How to respond to non-functional requirement specification

Sheet	TEC CIS General	TEC General & User Requirements	TEC SLA Requirements	TEC Data Exchange	TEC Documentation	TEC AI
Description	Requirements related to general IT security, personnel certification, GDPR, etc.	Requirements relating to general technical prerequisites as well as the user interface	Requirements relating to the design of the SLA, as well as information that must be identifiable through the SLA documentation	Requirements relating to the use, availability, and exchange of data, as well as integrations	Requirements relating to technical documentation of the solution, as well as user documentation	Requirements relating to the use and availability of AI functionality in systems and solutions
Special note			Please specify where the relevant information for the requirement is located in the relevant SLA documentation.			

Requrements structure	Req. Ref.	Category	Classification		Supplier's compliance (drop down menu)		Supplier's response
Description	The requirements' reference number	The non-functional requirement category	Shall / A Minimum requirement, must be compliant in order to deliver solution.	Should / B Evaluation requirement, shall have a response and Avinor will evaluate the response on a score from 1-10 (1 lowest, 10 highest)	Choose correct compliance-status in the drop-down menu in the cell.	Compliant Fully compliant with the requirement. Elaborate in the reponse cell. Partly compliant Partly compliant with the requirement. Elaborate in the reponse cell. Not compliant Not compliant with the requirement. Will require explicit elaboration.	Describe how the supplier/solution fulfills the requirement based on the requirement description.

Responses for A-req	Responses for B-req
Compliant	Compliant
Not compliant	Partly compliant
	Not compliant

TEC CIS General						
Req. Ref.	**Quality Dimension (ISO25000)**	**Category (ISO25000)**	**Requirement**	**Type of requirement**	**Supplier's compliance**	**Supplier's response**
TEC-CIS-01	Product Quality (ISO/IEC 25010)	Security	All data in transit between client, service and integrated components shall be protected with TLS version 1.2 or higher. The supplier shall confirm that this requirement is met.	A		
TEC-CIS-02	Product Quality (ISO/IEC 25010)	Security	Deprecated or insecure cryptographic protocols and algorithms (e.g. SSL, TLS 1.0/1.1, MD5, SHA-1) shall not be used anywhere in the service. The supplier shall confirm that this requirement is met.	A		
TEC-CIS-03	Product Quality (ISO/IEC 25010)	Security	The supplier is requested to describe how the encryption architecture of the offered service protects Avinor information. The description should cover how data is encrypted in transit and at rest, how keys are managed throughout their lifecycle, how access to cryptographic material is controlled, and whether and how customer-specific keys are separated from shared platform components where relevant. The description will form part of Avinor's evaluation of the service security architecture.	B		
TEC-CIS-04	Product Quality (ISO/IEC 25010)	Compatibility	If the service uses a domain name under "avinor.no", TLS certificates for that domain shall be issued with Avinor as certificate holder. The supplier shall confirm that this requirement is met.	A		
TEC-CIS-05	Product Quality (ISO/IEC 25010)	Compatibility	The supplier shall maintain a documented certificate lifecycle process for certificates used in the service. To demonstrate compliance, the supplier shall provide documentation that as a minimum covers issuance, renewal, revocation, key protection, monitoring of expiry, emergency replacement, and allocation of responsibilities. The supplier shall describe how this requirement is met.	A		
TEC-CIS-06	Product Quality (ISO/IEC 25010)	Security	All externally exposed APIs shall enforce server-side authorization, ensuring callers only access resources they are permitted to. The supplier shall confirm that this requirement is met.	A		
TEC-CIS-07	Product Quality (ISO/IEC 25010)	Security	The supplier shall implement controls against API abuse for services that expose APIs. To demonstrate compliance, the supplier shall document the API security architecture and how authentication, authorization, rate limiting, input validation, secret handling, and security testing are implemented. The documentation shall describe how these controls are applied consistently across externally exposed and internal APIs.	A		
TEC-CIS-08	Product Quality (ISO/IEC 25010)	Compatibility	If the solution sends emails on behalf of Avinor, SPF and DKIM shall be configured in collaboration with Avinor. The supplier shall confirm that this requirement is met.	A		
TEC-CIS-09	Product Quality (ISO/IEC 25010)	Security	The supplier shall, for personnel who will have privileged access, administrative access, physical access to equipment included in the service delivery, or access to Avinor information beyond ordinary end-user access, maintain a documented and role-based background screening process before such access is granted, in accordance with applicable law. The process shall at a minimum include verification of identity, relevant references and qualifications where relevant to the role, and be documentable upon request. The supplier shall describe how this requirement is met.	A		

