessment accurately reflects the AI System as provided to the Customer. The Supplier shall review and update the assessment regularly and, in any event, no later than 30 calendar days after any substantive change to the AI System that may affect its functionality, performance, security, operation, or risk profile. The Supplier shall maintain records of such reviews and updates and make them available to the Customer upon request.	All
B.AI.2.2	Risk Management	Pre-deployment Testing and Validation	Prior to deployment of the AI System, the Supplier shall perform appropriate testing activities to validate identified risks and to assess whether the AI System performs as intended within its defined scope. Such testing shall be proportionate to the level of risk associated with the AI	All

Number	Category	Title	Requirement	Applicability
			System and may include technical testing, scenario-based testing, or other relevant validation methods.	
B.AI.3	Data and Model Governance	Governance of Data Sets Used in AI Systems	The Supplier shall ensure that data sets used in the design, development, training, validation, testing, or operation of the AI System are subject to data governance measures appropriate to the context of use, the Intended Use(s) of the AI System, and the level of risk associated with potential harm. The Supplier shall document the data governance measures applied and furnish documentary evidence to the Customer upon request.	All
B.AI.3.1	Data and Model Governance	Documentation of Training, Validation, and Testing Data	The Supplier shall document, at an appropriate level of detail, the categories and sources of data used for training, validation, and testing of the AI System, to the extent relevant for understanding system behaviour and risks. This documentation shall describe the purpose for which the data sets are used and any material limitations known to the Supplier that may affect the performance or outcomes of the AI System.	High Risk AI Systems

Number	Category	Title	Requirement	Applicability
B.AI.3.2	Data and Model Governance	Model Development, Customisation, and Fine-Tuning	Where the Supplier has developed, customised, or fine-tuned a model used in the AI System, the Supplier shall document the nature and scope of such activities and assess their potential impact on the behaviour, performance, and risks of the AI System. .	If Applicable
B.AI.3.3	Data and Model Governance	Management of Data and Model Limitations	The Supplier shall identify and document known limitations of the data sets or models used in the AI System that may affect the system's performance, reliability, or suitability for specific Intended Use(s). Where relevant, the Supplier shall document measures implemented to mitigate the impact of such limitations.	High Risk AI Systems
B.AI.3.4	Data and Model Governance	Ongoing Governance of Data and Model Changes	The Supplier shall establish processes to govern material changes to data sets or models used in the AI System, including changes that may affect system behaviour or risk profile. Such processes shall be aligned with the lifecycle risk management activities applicable to the AI System.	High Risk AI Systems

Number	Category	Title	Requirement	Applicability
B.AI.4	Transparency and Explainability	Transparency of AI System Functioning	The Supplier shall ensure that the AI System is designed and developed in a manner that enables a reasonable understanding of how the system functions, taking into account its Intended Use(s), complexity, and associated risks. The Supplier shall provide the Customer with sufficient information to understand the general logic, system architecture, and operational characteristics of the AI System, at a level of detail appropriate to support governance, oversight, and responsible use. Such information shall be documented and made available to the Customer upon request.	All
B.AI.4.1	Transparency and Explainability	Explainability of AI System Outputs	Where the AI System generates outputs that may influence decisions, actions, or assessments, the Supplier shall provide explanations of how such outputs are produced. This shall include, where relevant, information on the main factors influencing the outputs, the role of rule-based logic or probabilistic components, and any material assumptions or	High Risk AI Systems

Number	Category	Title	Requirement	Applicability
			constraints affecting the results.	
B.AI.4.2	Transparency and Explainability	Information on Training Data Sources and Model Logic	To the extent necessary to support transparency and explainability, the Supplier shall provide information regarding the categories and sources of training data and the general logic of the model(s) used in the AI System, subject to the protection of legitimate confidentiality and security interests. The Supplier shall ensure that such information is sufficient to enable the Customer to understand relevant system behaviours and limitations.	All
B.AI.4.3	Transparency and Explainability	Communication of System Capabilities and Limitations	The Supplier shall document and communicate the known capabilities and limitations of the AI System relevant to its Intended Use(s), including foreseeable scenarios in which the system may underperform or produce unreliable results. This documentation shall support appropriate use of the AI System-.	All
B.AI.5	Human Oversight	Human Oversight by Design	The Supplier shall ensure that the AI System is designed and developed in a manner that enables effective oversight by	All

Number	Category	Title	Requirement	Applicability
			natural persons, proportionate to the risks associated with the AI System and its Intended Use(s). This shall include the ability for designated persons to understand system behaviour, detect anomalies or undesired outcomes, and take appropriate action where necessary. The Supplier shall document the oversight mechanisms implemented and make such documentation available to the Customer upon request.	
B.AI.5.1	Human Oversight	Allocation of Responsibility for AI System Outcomes	The Supplier shall ensure that responsibility for the operation and outcomes of the AI System is clearly assigned within the organisation. This shall include responsibility for overseeing system performance, addressing identified risks, and coordinating remediation measures where issues arise. The Supplier shall document the allocation of responsibilities and the associated authority to intervene.	All
B.AI.5.2	Human Oversight	Training and Awareness	The Supplier shall support awareness among relevant personnel of the capabilities, limitations, and appropriate use of the	All

Number	Category	Title	Requirement	Applicability
			AI System, including known constraints that may affect system performance or reliability and the risks of using the AI System. The Supplier shall document the measures implemented to support such awareness and make relevant documentation available to the Customer upon request.	
B.AI.5.3	Human Oversight	Capability to Intervene, Override, or Disable AI System Functions	Where appropriate in light of the risks associated with the AI System, the Supplier shall ensure that mechanisms are in place to allow for timely human intervention, including the ability to override, suspend, or disable specific functions of the AI System. The Supplier shall document the conditions under which such intervention may occur and the procedures for exercising these controls.	All
B.AI.5.4	Human Oversight	Escalation and Remediation Procedures	The Supplier shall establish and maintain procedures for escalating AI-related risks, incidents, or failures to appropriate decision-making levels within the organisation.	High Risk AI Systems
B.AI.6	Performance, Robustness and Security of AI Systems	Accuracy and Performance of AI Systems	The Supplier shall ensure that the AI System achieves and maintains a level of accuracy and	All

Number	Category	Title	Requirement	Applicability
			performance appropriate to its Intended Use(s) and the risks associated with its deployment. The Supplier shall define relevant performance metrics and, where appropriate, acceptable error ranges for the AI System. The Supplier shall document how such metrics are measured and monitored and shall furnish documentary evidence to the Customer upon request.	
B.AI.6.1	Performance, Robustness and Security of AI Systems	Robustness and Reliability of AI Systems	The Supplier shall design, develop, and operate the AI System to be sufficiently robust and reliable for its Intended Use(s), taking into account foreseeable variations in input data, operational conditions, and user behaviour. The Supplier shall document measures implemented to support robustness and reliability, including any known limitations.	All
B.AI.6.2	Performance, Robustness and Security of AI Systems	Safety and Predictable Failure Modes	Where relevant in light of the AI System's Intended Use(s), the Supplier shall identify and document foreseeable failure modes of the AI System and assess their potential impact. The Supplier shall implement measures to reduce the likelihood and severity of	High Risk AI Systems

Number	Category	Title	Requirement	Applicability
			harmful or unsafe outcomes arising from such failures.	
B.AI.6.3	Performance, Robustness and Security of AI Systems	AI-Specific Security and Protection Against Misuse	The Supplier shall implement measures to protect the AI System against AI-specific security risks and misuse, including, where relevant, risks related to manipulation of system behaviour, inference abuse, or unauthorised exploitation of system outputs. Such measures shall be proportionate to the risks associated with the AI System	All
B.AI.6.4	Performance, Robustness and Security of AI Systems	Red Teaming and Adversarial Testing	Where appropriate in light of the risks associated with the AI System, the Supplier shall conduct red teaming or other adversarial testing activities prior to deployment to identify vulnerabilities, potential misuse, or failure modes. Identified vulnerabilities shall be addressed before deployment of the AI System.	High Risk AI Systems
B.AI.6.5	Performance, Robustness and Security of AI Systems	Consistency of Performance Over the AI System Lifecycle	The Supplier shall ensure that the AI System performs consistently with the documented accuracy, robustness, and safety characteristics throughout its lifecycle. Where material	All

