Direktoratet for forvaltning
og økonomistyring

DFØ
August 2024

Cloud Security Reference Architecture– Information Security Requirements

Information Security Requirements for Cloud Contracts v0.9

Preface

As the public sector adopts cloud services as a key enabler for its digital transformation, information security and data protection represent critical risk areas. At the same time, cyber security 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 Security Reference Architecture Information Security requirements. 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 "Cloud Security 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. This document represents a key part of the reference architecture – the information security 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 all requirements do not 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. The first new revision – version 1.0 - is planned during 2024, based on feedback on the current version and with the addition of additional elements such as mapping to laws, standards and frameworks (e.g., CSA-CCM and ISO 27001) vendor input forms, and the inclusion of relevant data protection requirements.

We hope this comes to good use!

Content

1 Introduction ... 3

1.1 Audience ... 3

1.2 Structure and Methodology ... 4

2 Principal Security Requirements ... 6

3 Basic Security Requirements ... 8

4 Optional Security Requirements ... 17

5 References ... 20

1 Introduction

This document contains the first version of the Cloud Security Reference Architecture Information Security 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 standardized-security requirements, enabling the public sector to set requirements and verify the security 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 “Cloud Security 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 “Cloud Security Reference Architecture” will be developed over time, and is intended to include information security and data protection requirements (this document), mapping to legal / regulatory requirements and security standards / frameworks (to be published as part of v1.0), vendor input and evaluation forms (to be published as part of v1.0), as well as the vendor’s 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 skews competition in a public procurement process should not be used unless this is based on legitimate needs and requirements, e.g. regulatory requirements.

This version of the document covers only information security. Data protection is planned to be added to the document in an updated version and is expected to be published during 2024.

1.1 Audience

The document and the outlined requirements are written for the Norwegian public sector and vendors of cloud services and is 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 guidance provided by the Norwegian[1] Public Sector Cloud Marketplace.

[1] markedsplassen.anskaffelser.no

1.2 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.

The requirements are based on international standards and frameworks (including ISO 27001 and NIST Cyber Security Framework v2.0, also referred to as NIST CSF), 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 security requirements:** A comprehensive set of information security requirements intended to be included as a security annex in cloud services agreements.
C. **Optional security requirements:** A set of optional information security requirements intended to support the Norwegian public sector with "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])

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

- Customer: The entity buying or consuming cloud services
- Supplier: The cloud service provider

2 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.

Number	Category	Requirement
A.1	Purpose	The Supplier acknowledges that information security is of critical importance to the Norwegian government and 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 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 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 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. The same applies to breaches 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 reviews; C) carry out data security and data protection 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.

3 Basic Security Requirements

This section contains a comprehensive set of information security requirements intended to be included as a security annex in cloud services agreements.

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 security 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.

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 or other substantially equivalent standard(s) for information security management and any updates to such standards; b) cloud specific frameworks, such as ISO 27017, ISO 27018, CCM-CSA, C5 and FedRAMP.
B.IS.2	Security Governance	Information security management system	The Supplier shall establish and maintain an effective information security management system that addresses 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.
B.IS.3	Security Governance	Assurance	Upon request by the Customer, the Supplier shall 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

[3] See also requirement A.4

			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. Upon request by the Customer, the Supplier shall provide specifications of the type of testing performed, including which business processes are in scope for the testing requirements, e.g., change management and release management, and the frequency of such testing.
B.IS.5	Security Governance	Security audit and security testing obligations – Documentation and Remediation	The Supplier shall address any issues identified in a security audit or security testing 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.
B.IS.6	Security Governance	Access to Security Documents	The Supplier shall upon request make available to the Customer security policies and related security 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 meet the security requirements set out in this Contract.
B.IS.8	Security Governence	Third Party Security Management – Ownership and Operations of Data Centres and Infrastructure	The Supplier shall notify the Customer in advance of any planned changes to the ownership or operation of the data centres or infrastructure used to deliver the Services. 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.
B.IS.9 [4]	Cooperation regarding Informa	Information security responsible	The Supplier shall appoint an information security responsible under the Contract as a counterpart to the Customer, who is responsible for strategic security meetings, reporting, and management of material risks, incidents, and

