Direktoratet for forvaltning og økonomistyring

DFØ
August 2025

MPS Cloud Reference Architecture v1.1

Information Security and Data Protection 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 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 – v1.1 - incorporates BSI's C5:2020 (Cloud Computing Compliance Criteria Catalogue) in the compliance mapping tables.

We hope this comes to good use!

Content

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	**I**nformation 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 obligation**s –** 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.

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, such as NIS2 and NIS2 implementing regulations.

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

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)
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 expectations of interested parties				

		• 6.2 Information security objectives and planning to achieve them				
A.2 Purpose	• GV.OV Oversight (GV.OV-01, 02, 03) • GV.PO Policies, Processes, and Procedures (GV.PO-01) • GV.RM Risk Management Strategy (GV.RM-01, 02, 03, 04, 06, 07) • GV.RA Risk Assessment (ID.RA-05, 06, 07)	• 6.1.1 General		• 1.1 Identify management structures, deliverables and supporting systems (1.1.2, 1.1.3, 1.1.4, 1.1.5) • 2.1 Include security during procurement and development processes (2.1.4, 2.1.9) • 2.2 Establish a secure ICT architecture (2.2.7) • 2.3 Maintain a secure configuration (2.3.10)	• GRC Governance, Risk and Compliance (GRC-02, GRC-04) • TVM Threat & Vulnerability Management (TVM-01) • CCC Change Control and Configuration Management (CCC-03) • CEK Cryptography , Encryption & Key Management (CEK-07) • STA Supply Chain Management, Transparency , and	• OIS-06 Risk management policy • OIS-07 Application of the risk management policy

					• Accountability (STA-08) • BCR Business Continuity Management and Operational Resilience (BCR-02)	
A.3 Compliance	• OV.OC Organizational Context (GV.OC-03)	• 8.1 Operational Planning and Control	• 5.4 Management Responsibilities • 5.10 Acceptable use of information and other associated assets • 5.31 Legal, statutory, regulatory, and contractual requirements	• 3.2 Establish security monitoring (3.2.2)	• A&A Audit & Assurance (A&A-04)	• 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 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
A.5 Documentation		• 7.5 Documented information	• 5.37 Documented operating procedure • 6.8 Information security event reporting		• BCR Business Continuity Management and Operational Resilience (BCR-05)	• SP-01 Documentation, communication and provision of policies and instructions • DEV-08 Version Control

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

					• SEF Security Incident Management, E-Discovery & Cloud Forensics (SEF-08)	• COM-03 Internal audits of the information security management system • INQ-01 Legal Assessment of Investigative Inquiries • INQ-02 Informing Cloud Customers 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 Management Strategy (GV.RM-05) • GV.SC Cybersecurity Supply Chain Risk Management (GV.SC-02)	• 5.1 Leadership and Commitment • 5.3 Organizational roles, responsibilities and authorities • 7.1 Resources	• 5.2 Information security roles and responsibilities • 5.3 Segregation of duties	• 1.3 Identify users and access requirements (1.3.3) • 4.1 Prepare the organisation for incidents (4.1.3)	• GRC Governance, Risk and Compliance (GRC-06)	• OIS-04 Segregation of Duties • SP-01 Documentation, communication and provision of 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

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)
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, regulator, self-imposed or contractual requirements
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 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 •
B.IS.3 Security governance – Assurance			• GV.PO Policies, Processes, and Procedure (GV.PO-01)	• 2.1 Include security during procurement and development processes (2.1.3, 2.1.10)	• GRC Governance, Risk and Compliance (GRC-07) • A&A Audit & Assurance (A&A-02, A&A-03)	• COM-03 Internal audits of the information security management system •
B.IS.4 Security Governance – Security audit and testing obligations – regular security audits and testing	• ID.IM Improvement (ID.IM-01, 02, 03, 04)	• 9.2.2 Internal audit program • 9.2.1 Internal audit general	• 5.35 Independent review of information security • 8.34 Protection of information systems during audit testing		• Audit & Assurance (A&A-02, A&A-03, A&A-05) • STA Supply Chain Management, Transparency, and Accountability (STA-11)	• COM-02 Policy for planning and conducting audits • COM-03 Internal audits of the information security management system
B.IS.5 Security governance	• ID.IM Improvemen	• 9.2.2 Internal	• 5.35 Independent review of		• A&A Audit & Assurance (A&A-06)	• COM-02 Policy for planning and