Number	Category	Title	Requirement	Applicability
			deviations from expected performance are identified, the Supplier shall assess the causes and take appropriate corrective measures.	
B.AI.7	Bias and Harm Prevention	Identification of Bias and Potential Harm	The Supplier shall identify and assess potential sources of bias and harm associated with the AI System, including risks of differential or adverse impacts on specific individuals or demographic groups in light of the Intended Use(s) and operational context. The Supplier shall document the assumptions, factors, and system characteristics considered in this assessment and make such documentation available to the Customer upon request.	All
B.AI.7.1	Bias and Harm Prevention	Management and Mitigation of Algorithmic Bias	Where bias or risk of harm is identified, the Supplier shall implement appropriate measures to mitigate such bias or reduce the likelihood of harmful outcomes, proportionate to the risks associated with the AI System. The Supplier shall document the mitigation measures implemented and provide evidence demonstrating how identified bias is	High Risk AI Systems

Number	Category	Title	Requirement	Applicability
			managed in the context in which the AI System is deployed.	
B.AI.7.2	Bias and Harm Prevention	Assessment of Differential Performance Across Groups	Where relevant to the Intended Use(s) of the AI System, the Supplier shall assess whether the AI System exhibits materially different performance characteristics across demographic groups or other relevant categories. Where performance differences are identified, the Supplier shall document the factors contributing to such differences and any measures taken to address or justify them.	High Risk AI Systems
B.AI.8	Monitoring and Incident Response	Ongoing Monitoring of AI System Behaviour	The Supplier shall establish and maintain processes to monitor the behaviour and performance of the AI System during operation, considering its Intended Use(s) and associated risks. Monitoring activities shall be designed to detect deviations from expected behaviour, degradation in performance, or other issues that may affect the reliability, safety, or appropriateness of the AI System. The Supplier shall document the monitoring processes implemented and make such documentation	All

Number	Category	Title	Requirement	Applicability
			available to the Customer upon request.	
B.AI.8.1	Monitoring and Incident Response	Detection and Handling of AI-Related Incidents	The Supplier shall establish and maintain processes for the identification, assessment, and handling of AI-related incidents, including incidents that may result in unintended, harmful, or non-compliant system behaviour. Such processes shall support timely analysis of the causes and potential impacts of incidents and the implementation of appropriate corrective measures. The Supplier shall maintain records of AI-related incidents.	All
B.AI.8.2	Monitoring and Incident Response	Communication and Notification of Significant Issues	Where significant issues affecting the behaviour, performance, or risk profile of the AI System are identified, the Supplier shall communicate relevant information to the Customer without undue delay, to the extent necessary to support appropriate risk management and oversight.	All
B.AI.8.3	Monitoring and Incident Response	Corrective Actions and Remediation Measures	The Supplier shall implement appropriate corrective actions to address identified issues,	All

Number	Category	Title	Requirement	Applicability
			failures, or deviations in the behaviour of the AI System.	
B.AI.9	Supply Chain	AI Supply Chain and Third-Party Management	The Supplier shall establish a process to ensure that all third-party components (e.g., base models, APIs, datasets, or software libraries) align with the Responsible AI requirements. The Supplier shall perform due diligence on AI sub-processors and maintain a record of their compliance.	All

5 Cloud Enablement Security Requirements

This section contains a set of information security requirements intended to support the Norwegian public sector with “security in the cloud”, supported by the vendor’s reference architecture, specific national legal and regulatory requirements, and other security related services.

This section is a collection of identified optional cloud requirements and is not necessarily intended to be applied in full. It is recommended that only requirements relevant for the scope in question are included in procurement and / or contract documents.

Number	Title	Requirement
C.1	Security Architecture	The Supplier is requested to document its security architecture(s) and how it can be applied by the Customer. The security architecture should be aligned with industry best practice security architecture concepts, such as zero trust and defendable/defensible security architecture and established cyber security frameworks, such as NIST Cybersecurity framework v2.0 or equivalent.
C.2	Secure Cloud Adoption (“Security-in-the-cloud")	The Supplier should enable secure configuration, deployment, and operation of the cloud services in an automated fashion with the purpose of reducing security risks from an end-to-end perspective. If applicable, propose relevant landing zones for the Service in scope.
C.3	Governance and Compliance Dashboard	The Supplier should provide a security/ compliance/ trust portal or dashboard that provides access to relevant security policies and up-to-date access to Customer security and compliance information.
C.4	Governance and Compliance Matrix – International Standards and Frameworks	The Supplier should provide a compliance matrix for the Service(s) to document compliance to common international legal frameworks and security standards/ frameworks, such as NIS2, GDPR, ISO 27001/2, ISO 27017, NIST CSF, HIPAA, CSA-CCM, FedRamp, and C5.
C.5	Governance and Compliance Matrix – National	The Supplier should provide a compliance matrix for the Service(s) to document compliance with national security laws/ regulations and security frameworks, such as “lov om digital sikkerhet“, “NSM Grunnprinsipper for IKT-sikkerhet”, and “Normen”.

Number	Title	Requirement
	Standards and Frameworks	
C.6	Security in multi-cloud and hybrid cloud environments	The Supplier should enable end-to-end security in multi-cloud and hybrid cloud environments, for example: • Extending security tools / services to other cloud services (SaaS/PaaS/IaaS). • Integrating security tools / services with the security tools / services of other cloud services.
C.7	Cryptography	The Supplier should provide mechanisms / services for encryption to enable effective encryption of Customer data at rest and in transit with customer-managed / customer-owned cryptographic keys. The Supplier should document its roadmap to ensure that cryptographic algorithms used in the Service are quantum resistant, in accordance with, e.g., CNSA 2.0 ("Commercial National Security Algorithm Suite 2.0"), NIST standards for post-quantum cryptography, “NSMs veileder for kvantemigrering”, “NSMs kryptografiske anbefalinger (utkast 2024)”, or similar.
C.8	Legal and Regulatory - Personnel Security	The Supplier should be able to meet legal and regulatory requirements related to personnel security, as mandated by laws and regulations, including: • National security clearance of personnel • Police certificate of personnel The Supplier should describe how they can support such requirements at the time of implementation or subsequently based on regulatory changes.
C.9	National Location[6]	The Supplier should be able to offer the Service, or a subset of the Service, from Norway. This includes using infrastructure and resources within Norway. The Supplier should also be able to limit the processing of Customer Data to Norway. This means no transfer of any Customer Data outside Norway, including for support services, except when obligated by law.

[6] Must assess in each case if there is a legitimate basis for thisequirement, ref. EU/EEA-law, etc.

Number	Title	Requirement
C.10	EU/EEA Location[7]	The Supplier should be able to offer the Service, or a subset of the Service, from EU/EEA. This includes using infrastructure and resources within EU/EEA. The Supplier should also be able to limit the processing of Customer Data to EU/EEA. This means no transfer of any Customer Data outside EU/EEA, including support services, except when obligated by law.
C.11	Training and Awareness	The Supplier should be able to provide training and awareness services. Describe how the Supplier can provide services and programs for training and awareness to enable secure cloud adoption for the Customer and for strengthening the security culture in the Customer's organization.
C.12	Professional Services	The Supplier should be able to provide professional services. Describe how the Supplier can provide implementation services to support a secure cloud implementation in compliance with the proposed security reference architecture.

[7] Must assess in each case if there is a legitimate basis for this requirement, ref. EU/EEA-law, etc.

6 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.

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).