TEC-CIS-10	Product Quality (ISO/IEC 25010)	Security	The service shall implement an access control architecture based on continuous verification, least privilege, segmentation, and conditional access for privileged or high-risk actions. To demonstrate compliance, the supplier shall document how identities, trust boundaries, administrative access, and access decisions are governed across relevant environments, and the principle of least privilege shall be enforced for all access to Avinor resources.	A		
TEC-CIS-11	Product Quality (ISO/IEC 25010)	Security	The service shall implement a consistent access control mechanism (RBAC, ABAC or equivalent) with deny-by-default and server-side enforcement across user interfaces, APIs and backend services. Authorization shall be verified at object level and function level so that users can access only resources and actions they are explicitly authorised for. The supplier shall describe how this requirement is met.	A		
TEC-CIS-12	Product Quality (ISO/IEC 25010)	Security	The supplier shall maintain a documented lifecycle process for all supplier-related accounts (administrators, operators, support, service accounts, etc.) used in the service across all environments (application, cloud infrastructure, and CI/CD pipelines), including which technologies are used for identity and access management and how exceptions are handled. The supplier shall describe how this requirement is met.	A		
TEC-CIS-13	Product Quality (ISO/IEC 25010)	Security	Privileged accounts used to operate or administer the service and its infrastructure shall follow the principle of least privilege, be separated from regular user accounts, and be governed by documented policies. Elevation of privileged access shall be time-limited, require explicit approval, be protected by multi-factor authentication, and use technical mechanisms such as Privileged Identity Management (PIM) or equivalent. Activities performed with privileged accounts shall be logged, monitored, periodically reviewed, and subject to audit. This requirement also applies to privileged accounts used by supplier personnel, and controls for such accounts shall be at least as strict as for regular user accounts. The supplier shall describe how this requirement is met.	A		
TEC-CIS-14	Product Quality (ISO/IEC 25010)	Security	If the service provides emergency access or break-glass accounts, these shall be disabled by default, time-limited when activated, require explicit approval, be protected by multi-factor authentication, be fully logged, and be subject to post-use review. The supplier shall describe how this requirement is met.	A		
TEC-CIS-15	Product Quality (ISO/IEC 25010)	Security	Multi-factor authentication (MFA) shall be used for all logins to the service, including for privileged and administrative accounts. MFA shall also be required for security zone changes, crossing of trust boundaries, or elevation of privileges in the service. The supplier shall use robust MFA methods (e.g. app-based authentication, hardware tokens, or FIDO2) and shall maintain a documented policy for handling exceptions and fallback solutions. The supplier shall describe how this requirement is met.	A		
TEC-CIS-16	Product Quality (ISO/IEC 25010)	Compatibility	The service shall be able to make selected audit and security logs available to Avinor or an Avinor-designated external monitoring or review solution in a structured format, subject to agreed interfaces and lawful restrictions. The supplier shall document any technical, legal, or retention-related limitations.	A		
TEC-CIS-17	Product Quality (ISO/IEC 25010)	Security	The service shall be monitored, and activities and events affecting security shall be logged. Logs shall be protected against unauthorised modification and deletion, encrypted at rest, and subject to strict access control. The supplier shall maintain a documented process for monitoring and logging that at a minimum describes which monitoring and logging tools are used, how events are correlated and alerted, which administrative activities are logged, how logs are reviewed, and what retention periods apply. The supplier shall describe how this requirement is met.	A		