– security audit and testing obligations – documentation and remediation	t (ID.IM-02, 03)	audit program • 10.2 non-conformity and corrective action • 10.1 Continual improvement	information security • 8.34 Protection of information systems during audit testing			conducting audits • COM-03 Internal audits of the information security management system
B.IS.6 Security governance – Access to security documents		• 5.2 Policy • 7.5 Documented information	• 5.1 Policies for information security • 5.37 Documented operating procedures		• BCR 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 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)		• 8.26 Application security requirements • 5.19 Information security in supplier relationships • 5.21 Managing	• 2.1 Include security during procurement and development processes (2.1.2, 2.1.3, 2.1.4, 2.1.9, 2.1.10,)	• STA Supply Chain Management, Transparency, and Accountability (STA-01 to STA-12) • UEM Universal Endpoint	• HR-06 Confidentiality agreements • DEV-01 Policies for the development / procurement of information systems

			information security in the ICT supply chain • 5.20 Addressing information security within supplier agreements • 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	• 4.1 Prepare the organisation for incidents (4.1.4)	Management (UEM-14)	• DEV-02 Outsourcing of the development • SSO-01 Policies and instructions for controlling and monitoring third parties • SSO-02 Risk assessment of service providers and suppliers • SSO-03 Directory of service providers and suppliers

B.IS.8 Security governance – Third party security management ownership and operations of data centres and infrastructure			• 5.22 Monitoring, review and change management of supplier services		• DCS Data Center Security (DCS-02)	• SSO-04 Monitoring of compliance 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)	
B.IS.10 Cooperation regarding information security - information security	• GV.RM Risk management strategy (GV.RM-05)					

responsible – summoning meetings						
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) • RS.MI Incident Mitigation		• 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, 4.1.3, 4.1.4, 4.1.5, 4.1.6)	• 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

	(RS.MI-01, 02) • RC.RP Incident Recovery Plan Execution (RC.RP-01 to 06)			• 4.2 Assess and categorize incidents (4.2.1, 4.2.2, 4.2.3) • 4.3 Control and manage incidents (4.3.1, 4.3.2, 4.3.3, 4.3.5, 4.3.6) • 4.4 Evaluate and learn from incidents (4.4.1, 4.4.2, 4.4.3, 4.4.4)		
B.IS.12 Incident, Asset and Vulnerability Management – Security incident management and threat intelligence – notification and documentation	• DE.AE Adverse Event Analysis (DE.AE-04, 08) • RC.CO Incident Recovery Communication (RC.CO-04)		• 5.24 Information security incident management planning and preparation • 5.28 Collection of evidence • 6.8 Information security event reporting	• 1.3 Identify users and access requirements (1.3.3) • 3.3 Analyse data from security monitoring (3.3.6) • 4.1 Prepare the organisation for incidents (4.1.5)	• SEF Security Incident Management, E-Discovery & Cloud Forensics (SEF-07)	• OPS-21 Involvement of Cloud customers in the event of incidents • SIM-01 Policy for security incident management • SIM-02 Processing of security incidents • SOM-03 Documentation and reporting of

				• 4.2 Assess and categorise incidents (4.2.1, 4.2.2, 4.2.3, 4.3.5)		security incidents • SIM-04 Duty of the users to report security incidents to a central body • INQ-02 Informing Cloud Customers about Investigation Requests
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			• 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		

	and Communication (RS.CO-02, 03, 08)			organisation for incidents (4.1.4, 4.1.4) • 4.2 Assess and categorize incidents (4.2.3) • Control and manage incidents (4.3.5)		
B.IS.14 Incident, Asset and Vulnerability Management – Security incident management and threat intelligence – Access to security logs	• PR.PS Platform security (PR.PS-04)		8.15 Logging	• 3.2 Establish security monitoring (3.2.4) • 4.2 Assess and categorize incidents (4.2.1) • 4.3 Control and manage incidents (4.3.3)		• 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 • 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 management and threat intelligence - Threat Intelligence	• ID.RA Risk Assessment (ID.RA-02, 03) • DE.AE Adverse Event Analysis (DE.AE-07)		8.7 Protection against malware	• 3.1 Detect and remove known vulnerabilities and threats (3.1.2, 3.1.3) • 3.3 Analyse data from security monitoring (3.3.4)		• OPS-04 Protection Against Malware – Concept • OPS-05 Protection Against Malware - Implementation
B.IS.16 Incident, Asset and Vulnerability Management - Security incident management and threat intelligence - Malicious Software	• ID.RA Risk Assessment (ID.RA-09)		8.7 Protection against malware	• 2.1 Include security during procurement and development processes (2.1.2, 2.1.3, 2.1.4)	• TVM Threat & Vulnerability Management (TVM-02)	OPS-05 Protection Against Malware - Implementation