6.1 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)	NIS2 Directive	NIS2 Implementing Regulation Annex
A.1 Purpose	• GV.OC Organizational Context (GV.OC-01, 02, 04, 05,)	• 4.1 Understanding the organization and its context • 4.2 Understanding the needs and expectation	• Not applicable	• Not applicable	• Not applicable	• Not applicable	• Art. 20 Governance • Art. 21.2(a) policies on risk analysis and information system security	• 1.1.1 Policy on the security of network and information systems

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
		s 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)	• 6.1.1 General	• Not applicable	• 1.1 Identify management structures, deliverables and supporting systems (1.1.2, 1.1.3, 1.1.4, 1.1.5) • 2.1 Include security during procurement and development	• GRC Governance, Risk and Compliance (GRC-02, GRC-04) • TVM Threat & Vulnerability Management (TVM-01) • CCC Change Control and Configuration	• OIS-06 Risk management policy • OIS-07 Application of the risk management policy	• Art. 20 Governance • Art. 21.2(a) policies on risk analysis and information system security • Art. 21.2(e) security in network and information systems acquisition, development and	• 1 .1.1 Policy on the security of network and information systems • 2.1.1, 2.1.2, 2.1.3, 2.1.4 Risk management framework • 6.1.1 Security in acquisition of ICT services or ICT products

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
	• GV.RA Risk Assessment (ID.RA-05, 06, 07)			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)	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)		maintenance, including vulnerability handling and disclosure • Art. 21.2(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures	• 7.1.1, 7.1.2, 7.1.3 POLICIES AND PROCEDURES TO ASSESS THE EFFECTIVENESS OF CYBERSECURITY RISK-MANAGEMENT MEASURES (ARTICLE 21(2), POINT (F), OF DIRECTIVE (EU) 2022/2555

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
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)	• AM-02 Acceptable Use and Safe Handling of Assets Policy • AM-06 Asset Classification and Labelling • PI-02 Contractual agreements for the provision of data • COM-01 Identification of applicable legal, regulatory, self-imposed or contractual requirement • PSS-12 Locations of Data	• Not applicable	• Not applicable

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
						Processing and Storage		
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)	• COM-01 Identification of applicable legal, regulatory, self-imposed or contractual requirements • COM-03 Internal audits of the information security management system	• Not applicable	• Not applicable
A.5 Documentation	• Not applicable	• 7.5 Documented information	• 5.37 Documented operating procedure • 6.8 Information security	• Not applicable	• BCR Business Continuity Management and Operational Resilience (BCR-05)	• SP-01 Documentation, communication and provision of policies and instructions	• Art. 21.2(a) policies on risk analysis and information system security	• 1.1.1 Policy on the security of network and information systems

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
			event reporting			• DEV-08 Version Control		
A.6 Notification	• Not applicable	• Not applicable	• 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)	• Not applicable	• SIM-01 Policy for security incident management • SIM-04 Duty of the users to report security incidents to a central body • SIM-05 Evaluation and learning process • INQ-02 Informing Cloud Customers about Investigation Requests	• Art. 21.2(b) incident handling • Art. 21.2(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers • Art. 23 Reporting obligations	• 3.1.1, 3.1.2 Incident handling policy • 5.1.4 Supply chain security policy

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
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	• Not applicable	• 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)	• PI-02 Contractual agreements for the provision of data • COM-02 Policy for planning and conducting audits • COM-03 Internal audits of the information security management system • INQ-01 Legal Assessment of Investigative Inquiries • INQ-02 Informing Cloud Customers	• Art. 21.2(a) policies on risk analysis and information system security • Art. 21.2(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	• 1.1.1 Policy on the security of network and information systems • 2.3.1 Independent review of information and network security • 5.1.4 Supply chain security policy

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
						about Investigation Requests • INQ-03 Conditions for Access to or Disclosure of Investigation Requests • INQ-04 Limiting Access to or Disclosure of Data in Investigation Requests		
A.8 Governance	• GV.RR Roles, Responsibilities, and Authorities (GV.RR-01, 02) • GV.RM Risk Manageme	• 5.1 Leadership and Commitment • 5.3 Organizational roles, responsibili	• 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)	• OIS-04 Segregation of Duties • SP-01 Documentation, communication and provision of	• Art. 20 Governance • Art. 21.2(a) policies on risk analysis and information system security	• 1.1.1 Policy on the security of network and information systems • 1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.2.6 Roles,

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
	nt Strategy (GV.RM-05) • GV.SC Cybersecurity Supply Chain Risk Management (GV.SC-02)	ties and authorities • 7.1 Resources				policies and instructions • SP-02 Review and Approval of Policies and Instructions • SP-03 Exceptions from Existing Policies and Instructions • SSO-03 Directory of service providers and suppliers	• Art. 21.2(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	responsibilities and authorities • 5.2 Directory of suppliers and service providers

6.2 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)	NIS2 Directive	NIS2 Implementing Regulation Annex
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)	• COM-01 Identification of applicable legal, regulatory, self-imposed or contractual requirements	• Not applicable	• Not applicable
B.IS.2 Security Governance – Information security management system	• GV.PO Policies, Processes, 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)	• OIS-01 Information Security Management System (ISMS) • OIS-02 Information Security Policy • OIS-03 Interfaces and	• Art. 21.2(a) policies on risk analysis and information system security • Art. 21.2(e) security in network and information systems	• 1.1.1 Policy on the security of network and information systems • 2.1.1, 2.1.2, 2.1.3 2.1-4 Risk Management Framework • 6.1.1 Security in acquisition

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
						Dependencies • OIS-06 Risk Management Policy • OIS-07 Application of the Risk Management Policy • COM-04 Information on information security performance and management assessment of the ISMS	acquisition, development and maintenance, including vulnerability handling and disclosure • Art. 21.2(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures	of ICT services or ICT products • 6.10.2 Vulnerability handling and disclosure • 7.1 7.2 7.3 POLICIES AND PROCEDURES TO ASSESS THE EFFECTIVENESS OF CYBERSECURITY RISK-MANAGEMENT MEASURES (ARTICLE 21(2), POINT (F), OF DIRECTIVE (EU) 2022/2555)
B.IS.3 Security	• Not applicable	• Not applicable	• GV.PO Policies,	• 2.1 Include security	• GRC Governance,	• COM-03 Internal	• Art. 21.2(a) policies on	• 1.1.1, 1.1.2, Policy on the

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
governance – Assurance			Processes, and Procedure (GV.PO-01)	during procurement and development processes (2.1.3, 2.1.10)	Risk and Compliance (GRC-07) • A&A Audit & Assurance (A&A-02, A&A-03)	audits of the information security management system	risk analysis and information system security • Art. 21.2(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	security of network and information systems • 2.2.1, 2.2.2 Compliance monitoring • 2.3.2 Independent review of information and network security • 6.1.2 Security in acquisition of ICT services or ICT products
B.IS.4 Security Governance – Security audit and	• ID.IM Improvement (ID.IM-01, 02, 03, 04)	• 9.2.2 Internal audit program • 9.2.1 Internal	• 5.35 Independent review of information security	• Not applicable	• Audit & Assurance (A&A-02, A&A-03, A&A-05) • STA Supply Chain	• COM-02 Policy for planning and conducting audits	• Art. 21.2(a) policies on risk analysis and information	• 1.1.1, 1.1.2 Policy on the security of network and information systems

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
testing obligations – regular security audits and testing		audit general	• 8.34 Protection of information systems during audit testing		Management, Transparency, and Accountability (STA-11)	• COM-03 Internal audits of the information security management system	system security • Art. 21.2(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	• 2.2.1, 2.2.3 Compliance monitoring • 2.3.2, 2.3.4 Independent review of information and network security • 6.1.2 Security in acquisition of ICT services or ICT products • 6.5.1, 6.5.2 6.5.3 Security Testing
B.IS.5 Security governance – security audit and testing obligations –	• ID.IM Improvement (ID.IM-02, 03)	• 9.2.2 Internal audit program • 10.2 non-conformity and corrective action	• 5.35 Independent review of information security • 8.34 Protection of information	• Not applicable	• A&A Audit & Assurance (A&A-06)	• COM-02 Policy for planning and conducting audits • COM-03 Internal audits of the information	• Art. 21.2(a) policies on risk analysis and information system security • Art. 21.2(e) security in	• 2.3.3 Independent review of information and network security 6.5.2 Security testing

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
documentation and remediation		• 10.1 Continual improvement	systems during audit testing			security management system	network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	
B.IS.6 Security governance – Access to security documents	• Not applicable	• 5.2 Policy • 7.5 Documented information	• 5.1 Policies for information security • 5.37 Documented operating procedures	• Not applicable	• BCR Business Continuity Management and Operational Resilience (BCR-05)	• OIS-02 Information Security Policy • SP-02 Review and Approval of Policies and Instructions • SP-03 Exceptions from Existing	• Art. 21.2(a) policies on risk analysis and information system security	• 1.1.1, 1.1.2 Policy on the security of network and information systems