TEC-CIS-18	Data Quality (ISO/IEC 25012)	Data Centric IT Requirements	When the service involves processing personal data, the supplier shall comply with applicable data protection legislation and maintain documented processes for privacy by design, handling of data subject rights, and assessing the need for a data protection impact assessment before processing that may involve high risk is put into operation. The supplier shall describe how this requirement is met, and is requested to describe which personal data are processed in the solution.	A		
TEC-CIS-19	Data Quality (ISO/IEC 25012)	Data Centric IT Requirements	Processing of Avinor personal data and business-høy information shall as a general rule take place within the EU/EEA. Processing outside the EU/EEA, including remote access from third countries, requires Avinor's prior written approval. For any processing outside the EU/EEA, the supplier shall document: the countries used, the transfer mechanism applied (adequacy decision, SCC, BCR, or other valid basis), the sub-suppliers involved, the data categories processed, and a Transfer Impact Assessment identifying relevant risks arising from the third country's legal regime (cf. Schrems II) and the supplementary technical, organisational, and contractual measures put in place to ensure an equivalent level of protection. The supplier shall notify Avinor of any changes to processing location or transfer mechanism. The supplier shall describe how this requirement is met.	A		
TEC-CIS-20	Product Quality (ISO/IEC 25010)	Maintainability	The supplier shall maintain a documented process for identifying, prioritising, testing and implementing security updates and maintenance changes for components included in the service. The process shall include continuous monitoring of relevant security updates, dedicated handling of høy updates, rollback capability in case of failure, and clear allocation of responsibilities. The supplier shall describe how this requirement is met.	A		
TEC-CIS-21	Product Quality (ISO/IEC 25010)	Security	When the service is delivered in supplier-managed cloud infrastructure, the supplier shall have a documented cloud security posture management process covering scope, baselines, detection of misconfigurations, prioritisation, exception handling, remediation, and follow-up. The supplier shall describe how this requirement is met.	A		
TEC-CIS-22	Product Quality (ISO/IEC 25010)	Reliability	Security incidents affecting Avinor shall be reported within 24 hours of detection to csirt@avinor.no. The supplier shall confirm that this requirement is met.	A		
TEC-CIS-23	Product Quality (ISO/IEC 25010)	Reliability	The supplier shall maintain a documented process for detecting, recording, triaging, escalating, handling and closing security incidents that affect the service or Avinor's information. The process shall include defined contact points towards Avinor and criteria for when Avinor must be notified. The supplier shall describe how this requirement is met.	A		
TEC-CIS-24	Product Quality (ISO/IEC 25010)	Maintainability	For services that are developed, configured or updated by the supplier, the supplier shall maintain a documented secure development and delivery chain process that at a minimum includes secure coding practices, code review, security hardening, risk assessment for material changes, security testing, and management of dependencies and the build and deployment chain. The supplier shall describe how this requirement is met.	A		