				• 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)		
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		• 5.11 Return of assets • 7.9 Security of assets off-premises • 7.10 Storage media • 7.14 Secure disposal or re-use of	• 1.1 Identify management structures, deliverables and supporting systems (1.1.3) • 1.2 Identify devices and software	• HRS Human Resources (HRS-02, HRS-05) • CCC Change Control and Configuration Management (CCC-04) • DCS Data	• AM-01 Asset Inventory • AM-02 Acceptable Use and Safe Handling of Assets Policy • AM-03 Commissioning of Hardware • AM-04 Decommissioning of Hardware

	(ID.RA-09)		equipment • 5.9 Inventory of information and other associated assets • 5.10 Acceptable use of information and other associated assets	(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) • 2.3 Maintain a secure configuration (2.3.10)	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 (DSP-02 to DSP-06)	• AM-05 Commitment to Permissible Use, Safe Handling and Return of Assets • AM-06 Asset Classification and Labelling • PI-03 Secure deletion of data
B.IS.18 Incident, Asset and Vulnerability Managemen	• ID.RA Risk Assessment		• 8.8 Management of technical	• 2.3 Maintain a secure configuration	• TVM Threat & Vulnerability Manage	• OPS-18 Managing Vulnerabilities, Malfunction

t - Asset and Vulnerability Management – Vulnerability Management	(ID.RA-01, 08)		vulnerabilities	(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)	ment (TVM-01, TVM-03, TVM-03, TVM-07, TVM-08, TVM-10) • AIS Application & Interface Security (AIS-07)	s and Errors – Measurements, Analyses and Assessments of Procedures • OPS-22 Testing and Documentation of known Vulnerabilities • PSS-02 Identification of Vulnerabilities of the Cloud Service
B.IS.19 Incident, Asset and Vulnerability Management - Asset and Vulnerability Management – third-party	• ID.RA Risk Assessment (ID.RA-05)	•	• 8.16 Monitoring activities • 8.30 Outsourced development	• 3.1 Detect and remove known vulnerabilities and threats (3.1.2)	• TVM Threat & Vulnerability Management (TVM-01, TVM-05, TVM-10)	

vulnerabilities						
B.IS.20 Incident, Asset and Vulnerability Management - Asset and Vulnerability Management – Vulnerability Identification and Scoring					• 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 • 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	• ID.RA Risk Assessment (ID.RA-05)				• TVM Threat & Vulnerability Management	• OPS-18 Managing Vulnerabilities, Malfunctions

Management - Asset and Vulnerability Management – Vulnerability Notification					(TVM-01, TVM-09)	and Errors – Concepts • OPS-20 Managing Vulnerabilities, 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
B.IS.22 Incident, Asset and Vulnerability Management - Suspension of service	•			• 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

due to security incidents and vulnerabilities						Vulnerabilities, Malfunctions and Errors – Measurements, Analyses and Assessments of Procedures
B.IS.23 Incident, Asset and Vulnerability Management - Penetration testing rights	• ID.IM Improvement (ID.IM-02)			• 3.4 Perform penetration tests (3.4.1 to 3.4.6)	• TVM Threat & Vulnerability Management (TVM-06)	
B.IS.24 Access Control and Customer Data – Security Access Management	• PR.AA Identity Management, Authentication, and Access Control (PR.AA-01, 02, 03, 04, 05) • PR.IR Technology Infrastructure Resilience (PR.IR-01)		• 8.3 Information access restriction • 5.15 Access control • 5.17 Authentication information • 5.18 Access rights • 8.5 Secure authentication • 8.2 Privileged access rights	• 1.3 Identify users and access requirements (1.3.1 to 1.3.3) • 2.2 Establish a secure ICT architecture (2.2.6) • 2.3 Maintain a secure configuration (2.3.7, 2.3.10) • 2.4 Protect the organisation’	• 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 accounts and access rights