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
						Policies and Instructions		
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)	• Not applicable	• 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 supplier agreements	• 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)	• HR-06 Confidentiality agreements • DEV-01 Policies for the development / procurement of information systems • DEV-02 Outsourcing of the development • SSO-01 Policies and instructions for controlling and monitoring third parties	• Art. 21.2(a) policies on risk analysis and information system security • Art. 21.2(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	• 1.2.2 Roles, responsibilities and authorities • 5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.1.6, 5.1.7 Supply chain security policy • 6.1.1, 6.1.2, 6.1.3 Security in acquisition of ICT services or ICT products • 6.1.2 Security in acquisition of ICT services or ICT products

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
			• 5.21 Managing information security in the ICT supply chain • 5.20 Addressing information security within supplier agreements • 6.6 Confidentiality or non-disclosure agreements • 8.30 Outsourced development			• SSO-02 Risk assessment of service providers and suppliers • SSO-03 Directory of service providers and suppliers	• Art. 21.2(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	
B.IS.8 Security governance – Third	• Not applicable	• Not applicable	• 5.22 Monitoring, review and change	• Not applicable	• DCS Data Center Security (DCS-02)	• SSO-04 Monitoring of compliance	• Not applicable	• Not applicable

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
party security management ownership and operations of data centres and infrastructure			management of supplier services			with requirements • PSS-12 Locations of Data Processing and Storage		
B.IS.9 Cooperation regarding information security – information security responsible	• GV.RR Roles, Responsibilities, and Authorities (GV.RR-01, 02, 03, 05)	• 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) • SEF Security Incident Management, E-Discovery & Cloud Forensics (SEF-08)	• Not applicable	• Art. 21.2(a) policies on risk analysis and information system security • Art. 21.2(d) supply chain security, including security-related aspects	• 1.1.1 Policy on the security of network and information systems • 1.2.1 – 1.2.6 Roles, responsibilities and authorities • 5.2 Directory of suppliers and service providers

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
							concerning the relationships between each entity and its direct suppliers or service providers	
B.IS.10 Cooperation regarding information security - information security responsible – summoning meetings	• GV.RM Risk management strategy (GV.RM-05)						• Not applicable	• Not applicable

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
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 (RS.MA-01, 02, 03, 04, 05) • RS.AN Incident Analysis (RS.AN-03, 06, 07, 08)	• Not applicable	• 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 monitoring (3.3.6) • 4.1 Prepare the organisation for incidents (4.1.1, 4.1.2,	• SEF Security Incident Management, E-Discovery & Cloud Forensics (SEF-01 to SEF-07)	• OPS-13 Logging and Monitoring – Identification of Events • SIM-01 Policy for security incident management • SIM-02 Processing of security incidents • SIM-03 Documentation and reporting of security incidents • SIM-05 Evaluation and learning process	• Art. 21.2(b) incident handling	• 3.1.1 to 3.1.3 Incident handling policy • 3.4.1, 3.4.2 Event assessment and classification • 3.5.1, 3.5.2, 3.5.4, 3.5.5 Incident response • 3.6.1 Post-incident reviews

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
	• RS.MI Incident Mitigation (RS.MI-01, 02) • RC.RP Incident Recovery Plan Execution (RC.RP-01 to 06)			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 –	• DE.AE Adverse Event Analysis (DE.AE-04, 08)	• Not applicable	• 5.24 Information security incident management planning	• 1.3 Identify users and access requirements (1.3.3) • 3.3 Analyse data from	• SEF Security Incident Management, E-Discovery & Cloud Forensics (SEF-07)	• OPS-21 Involvement of Cloud customers in the event of incidents	• Art. 21.2(b) incident handling • Art. 21.2(d) supply chain security,	• 3.1.1, 3.1.2 Incident handling policy • 3.5.3 Incident response

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
Security incident management and threat intelligence – notification and documentation	• RC.CO Incident Recovery Communication (RC.CO-04)		and preparation • 5.28 Collection of evidence • 6.8 Information security event reporting	security monitoring (3.3.6) • 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)		• SIM-01 Policy for security incident management • SIM-02 Processing of security incidents • SOM-03 Documentation and reporting of security incidents • SIM-04 Duty of the users to report security incidents to a central body • INQ-02 Informing Cloud Customers about Investigation Requests	including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers • Art. 23 Reporting obligations	• 5.1.4 Supply chain security policy

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
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)	• Not applicable	• Not applicable	• 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	• Not applicable	• Not applicable	• Art. 21.2(b) incident handling	• 3.1.1, 3.1.2 Incident handling policy

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
				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)	• Not applicable	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)	• Not applicable	• OPS-10 Logging and Monitoring – Concept • OPS-11 Logging and Monitoring – Metadata Management Concept • OPS-12 Logging and Monitoring – Access, Storage and Deletion • OPS-14 Logging and Monitoring – Storage of	• Not applicable	Not applicable

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
						the Logging Data • OPS-15 Logging and Monitoring – Accountability • OPS-16 Logging and Monitoring – Configuration • PSS-01 Guidelines and Recommendations for Cloud Customers		
B.IS.15 Incident, Asset and Vulnerability Management - Security incident	• ID.RA Risk Assessment (ID.RA-02, 03) • DE.AE Adverse Event Analysis (DE.AE-07)	• Not applicable	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	• Not applicable	• OPS-04 Protection Against Malware – Concept • OPS-05 Protection Against Malware -	• Not applicable	• Not applicable

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
management and threat intelligence - Threat Intelligence				monitoring (3.3.4)		Implementation		
B.IS.16 Incident, Asset and Vulnerability Management - Security incident management and threat intelligence - Malicious Software	• ID.RA Risk Assessment (ID.RA-09)	• Not applicable	• 8.7 Protection against malware	• 2.1 Include security during 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)	• TVM Threat & Vulnerability Management (TVM-02)	• OPS-05 Protection Against Malware - Implementation	• Art. 21.2(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	• 6.9.1, 6.9.2 Protection against malicious and unauthorised software

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
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)	• Not applicable	• 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 associated assets	• 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 during procurement and development processes (2.1.1, 2.1.2, 2.1.3) • 2.2 Establish a secure ICT architecture (2.2.6)	• HRS Human Resources (HRS-02, HRS-05) • CCC Change Control and Configuration Management (CCC-04) • DCS Data Center Security (DCS-01, DCS-04, DCS-05, DCS-06) • UEM Universal Endpoint Management (UEM-01, UEM-02, UEM-04) • DSP Data Security and Privacy Lifecycle Management	• AM-01 Asset Inventory • AM-02 Acceptable Use and Safe Handling of Assets Policy • AM-03 Commissioning of Hardware • AM-04 Decommissioning of Hardware • AM-05 Commitment to Permissible Use, Safe Handling and Return of Assets • AM-06 Asset Classificatio	Art. 21.2(i) human resources security, access control policies and asset management	• 12.1.1 to 12.1.3 Asset classification • 12.2.1 to 12.2.3 Handling of assets • 12.3.1 to 12.3.3 Removeble media policy • 12.4.1 to 12.4.3 Asset inventory • 12.5 Deposit, return or deletion of assets upon termination of employment

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
			• 5.10 Acceptable use of information and other associated assets	• 2.3 Maintain a secure configuration (2.3.10)	(DSP-02 to DSP-06)	n and Labelling • PI-03 Secure deletion of data		
B.IS.18 Incident, Asset and Vulnerability Management - Asset and Vulnerability Management – Vulnerability Management	• ID.RA Risk Assessment (ID.RA-01, 08)	• Not applicable	• 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 vulnerabilities and threats (3.1.1)	• TVM Threat & Vulnerability Management (TVM-01, TVM-03, TVM-03, TVM-07, TVM-08, TVM-10) • AIS Application & Interface Security (AIS-07)	• OPS-18 Managing Vulnerabilities, Malfunctions and Errors – Measurements, Analyses and Assessments of Procedures • OPS-22 Testing and Documentation of known Vulnerabilities • PSS-02 Identification	• Art. 21.2(c) business continuity, such as backup management and disaster recovery, and crisis management • Art. 21.2(e) security in network and information systems acquisition,	• 4.3.3 Crisis management • 6.6.1, 6.6.2 Security patch management • 6.10.1, 6.10.2, 6.10.3 Vulnerability handling and disclosure