TEC-CIS-25	Data Quality (ISO/IEC 25012)	Data Centric IT Requirements	Information that Avinor generates or processes in the service shall be owned by Avinor. Avinor shall have free-of-charge access to its own data. The information shall not be shared with other parties without Avinor's approval, and shall not be copied or used outside the scope of the service delivery as set out in the contract. The supplier shall describe how this requirement is met.	A		
TEC-CIS-26	Data Quality (ISO/IEC 25012)	Data Centric IT Requirements	The supplier should classify data processed by the service and implement masking/tokenization of sensitive fields in logs, APIs, and UIs etc. Guidance: Provide classification scheme and masking/tokenization approach. The supplier shall describe how this requirement is met.	B		
TEC-CIS-28	Product Quality (ISO/IEC 25010)	Security	Only personnel necessary for fulfilling the agreement shall be granted access according to need-to-know and least privilege. The supplier shall confirm that this requirement is met.	A		
TEC-CIS-29	Product Quality (ISO/IEC 25010)	Security	The supplier shall have control over all communication to and from the service. The supplier shall describe how this requirement is met.	A		
TEC-CIS-30	Product Quality (ISO/IEC 25010)	Security	The supplier shall perform risk-based security testing of the service at least every 12 months and after significant changes to the service. Where relevant, the testing shall include penetration testing. The supplier shall maintain a documented security testing process that describes test frequency, scope, roles, and how findings are recorded, prioritised, and closed within defined remediation times, and shall be able to provide documentation (e.g. test plan, anonymised security test report, and follow-up of findings) demonstrating that the process is applied in practice. The supplier is requested to confirm whether this requirement is met. The supplier shall describe how this requirement is met.	A		
TEC-CIS-31	Product Quality (ISO/IEC 25010)	Maintainability	The supplier shall maintain a documented vulnerability management process providing continuous visibility into vulnerabilities in all components used in the service (infrastructure, containers, code, and dependencies), including how components are scanned and findings prioritised. The supplier shall define maximum remediation times by severity (at minimum høy, high, medium, and low). Deviations shall be handled with documented compensating controls. The supplier shall describe how this requirement is met.	A		
TEC-CIS-33	Product Quality (ISO/IEC 25010)	Security	The supplier shall have an established and documented process for supply-chain management, including identification, security assessment, requirement-setting, and follow-up of sub-suppliers and other third parties that store, process, transmit, or have administrative access to Avinor information, or that deliver høy components of the service. The supplier is requested to describe the relevant data flows and dependencies, including the data involved, the actors involved, and the storage/processing location where relevant. Upon request, the supplier shall be able to provide an up-to-date overview of relevant sub-suppliers/third parties and documentation of completed security assessments and follow-up. The supplier shall describe how this requirement is met.	A		
TEC-CIS-34	Product Quality (ISO/IEC 25010)	Maintainability	The supplier shall be able to produce an up-to-date software bill of materials (SBOM) for software included in the delivery, perform continuous scanning of dependencies and components, and verify the origin and integrity of third-party components and build artefacts before they are put into use. The supplier is requested to attach an up-to-date SBOM. The supplier shall describe how this requirement is met.	A		

TEC-CIS-35	Product Quality (ISO/IEC 25010)	Security	The supplier shall contractually flow down relevant security requirements from this requirement set, as a minimum, all mandatory (A) requirements and the obligations under the data processing agreement, to all sub-suppliers and sub-processors that store, process, transmit, or have administrative access to Avinor information, or that deliver høy components of the service. The supplier shall confirm that this requirement is met.	A		
TEC-CIS-36	Product Quality (ISO/IEC 25010)	Security	The supplier shall notify Avinor in writing and with reasonable advance notice before replacing or adding sub-suppliers that process Avinor data or deliver høy functions in the service, so that Avinor has the opportunity to assess and, where appropriate, object to the change before it takes effect. The supplier shall confirm that this requirement is met.	A		
TEC-CIS-37	Product Quality (ISO/IEC 25010)	Security	The supplier is requested to describe their Information Security Management System (ISMS), including the risk management process for the service/system, and how compliance status and service-specific risk assessments can be reported to Avinor at least annually. The supplier is also requested to specify which standards they comply with, and/or which certifications they have obtained for the ISMS (Information Security Management System). A customised version of the risk assessment results is acceptable. Guidance: - Describe the ISMS and the risk management process. - Describe how service-specific risk assessments are performed and shared with Avinor. - List standards and certifications. - Provide policy and reporting process.	B		
TEC-CIS-38	Product Quality (ISO/IEC 25010)	Security	The supplier shall maintain a documented and systematic risk management process for the service or system. The process shall include identification, assessment, treatment and follow-up of risk, be updated at least annually and upon material changes, and the results shall be shareable with Avinor in an adapted form. The supplier shall describe how this requirement is met.	A		
TEC-CIS-41	Product Quality (ISO/IEC 25010)	Security	If the service uses passwords as an authentication factor, the solution shall allow passwords and passphrases of at least 14 characters, block known compromised passwords, not require generic composition rules or periodic password changes without specific reason, and protect sign-in with rate limiting or equivalent controls against brute-force attacks. The supplier shall describe how this requirement is met.	A		
TEC-CIS-42	Product Quality (ISO/IEC 25010)	Security	The service shall store and manage secrets in a dedicated secrets management solution or equivalent controlled mechanism, not in source code or static configuration files. Access to secrets shall be role-based and logged, secrets shall be rotatable upon compromise and at defined intervals, and the supplier shall use automated scanning to detect exposed secrets in code and build environments. The supplier shall confirm that this requirement is met.	A		
TEC-CIS-43	Product Quality (ISO/IEC 25010)	Reliability	The supplier shall maintain a documented business continuity plan and disaster recovery plan for the service. The plans shall cover høy components, define recovery objectives for time and data, be tested at least annually and upon material changes, and the supplier shall be able to provide a summary of the latest test and identified improvement actions. The supplier shall confirm that this requirement is met.	A		
TEC-CIS-44	Product Quality (ISO/IEC 25010)	Reliability	If the service relies on backups for recovery of Avinor information or service functionality, the supplier shall document the use of immutable or logically isolated backups, retention periods, separation from production environments, and how recovery testing is planned and performed. The supplier shall be able to present an anonymised summary of the latest recovery test. The supplier shall confirm that this requirement is met.	A		