				s networks (2.4.1, 2.4.2) • 2.6 Control identities and access rights (2.6.1 to 2.6.7)		• 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 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 Mechanisms
B.IS.25 Access Control and Customer Data – Security Access Management – Regular Access Reviews				• 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?
B.IS.26 Access Control and Customer Data - Flexible and fine-grained identity and access management – Customer Identity and Access Management	• PR.AA Identity Management, Authentication, and Access Control (PR.AA-01 to 04)		• 5.18 Access Rights • 8.2 Privileged access rights	• 1.3 Identify users and access requirements (1.3.1)	• IAM Identity & Access Management (IAM-01 to IAM-07, IAM-09 to IAM-11, IAM-13 to IAM-16) • DCS 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 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 management – Standards for Cross-domain Identity Management			• 5.23 Information security for use of cloud services • 5.18 Use of privileged utility programs • 8.20 Networks security • 8.24 Use of cryptography • 5.17 Authentication information • 8.5 Secure authentication • 8.20 Networks security		• IAM Identity & Access Management (IAM-01, IAM-04)	
B.IS.28 Access Control and Customer Data – Secure	• 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	• 2.3 Maintain a secure configuration (2.3.10) • 2.4 Protect the organisation’	• HRS Human Resources (HRS-04) • IVS Infrastructure & Virtualization	• IDM-08 Confidentiality of authentication information

Remote Access			• 6.7 Remote working • 8.20 Networks security • 8.21 Security of network services	s networks (2.4.1, 2.4.2, 2.4.4) • 2.5 Control data flow (2.5.2, 2.5.5, 2.5.7)	Security (IVS-03, IVS-07, IVS-09)	• IDM-09 Authentication mechanisms • 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 Confidentiality of Authentication Information • PSS-08 Roles and Rights - Concept

B.IS.29 Access Control and Customer Data - Separation of Customer Data	• PR.DS Data Security (PR.DS-05, 09)		• 8.12 Data leakage prevention • 8.22 Segregation of Networks	• 1.1 Identify management structures, deliverables and supporting systems (1.1.6) • 2.1 Include security during procurement and development of processes (2.1.10) • 2.2 Establish a secure ICT architecture (2.2.3) • 2.3 Maintain a secure configuration (2.3.10) • 2.5 Control data flow (2.5.1)	• 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 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 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)		• 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 (DSP-01, DSP-10, DSP-17)	• 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 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 • PSS-08 Roles and Rights Concept
B.IS.31 Encryption of Customer Data – State of the Art Encryption			• 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 sensitive data for storage • CRY-04 Secure key management
B.IS.32 Access Control and Customer Data - Encryption of Customer Data – Quantum Resistant Cryptographic Algorithms			• 8.24 Use of cryptography		• CEK Cryptography, Encryption & Key Management (CEK-07)	• 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 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)		• 8.5 Secure authentication • 8.15 Logging	• 3.2 Establish security monitoring (3.2.1 to 3.2.7)	• LOG Logging and monitoring (LOG-01 to LOG-05, LOG-07 to LOG-09, LOG-12, LOG-13) • IAM Identity & Access Management (IAM-12) • DSP Data Security and Privacy Lifecycle Management (DSP-01)	• 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 • 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 •
B.IS.34 Access Control and			• 8.10 Information deletion	• 3.2 Establish security		• AM-04 Decommissioning of Hardware

Customer Data - Logging of access to Customer Data – Retention Period			• 8.15 Logging	monitoring (3.2.2)		• 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 • 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 Customer Data			• 5.14 Information transfer		• 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 Data Processing and Storage

B.IS.36 Change Management and Security by Design – Change Management			• 8.32 Change Management	• 2.3 Maintain a secure configuration (2.3.5) • 2.10 Include security in the change management process (2.10.1 to 2.10.4) •	• CCC Change Control and Configuration Management (CCC-01 to CCC-05, CCC-07 to CCC-09) • CEK Cryptography, Encryption & Key Management (CEK-05) • Universal Endpoint Management (UEM-02, UEM-07) • IVS Infrastructure & Virtualization Security (IVS-05) • AIS Application & Interface Security (AIS, 04, AIS-06)	• 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 production environments
B.IS.37 Change Management and			• 8.32 Change Management • 6.3 Planning of Changes		• CCC Change Control and Configuration	• DEV-03 Policies and changes to information systems