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
						of Vulnerabilities of the Cloud Service	development and maintenance, including vulnerability handling and disclosure	
B.IS.19 Incident, Asset and Vulnerability Management - Asset and Vulnerability Management – third-party vulnerabilities	• ID.RA Risk Assessment (ID.RA-05)	• Not applicable	• 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)	• Not applicable	• Art. 21.2(c) business continuity, such as backup management and disaster recovery, and crisis management • Art. 21.2(e) security in network and information systems acquisition,	• 4.3.3 Crisis management • 6.10.1, 6.10.2 6.10.4 Vulnerability handling and disclosure

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
							development and maintenance, including vulnerability handling and disclosure	
B.IS.20 Incident, Asset and Vulnerability Management - Asset and Vulnerability Management – Vulnerability Identification and Scoring	• Not applicable	• Not applicable	• Not applicable	• Not applicable	• TVM Threat & Vulnerability Management (TVM-01, TVM-09)	• OPS-18 Managing Vulnerabilities, Malfunctions and Errors – Concepts • OPS-20 Managing Vulnerabilities, Malfunctions and Errors – Measurements, Analyses and Assessments of Procedures	• Art. 21.2(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	• 6.10.1, 6.10.2 Vulnerability handling and disclosure

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
						• DEV-02 Outsourcing of the development • PSS-02 Identification of Vulnerabilities of the Cloud Service • PSS—03 Online Register of Known Vulnerabilities		
B.IS.21 Incident, Asset and Vulnerability Management - Asset and Vulnerability Managem	• ID.RA Risk Assessment (ID.RA-05)	• Not applicable	• Not applicable	• Not applicable	• TVM Threat & Vulnerability Management (TVM-01, TVM-09)	• OPS-18 Managing Vulnerabilities, Malfunctions and Errors – Concepts • OPS-20 Managing Vulnerabilities,	• Art. 21.2(d) supply chain security, including security-related aspects concerning the relationship	• 5.1.4 Supply chain security policy • 6.10.1- 6.10.3 Vulnerability handling and disclosure

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
ent – Vulnerability Notification						Malfunctions and Errors – Measurements, Analyses and Assessments of Procedures • PSS-01 Guidelines and Recommendations for Cloud Customers • PSS-02 Identification of Vulnerabilities of the Cloud Service • PSS-03 Online Register of Known Vulnerabilities	s between each entity and its direct suppliers or service providers • Art. 21.2(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
B.IS.22 Incident, Asset and Vulnerability Management - Suspension of service due to security incidents and vulnerabilities	• Not applicable	• Not applicable	• Not applicable	• 4.3 Control and manage incidents (4.3.2)	• TVM Threat & Vulnerability Management (TVM-01)	• OPS-19 Managing Vulnerabilities, Malfunctions and Errors – Concept • OPS-20 Managing Vulnerabilities, Malfunctions and Errors – Measurements, Analyses and Assessments of Procedures	• Art. 21.2(b) incident handling • Art. 21.2(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	• 3.1.1 Incident handling policy • 8.10.1 and 8.10.2 Vulnerability handling and disclosure
B.IS.23 Incident, Asset and Vulnerability Management – Penetratio	• ID.IM Improvement (ID.IM-02)	• Not applicable	• Not applicable	• 3.4 Perform penetration tests (3.4.1 to 3.4.6)	• TVM Threat & Vulnerability Management (TVM-06)	• Not applicable	• Art. 21.2(e) security in network and information systems acquisition, development and	• 6.5.1 to 6.5.3 Security testing

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
n testing rights							maintenance, including vulnerability handling and disclosure	
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)	• Not applicable	• 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	• IAM Identity & Access Management (IAM-01 to IAM-07, IAM-09, IAM-10, IAM-13 to IAM-16) • DCS Datacenter Security (DCS-08)	• PS-04 Physical site access control • OPS-06 Data Protection and Recovery • OPS-12 Logging and Monitoring – Access, Storage and Deletion • IDM-01 Policy for user accounts and access rights • IDM-02 Granting and change of user	• Art. 21.2(a) policies on risk analysis and information system security • Art. 21.2(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling	• 1.1.1 Policy on the security of network and information systems • 6.7.2 Network security • 11.1.1 to 11.1.3 Access control policy • 11.2.1 to 11.2.3 Management of access rights • 11.3.1 to 11.3.3 Privileged

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
				access rights (2.6.1 to 2.6.7)		accounts and access rights • IDM-03 Locking and withdrawal of user accounts in the event of inactivity or multiple failed loggings • IDM-04 Withdraw or adjust access rights as the task area changes • IDM-06 Privileged access rights • IDM-08 Confidentiality of	and disclosure • Art. 21.2(i) human resources security, access control policies and asset management • Art. 21.2(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured	accounts and system administration accounts • 11.4.1 and 11.4.2 Administration systems • 11.6.1 to 11.6.4 Authentication • 11.7.1 and 11.7.2 Multi-factor authentication

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
						authentication information • IDM-09 Authentication mechanisms • PSS-01 Guidelines and Recommendations for Cloud Customers • PSS-05 Authentication Mechanisms • PSS-08 Roles and Rights Concept • PSS-09 Authorisation	emergency communication systems within the entity, where appropriate	

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
						Mechanisms		
B.IS.25 Access Control and Customer Data – Security Access Management – Regular Access Reviews	• Not applicable	• Not applicable	• Not applicable	• 2.6 Control identities and access rights (2.6.1)	• IAM Identity & Access Management (IAM-01, IAM-08)	• IDM-05 Regular review of access rights?	• Art. 21.2(i) human resources security, access control policies and asset management	• 11.1.3 Access control policy • 11.2.3 Management of access rights • 11.3.3 Privileged accounts and system administration accounts
B.IS.26 Access Control and Customer Data - Flexible and fine-grained identity and access managem	• PR.AA Identity Management, Authentication, and Access Control (PR.AA-01 to 04)	• Not applicable	• 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 Data Center Security (DCS-08)	• IDM-02 Granting and change of user accounts and access rights • IDM-03 Locking and withdrawal of user accounts in the event of	• Art. 21.2(i) human resources security, access control policies and asset management	• 11.5.1 to 11.5.4 Identification

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
ent – Customer Identity and Access Management						inactivity or multiple failed logins • IDM-04 Withdraw or adjust access rights as the task area changes • IDM-05 Regular review of access rights • IDM-06 Privileged access rights		
B.IS.27 Access Control and Customer Data - Flexible and fine-grained identity and access	• Not applicable	• Not applicable	• 5.23 Information security for use of cloud services • 5.18 Use of privileged utility programs	• Not applicable	• IAM Identity & Access Management (IAM-01, IAM-04)	• Not applicable	• Not applicable	• Not applicable

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
management – Standards for Cross-domain Identity Management			• 8.20 Networks security • 8.24 Use of cryptography • 5.17 Authentication information • 8.5 Secure authentication • 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	• 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)	• HRS Human Resources (HRS-04) • IVS Infrastructure & Virtualization Security (IVS-03, IVS-07, IVS-09)	• IDM-08 Confidentiality of authentication information • IDM-09 Authentication mechanisms	• Art. 21.2(e) security in network and information systems acquisition, development and maintenance, including	• 6.7.2 Network security • 11.6.1 to 11.6.4 Authentication • 11.7.1 and 11.7.2 Multi-factor

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
			• 8.20 Networks security • 8.21 Security of network services	• 2.5 Control data flow (2.5.2, 2.5.5, 2.5.7)		• COS-01 Technical safeguards • COS-03 Monitoring of connections in the Cloud Service Provider's network • COS-04 Cross-network access • PSS-01 Guidelines and Recommendations for Cloud Customers • PSS-05 Authentication Mechanisms • PSS-07 Confidentialit	vulnerability handling and disclosure • Art. 21.2(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption • Art. 21.2(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communica	authentication

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
						y of Authentication Information • PSS-08 Roles and Rights - Concept	tions and secured emergency communication systems within the entity, where appropriate	
B.IS.29 Access Control and Customer Data - Separation of Customer Data	• PR.DS Data Security (PR.DS-05, 09)	• Not applicable	• 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)	• DSP Data Security and Privacy Lifecycle Management (DSP-01) • AIS Application & Interface Security (AIS-01, AIS-03) • IVS Infrastructure & Virtualization Security (IVS-06)	• PS-04 Physical site access control • OPS-15 Logging and Monitoring – Accountability • OPS-24 Separation of Datasets in the Cloud Infrastructure • IDM-07 Access to cloud	• Art. 21.2(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	• 6.8.1 to 6.8.3 Network segmentation