TEC AI Requirements						
Req. Ref.	**Quality Dimension (ISO25000)**	**Category (ISO25000)**	**Requirement**	**Type of requirement**	**Supplier's compliance**	**Supplier's response**
TEC-AI-1	Product Quality (ISO/IEC 25010) Quality model for AI systems (ISO/IEC 25059:2023)	Functional Suitability	The supplier shall confirm whether the solution uses artificial intelligence as an integrated part of its functionality and specify whether AI is core functionality or additional functionality in the solution.	A		
TEC-AI-2	Data Quality (ISO/IEC 25012)	Usability (Transparency)	The supplier is requested to describe how artificial intelligence is used in the solution, including: - which AI modules and components are included, and their purpose - the main data flows and the purpose of processing, transformation and analysis - how the role of the modules and their data processing can be reviewed and understood by Avinor.	B		
TEC-AI-3	Data Quality (ISO/IEC 25012)	Freedom from Risk	The supplier shall ensure that bias is identified, measured, and mitigated in the AI solution, including how relevant data quality issues are taken into account to support fair and non-discriminatory outcomes. The supplier shall describe how this requirement is met.	A		
TEC-AI-4	Product Quality (ISO/IEC 25010) Data Quality (ISO/IEC 25012)	Safety	The supplier shall establish and maintain the necessary controls to ensure that the AI solution is robust, secure, and resistant to manipulation, misuse, and unintended behaviour. The supplier shall document its processes and controls for safe use, adversarial testing, AI red-teaming, detection of model poisoning, data drift and anomalous behaviour, as well as measures against AI-related resource abuse. The supplier shall describe how this requirement is met.	A		
TEC-AI-5	Data Quality (ISO/IEC 25012)	Functional Suitability	The supplier shall ensure that the solution supports transparency of AI-generated results, including: - source attribution and grounding, and how the level of precision in source references can be configured and controlled - explanations tailored to the user's context, ranging from simple confidence indicators to more detailed explanatory information where relevant. The supplier shall describe how this requirement is met.	A		
TEC-AI-6	Product Quality (ISO/IEC 25010)	Data Centric IT Requirements	The supplier shall provide mechanisms that ensure Avinor's data, including prompts, outputs, usage patterns, and content, is not used to train or improve general AI models without Avinor's explicit and documented consent. The supplier shall describe how this requirement is met.	A		