[4] See also requirement A.8

	tion Security		vulnerabilities. The Customer shall be entitled to escalate any issues to the responsible at executive level.
B.IS.10	Cooperation regarding information security	Information security responsible – 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 to 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 - Notifications and Documentation	In the event of a serious security incident or significantly increased threat to the information security relating to 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. The same applies to breaches 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 of 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	Security incident management and threat intelligence -	The Supplier shall maintain and on request from the Customer provide access to a security log of all incidents concerning Customer Data, including log data and relevant indicators of

[5] See also requirement A.6

	Management	Access to Security Logs	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 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 performance of the Service(s) is free of any malicious software.
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 in the Services. 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	Asset and Vulnerability Management – Vulnerability	Each vulnerability identified in the Service(s) shall be assigned a unique Common Vulnerability and Exposures (“CVE”) identifier and a Common Vulnerability Scoring System

	Management	Identification and Scoring	("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 notify the Customer without undue delay of any vulnerabilities identified in the Services 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.
B.IS.22	Incident, Asset and Vulnerability Management	Suspension of service due to security incidents and vulnerabilities	In the event of a serious security incident or vulnerability in 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 Services according to agreed routines, to identify and analyse any 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 personnel have access to the Service(s) and their management system. The policies must, at minimum, address privileged access management, password management, authentication, authorisation, provisioning, 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 facilitating integration with the Customer's existing identity and access management systems, such as user directories.
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) is secured with strong encryption and 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, encryption at rest and strong authentication.
B.IS.32	Access Control and Customer Data	Encryption of Customer Data – Quantum Resistant Cryptographic Algorithms	Cryptographic algorithms used by the Supplier as part of the Service should be quantum resistant, in accordance with CNSA 2.0 ("Commercial National Security Algorithm Suite 2.0") or equivalent.
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 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 Parties shall agree on a retention period for the access logs under the Contract, taking into account applicable Laws and regulations, as well as any recommendations from Norwegian national security and information security 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 data center or any other location.
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	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.

	by Design		
B.IS.38	Change Management and Security by Design	Security by Design	The Supplier shall implement and adhere to security by design principles in the provision 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 Personell Security	Physical Security	The Supplier shall implement and maintain appropriate physical security measures for its data centres, cloud infrastructure, operations environments (including remote operations), and any equipment installed on Customer premises, in accordance with relevant international standards and the Supplier's own policies.
B.IS.45	Physical and Personell 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 Personell 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 Personell 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 appropriate level of security clearance in accordance with best industry practice and any applicable laws.
B.IS.48	Physical and Personell 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 Optional Security Requirements

This chapter contains a set of optional 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 chapter 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. 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 to document compliance to common international legal frameworks and security standards/ frameworks, such as NIS2, GDPR, ISO27001/2, ISO27017, ISO 27018, ISO27701, NIST CSF, HIPAA, CSA-CCM, FedRamp, and C5.
C.5	Governance and Compliance Matrix – National Standards and Frameworks	The Supplier should provide a compliance matrix to document compliance with national security laws/ regulations and security frameworks, such as “sikkerhetsloven”, “lov om digital sikkerhet“, “arkivloven”, “regnskapsloven, “NSM Grunnprinsipper for IKT-sikkerhet”, and “Normen”.

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 encryption services to enable strong encryption of Customer data at rest and in transit with customer-managed / customer-owned cryptographic keys. The Supplier should document it roadmap to ensure that cryptographic algorithms used in the Service are quantum resistant, in accordance with CNSA 2.0 ("Commercial National Security Algorithm Suite 2.0") or equivalent. Describe how this is solved, including key encryption protocols, key management.
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.
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 data to EU/EEA. This means no transfer of any data outside

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

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

		EU/EEA, including for 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 a 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.

5 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/
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	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

ISO 22123	ISO/IEC 22123-1:2023 Information Technology – Cloud Computing	https://www.iso.org/standard/82758.html
ISO 22313	ISO 22313:2020Security 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 27002 for privacy information	https://www.iso.org/standard/71670.html

	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/
NIST CSF 2.0	NIST Cyber Security Framework 2.0	https://www.nist.gov/cyberframework
NIS2	Network & Information Security Directive	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/
SCIM 2	System for Cross-domain Identity Management 2.0	https://scim.cloud/
SOC2 Type 2	American Institute of Certified Public Accountants (AICPA) SOC 2 Type II Report	https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services

www.dfo.no