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
				• 2.2 Establish a secure ICT architecture (2.2.3) • 2.3 Maintain a secure configuration (2.3.10) • 2.5 Control data flow (2.5.1)		customer data • COS-01 Technical safeguards • COS-02 Security requirements for connections in the Cloud Service Provider's network • COS-04 Cross-network access • COS-05 Networks for administration • COS-06 Segregation of data traffic in jointly used network		

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
						environments • COS-08 Policies for data transmission		
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)	• Not applicable	• 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 Data Center Security (DCS-02) • UEM Universal Endpoint Management (UEM-08, UEM-11) • DSP Data Security and Privacy Lifecycle Management	• OPS-06 Data Protection and Recovery – Concept • OPS-16 Logging and Monitoring – Configuration • IDM-07 Access to cloud customer data • CRY-01 Policy for the use of encryption procedures and key management • CRY-02 Encryption of	• Not applicable	• Not applicable

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
					(DSP-01, DSP-10, DSP-17)	data for transmission (transport encryption) • CRY-03 Encryption of sensitive data for storage • CRY-04 Secure key management • PSS-01 Guidelines and Recommendations for Cloud Customers • PSS-05 Authentication Mechanisms • PSS-07 Confidentiality of Authentication Information		

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
						• PSS-08 Roles and Rights Concept		
B.IS.31 Encryption of Customer Data – State of the Art Encryption	• Not applicable	• Not applicable	• 8.20 Network 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)	• OPS-06 Data Protection and Recovery – Concept • CRY-01 Policy for the use of encryption procedures and key management • CRY-02 Encryption of data for transmission (transport encryption) • CRY-03 Encryption of	• Art. 21.2(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption • Art. 21.2(j) the use of multi-factor authentication or continuous authentication solutions,	• 9.1 to 9.3 CRYPTOGRAPHY (ARTICLE 21(2), POINT (H), OF DIRECTIVE (EU) 2022/2555) • 11.8.1 to 11.8.4 Authentication • 11.7.1 and 11.7.2 Multi-factor authentication

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
						sensitive data for storage • CRY-04 Secure key management	secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate	
B.IS.32 Access Control and Customer Data - Encryption of Customer Data – Quantum Resistant Cryptogra	• Not applicable	• Not applicable	• 8.24 Use of cryptography	• Not applicable	• CEK Cryptography, Encryption & Key Management (CEK-07)	• OPS-06 Data Protection and Recovery – Concept • CRY-01 Policy for the use of encryption procedures and key management • CRY-02 Encryption of data for	• Art. 21.2(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption	• 9.1 to 9.3 CRYPTOGRAPHY (ARTICLE 21(2), POINT (H), OF DIRECTIVE (EU) 2022/2555)

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
phic Algorithms						transmission (transport encryption) • CRY-03 Encryption of sensitive data for storage • CRY-04 Secure key management		
B .IS.33 Access Control and Customer Data - Logging of access to Customer Data	• PR.PS Platform Security (PR.PS-04)	• Not applicable	• 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	• OPS-10 Logging and Monitoring – Concept • OPS-11 Logging and Monitoring – Metadata Management Concept • OPS-12 Logging and Monitoring – Access, Storage and Deletion	• Art. 21.2(b) incident handling	• 3.2.1 to to 3.2.4, 3.2.6, 3.2.7 Monitoring and logging

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
					Management (DSP-01)	• OPS-14 Logging and Monitoring – Storage of the Logging Data • OPS-15 Logging and Monitoring – Accountability • OPS-16 Logging and Monitoring – Configuration • IDM-07 Access to cloud customer data • PSS-04 Error handling and Logging Mechanisms		

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
B.IS.34 Access Control and Customer Data - Logging of access to Customer Data – Retention Period	• Not applicable	• Not applicable	• 8.10 Information deletion • 8.15 Logging	• 3.2 Establish security monitoring (3.2.2)	• Not applicable	• AM-04 Decommissioning of Hardware • OPS-10 Logging and Monitoring – Concept • OPS-11 Logging and Monitoring – Metadata Management Concept • OPS-12 Logging and Monitoring – Access, Storage and Deletion • OPS-14 Logging and Monitoring – Storage of the Logging Data	• Art. 21.2(b) incident handling	• 3.2.5 Monitoring and logging

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
						• OPS-15 Logging and Monitoring Accountability • OPS-16 Logging and Monitoring – Configuration • PI-02 Contractual agreements for the provision of data		
B.IS.35 Access Control and Customer Data - Notification of relocation of	• Not applicable	• Not applicable	• 5.14 Information transfer	• Not applicable	• DCS Data Center security (DCS-02) • DSP Data Security and Privacy Lifecycle Management (DSP-01)	• IDM-07 Access to cloud customer data • COS-08 Policies for data transmission • PSS-12 Locations of	• Art. 21.2(c) business continuity, such as backup management and disaster recovery, and crisis	• 4.2.2 Backup and redundancy

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
Customer Data						Data Processing and Storage	management	
B.IS.36 Change Management and Security by Design – Change Management	• Not applicable	• Not applicable	• 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)	• DEV-03 Policies for changes to information systems • DEV-05 Risk assessment, categorisation and prioritisation of changes • DEV-06 Testing changes • DEV-07 Logging of changes • DEV-08 Version Control • DEV-09 Approvals of provision in the	• Art. 21.2(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	• 6.4.1 to 6.4.4 Change management, repairs and maintenance • 6.10.2 Vulnerability handling and disclosure

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
					• AIS Application & Interface Security (AIS, 04, AIS-06)	production environments		
B.IS.37 Change Management and Security by Design – Change Management – Advance Notice	• Not applicable	• Not applicable	• 8.32 Change Management • 6.3 Planning of Changes	• Not applicable	• CCC Change Control and Configuration Management (CCC-02)	• DEV-03 Policies and changes to information systems • DEV-05 Risk assessment, categorisation and prioritisation of changes • DEV-06 Testing changes • DEV-07 Logging of changes • DEV-08 Version control • DEV-09 Approvals for	• Not applicable	• Not applicable

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
						provision in the production environment		
B.IS.38 Change Management and Security by Design – Security by Design	• ID.RA Risk Assessment (ID.RA-09)	• Not applicable	• 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	• 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	• AM-03 Commissioning of Hardware • OPS-16 Logging and Monitoring – Configuration • OPS-23 Managing Vulnerabilities, Malfunctions and Errors – System Hardening • COS-03 Monitoring of connections in the Cloud Service Provider's network	• Art. 21.2(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	• 6.2.1 and 6.2.4 Secure development life cycle • 6.3.1 to 6.3.3 Configuration management • 6.7.1 to 6.7.3 Network security

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
			management		Security (AIS-02) • LOG Logging and Monitoring (LOG-06)	• COS-07 Documentation of the network topology • PI-01 Documentation and safety of input and output interfaces • DEV-01 Policies for the development / procurement of information systems • PSS-01 Guidelines and Recommendations for Cloud Customers		

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
B.IS.39 Change Management and Security by Design – Security by Design – Testing	• ID.IM Improvement (ID.IM-02)	• Not applicable	• 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 & Interface Security (AIS-05) • CCC Change Control and Configuration Management (CCC-02)	• DEV-01 Policies for the development / procurement of information systems • DEV-02 Outsourcing of the development • DEV-06 Testing changes	• Art. 21.2(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	• 6.2.1, 6.2.2, 6.2.4 Secure development life cycle
B.IS.40 Change Management and Security by Design – Standards and Best Practices	• Not applicable	• Not applicable	• 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 Management (CCC-06) • IVS Infrastructure & Virtualization Security (IVS-04)	• DEV-01 Policies for the development / procurement of information systems	• Art. 21.2(b) incident handling • Art. 21.2(e) security in network and information systems acquisition, developme	• 3.2.6 Monitoring and logging • 6.2.2 Secure development life cycle