TEC-AI-7	Quality model for AI systems (ISO/IEC 25059:2023)	Usability (User Controllability)	The supplier shall ensure that AI-generated results can always be quality assured by a human before use and that the solution does not make decisions affecting rights or obligations without necessary human assessment and control. The supplier shall describe how this requirement is met.	A		
TEC-AI-8	Data Quality (ISO/IEC 25012)	Usability (Transparency)	The supplier is requested to explain how AI-generated content can be clearly labelled when shared internally or externally and how it can be shown whether such content has been reviewed or quality assured by a human. The supplier shall describe how this requirement is met.	B		
TEC-AI-9	Quality in Use (ISO/IEC 25010)	Freedom from Risk	The supplier shall have performed an AI risk assessment and classify the solution in accordance with the EU AI Act risk categories. The classification method, assumptions, justification, and resulting control implications shall be documented and made available to Avinor. The supplier shall describe how this requirement is met.	A		
TEC-AI-10	Product Quality (ISO/IEC 25010)	Reliability	The supplier is requested to describe its management plan for the AI solution covering the entire lifecycle. The plan should include: - operations, maintenance and continued development, including roles, responsibilities, decision authority, change management, updates and handling of new or changed requirements - monitoring and evaluation over time, including how performance, quality, security, data drift, model behaviour, error rates and compliance are measured, followed up and documented - criteria for reassessment, corrective actions and escalation, including thresholds, events or changes that trigger revalidation, risk assessment, security assessment, model update or other follow-up - decommissioning or orderly phase-out, including plans for migration, deletion or archiving of data, termination of integrations, access management, documentation and handling of dependencies - how measures are carried out in practice, who is responsible, and how execution, deviations and decisions are documented and reported to the customer.	B		
TEC-AI-11	Product Quality (ISO/IEC 25010) Quality model for AI systems (ISO/IEC 25059:2023)	Usability / Interaction Capability	The supplier is requested to describe how safe, effective, and controlled introduction and use of the AI solution is supported, including: - training and support for Avinor's users and stakeholders, and how this contributes to competence development - user involvement and change management when introducing the solution, so that it can be adopted in a controlled and effective manner.	B		
TEC-AI-12	Quality model for AI systems (ISO/IEC 25059:2023)	Usability (Transparency)	The supplier shall document the AI solution's functionality, relevant data basis, and decision-related processes so that Avinor can review how the solution works, what information it relies on, and how key outcomes can be traced and assessed. The supplier is requested to confirm that this is met.	A		

TEC-AI-13	Product Quality (ISO/IEC 25010)	Freedom from Risk	The supplier shall ensure technical controls that protect the AI solution against prompt injection, indirect prompt manipulation, tool poisoning, exposure of system prompts, and unsafe execution of AI-generated output. The supplier shall describe how this requirement is met.	A		
TEC-AI-14	Product Quality (ISO/IEC 25010)	Security	The supplier shall ensure that AI agents and AI-enabled actions are constrained through least privilege, per-call authentication and authorization, explicit human approval for consequential actions, and technical isolation of agent runtime environments and available tools. The supplier shall describe how this requirement is met.	A		
TEC-AI-15	Product Quality (ISO/IEC 25010)	Security	The supplier shall document provenance, versioning, integrity verification, and software bill of materials or equivalent artefacts for AI models, frameworks, plugins, skills, data sources, and other third-party components used in the solution. The supplier shall describe how this is met, and attach an up-to-date SBOM or equivalent artefact.	A		
TEC-AI-16	Product Quality (ISO/IEC 25010)	Data Centric IT Requirements	The supplier shall ensure technical controls that prevent confidential, internal, or personal information from leaking through model responses, logs, embeddings, metadata, vector databases, or retrieval mechanisms. The supplier shall describe how this requirement is met.	A		
TEC-AI-17	Product Quality (ISO/IEC 25010)	Security	The supplier shall ensure AI-specific security logging, monitoring, incident management, and relevant security integrations, including how AI traffic can be governed, how security events are detected and escalated, and how Avinor can investigate misuse, anomalous behaviour, or unmanaged AI usage. The supplier shall describe how this requirement is met.	A		