Security by Design – Change Management – Advance Notice					Management (CCC-02)	• 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 provision in the production environment
B.IS.38 Change Management and Security by Design – Security by Design	ID.RA Risk Assessment (ID.RA-09)		• 8.9 Configuration management • 8.26 Application security requirements • 8.27 Secure system architecture and engineering principles • 8.25 Secure development life cycle	• 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	• 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)	• 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

			• 5.8 Information security in project management	and browsers (2.8.1 to 2.8.4)	• IVS Infrastructure & Virtualization Security (IVS-04) • AIS Application & Interface Security (AIS-02) • LOG Logging and Monitoring (LOG-06)	the Cloud Service Provider's network • 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
B.IS.39 Change Management and Security by Design – Security by Design – Testing	ID.IM Improvement (ID.IM-02)		• 8.25 Secure development life cycle • 8.29 Security testing in development and acceptance	• 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	• DEV-01 Policies for the development / procurement of information systems • DEV-02 Outsourcing of the development

			• 8.33 Test information		Management (CCC-02)	• DEV-06 Testing changes
B.IS.40 Change Management and Security by Design – Standards and Best Practices			• 8.4 Access to source code • 8.27 Secure system architecture and engineering principles • 8.28 Source coding	• 2.1 Include security during procurement and development processes (2.1.4, 2.1.5, 2.1.8)	• CCC Change Control and Configuration Management (CCC-06) • IVS Infrastructure & Virtualization Security (IVS-04) • DSP Data Security and Privacy Lifecycle Management (DSP-07, DSP-08)	• DEV-01 Policies for the development/ procurement of information systems
B.IS.41 Business Continuity – Business Continuity and Disaster Recovery	• PR.IR Technology Infrastructure Resilience (PR.IR-03)		• 8.14 Redundancy of information processing facilities • 5.29 Information security during disruption • 5.30 ICT readiness for	• 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

			business continuity			Recovery – Storage • OPS-17 Logging and Monitoring – Availability of the 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
B.IS.42 Business Continuity – Business Continuity and Disaster Recovery – Capacity Management	PR.IR Technology Infrastructure Resilience		• 8.6 Capacity Management	• 2.2 Establish a secure ICT architecture (2.2.7)	• IVS Infrastructure & Virtualization Security (IVS-02) • BCR Business Continuity Management and Operational	• OPS-01 Capacity Management – Planning • OPS-02 Capacity Management – Monitoring • OPS-03 Capacity Management – Controlling and Resources

					Resilience (BCR-11)	
B.IS.43 Business Continuity – Backup and Restore of the Supplier's Systems	• PR.DS Data Security (PR.DS-11) • RC.RP Incident Recovery Plan Execution (RC.RP-03)		• 8.13 Information backup	• 2.9 Establish capability to restore data (2.9.1 to 2.9.4)	BCR Business Continuity Management and Operational Resilience (BCR-08)	• 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
B.IS.44 Physical and Personnel Security – Physical Security	• PR.AA Identity Management, Authentication, and Access Control (PR.AA-06) • PR.IR Technology Infrastructure Resilience (PR.IR-02)		• 7.13 Equipment maintenance • 8.1 User endpoint devices • 7.1 Physical security perimeters • 7.5 Protecting against physical and environmental threats	• 2.1 Include security during procurement and development processes (2.1.4) • 2.4 Protect the organisation's networks (2.4.2, 2.4.3)	DCS Data Center Security (DCS-03, DCS-07, DCS-09 to DCS-15)	• PS-01 Physical Security and Environmental Control Requirements • PS-03 Perimeter Protection • PS-04 Physical site access control • PS-05 Protection against threats from outside and from the environment