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
					• DSP Data Security and Privacy Lifecycle Management (DSP-07, DSP-08)		nt and maintenance, including vulnerability handling and disclosure	
B.IS.41 Business Continuity – Business Continuity and Disaster Recovery	• PR.IR Technology Infrastructure Resilience (PR.IR-03)	• Not applicable	• 8.14 Redundancy of information processing facilities • 5.29 Information security during disruption • 5.30 ICT readiness for business continuity	• 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)	• PS-02 Redundancy model • OPS-06 Data Protection and Recovery – Concept • OPS-07 Data Backup and Recovery – Monitoring • OPS-09 Data Backup and Recovery – Storage • OPS-17 Logging and Monitoring – Availability of the	• Art. 21.2(c) business continuity, such as backup management and disaster recovery, and crisis management • Art. 21.2(e) security in network and information systems acquisition, developme	• 4.1.1 to 4.1.4 Business continuity and disaster recovery plan • 13.1.1 to 13.1.3 Supporting utilities • 13.2.1 to 13.23 Protection against physical and environmental threats

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
						Monitoring Software • BCM-01 Top management responsibility • BCM-02 Business impact analysis policies and instructions • BCM-03 Planning business continuity • BCM-04 Verification, updating of the business continuity	nt and maintenance, including vulnerability handling and disclosure • Art. 21.2(i) human resources security, access control policies and asset management	
B.IS.42 Business Continuity – Business Continuity and Disaster	• PR.IR Technology Infrastructure Resilience	• Not applicable	• 8.6 Capacity Management	• 2.2 Establish a secure ICT architecture (2.2.7)	• IVS Infrastructure & Virtualization Security (IVS-02)	• OPS-01 Capacity Management – Planning • OPS-02 Capacity	• Art. 21.2(c) business continuity, such as backup management and	• 4.1.2 Business continuity and disaster recovery plan

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
Recovery – Capacity Management					• BCR Business Continuity Management and Operational Resilience (BCR-11)	Management – Monitoring • OPS-03 Capacity Management – Controlling and Resources	disaster recovery, and crisis management • Art. 21.2(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure • Art. 21.2(i) human resources security, access control policies and	• 4.2.4, 4.2.5 Backup and redundancy management • 13.1.1, 13.1.2, 13.1.3 Supporting utilities

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
							asset management	
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)	• Not applicable	• 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)	• OPS-06 Data Protection and Recovery – Concept • OPS-07 Data Backup and Recovery – Monitoring • OPS-08 Data Backup and Recovery – Regular Testing • OPS-09 Data Backup and Recovery - Storage	• Art. 21.2(c) business continuity, such as backup management and disaster recovery, and crisis management	• 4.2.1, 4.2.2, 4.2.3, 4.2.6 Backup and redundancy management
B.IS.44 Physical and Personnel Security – Physical Security	• PR.AA Identity Management, Authentication, and Access	• Not applicable	• 7.13 Equipment maintenance • 8.1 User endpoint devices	• 2.1 Include security during procurement and development	• DCS Data Center Security (DCS-03, DCS-07, DCS-09 to DCS-15)	• PS-01 Physical Security and Environmental Control Requirements	• Art. 21.2(i) human resources security, access control policies and	• 11.1.1 to 11.1.3 Access control policy • 13.3.1 to 13.3.3

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
	Control (PR.AA-06) • PR.IR Technology Infrastructure Resilience (PR.IR-02) • DE.CM Continuous Monitoring (DE.CM-02, 03)		• 7.1 Physical security perimeters • 7.5 Protecting against physical and 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	processes (2.1.4) • 2.4 Protect the organisation's networks (2.4.2, 2.4.3)		• PS-03 Perimeter Protection • PS-04 Physical site access control • PS-05 Protection against threats from outside and from the environment • PS-06 Protection against interruptions caused by power failures and other such risks	asset management	Paramater and physical access control

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
			• 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)	• Not applicable	• Not applicable	• Not applicable	• A&A Audit & Assurance (A&A-02, A&A-03)	• PS-01 Physical Security and Environmental Control Requirements	• Art. 21.2(c) business continuity, such as backup management and disaster recovery, and crisis management • Art. 21.2(e) security in network and information systems acquisition, development and	• 11.1.3 Access control policy • 13.3.3 Parameter and physical access control

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
							maintenance, including vulnerability handling and disclosure • Art. 21.2(i) human resources security, access control policies and asset management	
B.IS.46 Physical and Personnel Security – Personnel Security	• GV.RR Roles, Responsibilities, and Authorities (GV.RR-04) • PR.AT Awareness and Training	• 7.2 Competence • 7.3 Awareness	• 5.4 Management responsibilities • 6.3 Information security awareness, education and training	• Not applicable	• DCS Data Center Security (DCS-11) • HRS Human Resources (HRS-03, HRS-05 to HRS-13)	• HR-02 Employment terms and conditions • HR-03 Security training and awareness programme	• Art. 21.2(d) supply chain security, including security-related aspects concerning the relationship	• 5.1.4 Supply chain security policy • 8.1.1 to 8.1.3 Awareness raising and basic cyber hygiene practices

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
	(PR.AT-01, 02)		• 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			• HR-04 Disciplinary measures • HR-05 Responsibilities in the event of termination or change of employment • HR-06 Confidentiality agreement • DEV-04 Safety training and awareness programme regarding continuous software delivery and associated systems, components or tools. • SSO-01 Policies and	s between each entity and its direct suppliers or service providers • Art. 21.2(g) basic cyber hygiene practices and cybersecurity training • Art. 21.2(i) human resources security, access control policies and asset management	• 8.2.1 to 8.2.5 Security training • 10.1.1, 10.1.2 Human resources security

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
						instructions for controlling and monitoring third parties.		
B.IS.47 Physical and Personnel Security – Personnel Security – Security Screening and Clearance	• GV.RR Roles, Responsibilities, and Authorities (GV.RR-04)	• Not applicable	• 6.1 Screening	• Not applicable	• HRS Human Resources (HRS-01)	• HR-01 Verification of qualifications and trustworthiness	• Art. 21.2(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers • Art. 21.2(i) human resources	• 5.1.4 Supply chain security policy • 10.1.2 Human resources security • 10.2.1 to 10.2.3 Verification of background

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
							security, access control policies and asset management	
B.IS.48 Physical and Personnel Security – Personnel Security – Audits	• ID.IM Improvement (ID.IM-02)	• Not applicable	• Not applicable	• Not applicable	• A&A Audit & Assurance (A&A-02, A&A-03)	• Not applicable	• Art. 21.2(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers • Art. 21.2(i) human	• 5.1.4 Supply chain security policy • 10.1.3 Human resources security

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
							resources security, access control policies and asset management	

6.3 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)	NIS2 Directive	NIS2 Implementing Regulation Annex
C.1 Security Architecture	• Not applicable	• Not applicable	• 8.27 Secure system architecture and engineering principles	• Identify management structures, deliverables and supporting systems (1.1.5, 1.1.-6)	• IVS Infrastructure & Virtualization Security (IVS-08, IVS-09,	• DEV-01 Policies for the development / procurement of information systems	• Art. 21.2(e) security in network and information systems acquisition, development and	• 6.2.2 Secure development life cycle • 6.7.2 Network security

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
				• 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)		• PSS-06 Session management • PSS-10 Software-defined networking • PSS-11 Images for Virtual Machines and Containers	maintenance, including vulnerability handling and disclosure	
C.2 Secure Cloud Adoption	• PR.PS Platform Security (PR.PS-01, 02, 03, 06)	• Not applicable	• 8.9 Configuration management	• 1.1 Identify management structures, deliverables and	• IVS Infrastructure & Virtualization	• AM-03 Commissioning of Hardware	• Not applicable	• Not applicable

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
			• 5.23 Information security for use of cloud services • 8.25 Secure development life cycle • 8.31 Separation of development, test, and production environments	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)	Security (IVS-01)	• AM-04 Decommissioning of Hardware • OPS-16 Logging and Monitoring – Configuration • OPS-23 Managing Vulnerabilities and Errors – System Hardening • COS-03 Monitoring of connections in the Cloud Service Provider's Network • PI-01 Documentation and safety of input and output interfaces		

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
						• DEV-01 Policies for the development / procurement of information systems • DEV-10 Separation of environments • SSO-05 Exist strategy for the receipt of benefits • PSS-01 Guidelines and Recommendations for Cloud Customers		
C.3 Governance and	• Not applicable	• 5.2 Policy	• Not applicable	• Not applicable	• Not applicable	• Not applicable	• Art. 21.2(a) policies on risk analysis	• Policy on the security of network and

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
Compliance Dashboard		• 7.4 Communication					and information system security • Art. 21.2(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures	information systems • 2.2.2 Compliance monitoring
C.4 Governance and Compliance Matrix – International Standards and Frameworks	• GV.OC Organizational Context (GV.OC-03)	• 8.1 Operational planning and control	• 5.31 Legal, statutory, regulatory and contractual requirements	• Not applicable	• GRC Governance, Risk and Compliance (GRC-07)	• COM-01 Identification of applicable legal, regulatory, self-imposed or contractual requirements	• Not applicable	• Not applicable

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
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	• Not applicable	• GRC Governance, Risk and Compliance (GRC-07)	• COM-01 Identification of applicable legal, regulatory, self-imposed or contractual requirements	• Not applicable	• Not applicable
C.6 Security in multi-cloud and hybrid cloud environments	• Not applicable	• Not applicable	• 8.7 Protection against malware	• 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)	• OPS-05 Protection Against Malware - Implementation	• Not applicable	• Not applicable
C.7 Cryptography	• Not applicable	• Not applicable	• 8.24 Use of cryptography	• 2.7 Protect data at rest and in transit (2.7.1 to 2.7.5)	• CEK Cryptography, Encryption & Key	• OPS-06 Data Protection and Recovery – Concept	• Art. 21.2(h) policies and procedures regarding the use of	• 9.1 to 9.3 CRYPTOGRAPHY (ARTICLE 21(2), POINT (H), OF

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
				• 2.9 Establish capability to restore data (2.9.5)	Management (CEK-07)	• IDM-07 Access to cloud customer data • CRY-01 Policy for the use of encryption procedures and key management • CRY-02 Encryption of data for transmission (transport encryption) • CRY-03 Encryption of sensitive data for storage • CRY-04 Secure key management	cryptography and, where appropriate, encryption	DIRECTIVE (EU) 2022/2555)
C.8 Legal and Regulator	• GV.RR Roles, Responsibili	• Not applicable	• 6.1 Screening	• Not applicable	• Not applicable	• HR-01 Verification of	• Art. 21.2(i) human resources	• 10.2.2 Verification

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
y – Personnel security	ties, and Authorities (GV.RR-04)					qualification and trustworthiness	security, access control policies and asset management	of background
C.9 National Location	• Not applicable	• Not applicable	• 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)	• OPS-06 Data Protection and Recovery – Concept • OPS-12 Logging and Monitoring – Access, Storage and Deletion • IDM-07 Access to cloud customer data • COS-08 Policies for data transmission	• Not applicable	• Not applicable

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
						• SSO-03 Directory of service providers and suppliers • PSS-08 Roles and Rights – Concept • PSS-12 Locations of Data Processing and Storage		
C.10 EU / EEA Location	• Not applicable	• Not applicable	• 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)	• OPS-06 Data Protection and Recovery – Concept • OPS-12 Logging and Monitoring – Access, Storage and Deletion • IDM-07 Access to cloud	• Not applicable	• Not applicable

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
						customer data • COS-08 Policies for data transmission • SSO-03 Directory of service providers and suppliers • PSS-08 Roles and Rights – Concept • PSS-12 Locations of Data Processing and Storage		
C.11 Training and Awareness	• GV.RR Roles, Responsibilities, and Awareness (GV.RR-04)	• Not applicable	• 6.3 Information security awareness, education and training	• 4.1 Prepare the organisation for incidents (4.1.3)	• HRS Human Resources (HRS-11, HRS-12) • DCS Data Center Security (DCS-11)	• HR-03 Security training and awareness programme • DEV-04 Safety training and	• Art. 21.2(g) basic cyber hygiene practices and cybersecurity training	• 8.1.1 to 8.1.3 Awareness raising and basic cyber hygiene practices

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)	NIS2 Directive	NIS2 Implementing Regulation Annex
			• 7.7 Clear desk and clear screen • 8.7 Protection against malware			awareness programme		• 8.2.1 to 8.2.5 Security training
C.12 Professional Services	• Not applicable	• Not applicable	• Not applicable	• Not applicable	• Not applicable	• Not applicable	• Not applicable	• Not applicable

References

Abbreviation	Title	Source
C5	BSI Cloud Computing Compliance Criteria Catalogue	https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html
CIS	CIS Critical Security Controls v8.1	https://www.cisecurity.org/controls
CNSA 2.0	Commercial National Security Algorithm Suite 2.0	https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF
CSA-CCM	Cloud Security Alliance Cloud Controls Matrix Version 4	https://cloudsecurityalliance.org/research/cloud-controls-matrix
CVE	Common Vulnerabilities and Exposures	https://www.cve.org/
CVSS	Common Vulnerability Scoring System (CVSS) v4.0	https://www.first.org/cvss/
CWE Top 25	CWE Top 25 Most Dangerous Software Weaknesses	https://cwe.mitre.org/top25/
EPSS	Exploit Prediction Scoring system	Exploit Prediction Scoring System (EPSS)
FedRamp	US Federal Risk and Authorization Management Program	https://www.fedramp.gov/
GAPP	Generally accepted privacy principles (2009). See PMF – Privacy Management Framework for updated version.	https://us.aicpa.org/interestareas/informationtechnology/privacy-management-framework
GDPR	General Data Protection Regulation 2016/679	https://eur-lex.europa.eu/eli/reg/2016/679/oj
HIPAA	Health Insurance Portability and Accountability Act	https://www.hhs.gov/hipaa/index.html
IETF RFC 7643	IETF RFC 7643 System for Cross-domain Identity Management: Core Schema	https://datatracker.ietf.org/doc/html/rfc7643

Abbreviation	Title	Source
ISO 22123	ISO/IEC 22123-1:2023 Information Technology – Cloud Computing	https://www.iso.org/standard/82758.html
ISO 22313	ISO 22313:2020 Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301	https://www.iso.org/standard/75107.html
ISO 27001	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements	https://www.iso.org/standard/27001
ISO 27002	ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls	https://www.iso.org/standard/75652.html
ISO 27017	ISO/IEC 27017:2015Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services	https://www.iso.org/standard/43757.html
ISO 27018	ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	https://www.iso.org/standard/76559.html
ISO 27701	ISO/IEC 27701:2019Security techniques — Extension to ISO/IEC 27001 and ISO/IEC	https://www.iso.org/standard/71670.html

Abbreviation	Title	Source
	27002 for privacy information management — Requirements and guidelines	
NSM Grunnprinsipper	NSM Grunnprinsipper for IKT-sikkerhet 2.1	https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/ta-i-bruk-grunnprinsippene/
NSM kryptografiske anbefalinger	NSM kryptografiske anbefalinger (utkast 2024)	https://nsm.no/fagomrader/digital-sikkerhet/kryptosikkerhet/kryptografiske-anbefalinger/
NSM veileder kvantemigrasjon	NSM veileder kvantemigrasjon	https://nsm.no/fagomrader/digital-sikkerhet/kryptosikkerhet/kvantemigrasjon/kvantemigrasjon-veileder/kvantemigrasjon/
NIST CSF 2.0	NIST Cyber Security Framework 2.0	https://www.nist.gov/cyberframework
NIST PQC	NIST Post Quantum Cryptography	https://csrc.nist.gov/projects/post-quantum-cryptography
NIS2	Network & Information Security Directive 2022/2555	https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32022L2555
NIS2 Implementing Regulations	NIS2 Implementing Regulations	https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng
Normen	Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren versjon 6.0	https://www.ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren
OWASP Top 10	Open Worldwide Application Security Project Top 10 Web Application Security Risks	https://owasp.org/www-project-top-ten/
OWASP ASVS	Open Worldwide Application Security Project Application Security Verification Standard (ASVS)	https://owasp.org/www-project-application-security-verification-standard/
PMF	Privacy Management Framework	https://us.aicpa.org/interestareas/informationtechnology/privacy-management-framework
Sabsa	Sabsa Enterprise Security Architecture	https://sabsa.org/
SAML 2.0	Security Assertion Markup Language 2.0	https://www.oasis-open.org/standard/saml/

Abbreviation	Title	Source
SCIM 2	System for Cross-domain Identity Management 2.0	https://scim.cloud/
SOC2 Type 2	American Institute of Certified Public Accountants (AICPA) SOC 2 Type II Report	https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services

Direktoratet for forvaltning og økonomistyring

www.dfo.no