	• DE.CM Continuous Monitoring (DE.CM-02, 03)		• 7.2 Physical entry • 7.3 Securing offices, rooms and facilities • 7.6 Working in secure areas • 7.8 Equipment siting and protection • 7.11 Supporting utilities • 7.12 Cabling security • 7.4 Physical security monitoring			• PS-06 Protection against interruptions caused by power failures and other such risks
B.IS.45 Physical and Personnel Security – Physical Security – Audits	• ID.IM Improvement (ID.IM-01, 02)				• A&A Audit & Assurance (A&A-02, A&A-03)	• PS-01 Physical Security and Environmental Control Requirements
B.IS.46 Physical and Personnel Security – Personnel Security	• GV.RR Roles, Responsibilities, and Authorities (GV.RR-04) • PR.AT Awareness	• 7.2 Competence • 7.3 Awareness	• 5.4 Management responsibilities • 6.3 Information security		• DCS Data Center Security (DCS-11) • HRS Human Resources (HRS-03,	• HR-02 Employment terms and conditions • HR-03 Security training and

	and Training (PR.AT-01, 02)		awareness, education and training • 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		HRS-05 to HRS-13)	awareness programme • 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 instructions for controlling and monitoring third parties.
B.IS.47 Physical and Personnel	• GV.RR Roles, Responsibilities, and		• 6.1 Screening		• HRS Human Resources (HRS-01)	• HR-01 Verification of qualifications

Security – Personnel Security – Security Screening and Clearance	Authorities (GV.RR-04)					and trustworthiness
B.IS.48 Physical and Personnel Security – Personnel Security – Audits	• ID.IM Improvement (ID.IM-02)				• A&A Audit & Assurance (A&A-02, A&A-03)	

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)
C.1 Security Architecture			• 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 • PSS-06 Session management • PSS-10 Software-defined networking

				• 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-11 Images for Virtual Machines and Containers
C.2 Secure Cloud Adoption	PR.PS Platform Security (PR.PS-01, 02, 03, 06)		• 8.9 Configuration management • 5.23 Information	• 1.1 Identify management structures, deliverables and supporting	• IVS Infrastructure & Virtualization Security (IVS-01)	• AM-03 Commissioning of Hardware • AM-04 Decommissioning of Hardware

			security for use of cloud services • 8.25 Secure development life cycle • 8.31 Separation of development, test, and production environments	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)		• 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 • 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 Compliance Dashboard		• 5.2 Policy • 7.4 Communication				
C4 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		• GRC Governance, Risk and Compliance (GRC-07)	• COM-01 Identification of applicable legal, regulatory, self-imposed or contractual requirements
C5 Governance and Compliance Matrix – National Standards and Frameworks	• GV.OC Organizational Context (GV.OC-03)	• 8.1 Operational planning and control	• 5.31 Legal, statutory, regulatory and contractual requirements		• GRC Governance, Risk and Compliance (GRC-07)	• COM-01 Identification of applicable legal, regulatory, self-imposed or contractual requirements
C.6 Security in multi-cloud and hybrid cloud			• 8.7 Protection against malware	• 1.1 Identify management structures, deliverable	• IPY Interoperability & Portability	• OPS-05 Protection Against Malware - Implementation

environments				s and supporting systems (1.1.5) • 2.2 Establish a secure ICT architecture (2.2.2)	(IPY-01 to IPY-04)	
C.7 Cryptography			• 8.24 Use of cryptography	• 2.7 Protect data at rest and in transit (2.7.1 to 2.7.5) • 2.9 Establish capability to restore data (2.9.5)	• CEK Cryptography, Encryption & Key Management (CEK-07)	• OPS-06 Data Protection and Recovery – Concept • 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

C.8 Legal and Regulatory – Personnel security	• GV.RR Roles, Responsibilities, and Authorities (GV.RR-04)		• 6.1 Screening			• HR-01 Verification of qualification and trustworthiness
C.9 National Location			• 8.3 Information access restriction • 5.14 Information transfer	• 3.2 Establish security monitoring (3.2.2)	• DSP Data Security and Privacy Lifecycle Management (DSP-19)	• 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 • 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			• 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 • 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)		• 6.3 Information security awareness, education and training • 7.7 Clear desk and clear screen • 8.7 Protection against malware	• 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 awareness programme
C.12 Professional Services						

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
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/
SCIM 2	System for Cross-domain Identity Management 2.0	https://scim.cloud/

Abbreviation	Title	Source
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

www.dfo.no