TEC General & UX Requirements

Req. Ref.	Quality Dimension ISO25000)	Category (ISO25000)	Requirement	Classification	Supplier's compliance (drop down menu)	Supplier's response
TEC-GEN-1	**Product Quality (ISO/IEC 25010)**	**Compatibility**	The offered solution should be based on an open architecture, i.e., using standardized protocols and APIs, with clearly defined interfaces. The Supplier should clarify how the solution architecture complies with these recommendations.	**B**	Partly compliant	
TEC-GEN-2	**Product Quality (ISO/IEC 25010)**	**Compatibility**	The Supplier must describe whether the proposed solution requires third-party components or plugins to be installed in the browser, on PCs, or in server environments. Does the proposed solution rely on third-party solutions or products? If so, the Supplier is requested to specify which third-party solutions or products are utilized, the runtime environments they require (browsers, PCs, servers), and which versions of these are supported. Preferred solution for Avinor is to avoid third-party solutions as party of the delivery, so this would result in a lower score.	**B**		
TEC-UX-1	**Product Quality (ISO/IEC 25010)**	**Compatibility**	The user interface of the proposed solution must be available as a web-based solution. The solution must as a minimum be compatible with Microsoft Edge.	**A**		
TEC-UX-2	**Product Quality (ISO/IEC 25010)**	**Usability / Interaction Capability**	The supplier is requested to provide a detailed explanation of which browsers are supported, as well as describe any necessary customizations or requirements to ensure optimal functionality.	**B**		
TEC-UX-3	**Product Quality (ISO/IEC 25010)**	**Usability / Interaction Capability**	The user interface of the proposed solution should be available as a solution for mobile devices. The supplier is requested to provide a detailed explanation of which mobile platforms are supported, as well as describe any necessary customizations or requirements to ensure optimal functionality.	**B**		

Req. Ref.	Quality Dimension ISO25000)	Category (ISO25000)	Requirement	Classification	Supplier's compliance (drop down menu)	Supplier's response
TEC-UX-4	**Product Quality (ISO/IEC 25010)**	**Usability / Interaction Capability**	The proposed solution should support Norwegian characters and formats in accordance with current best practices and relevant standards, such as ISO/IEC 10646 for character sets and Unicode for text processing. This includes support for: - Information and content - User interface - Search functionality - API- and message-based interfaces Furthermore, the solution should support Norwegian date formats, currency formats, and other localization-specific requirements in compliance with standards such as ISO 8601 (date and time) and relevant specifications for currency formats. The Supplier is requested to explain how the solution meets these requirements. What technical measures or implementations ensure support for Norwegian characters and formats across all relevant parts of the solution, and how are standards such as ISO/IEC 10646, Unicode, and ISO 8601 adhered to?	**B**		

TEC General SLA Requirements

Req. Ref.	Quality Dimension ISO25000)	Category (ISO25000)	Requirement	Classification	Supplier's compliance (drop down menu)	Supplier's response
TEC-SLA-1	**Product Quality (ISO/IEC 25010)**	**Reliability**	The offered solution must perform reliably, automatically recover from failures, scale workloads, and manage automated changes effectively. How does the offered solution ensure reliability and handle failure scenarios?	**B**		
TEC-SLA-2	**Product Quality (ISO/IEC 25010)**	**Reliability**	The system must provide high availability, ensure quick recovery after failures, and set thresholds for acceptable data loss. How does the offered solution ensure high availability and define thresholds for recovery?	**B**		
TEC-SLA-3	**Product Quality (ISO/IEC 25010)**	**Reliability**	The system must monitor data exchange services for availability and quality and promptly inform stakeholders of detected issues. How does the offered solution monitor data exchange and handle stakeholder communication during service interruptions?	**B**		

TEC-SLA-4	**Product Quality (ISO/IEC 25010)**	**Reliability**	The Supplier must provide evidence of system uptime for both the Customer and end users, along with defined deadlines for correcting errors categorized by criticality. How does the Supplier ensure transparency and timely resolution of critical errors?	**B**		
TEC-SLA-5	**Product Quality (ISO/IEC 25010)**	**Reliability**	The system must be resilient to failures and capable of recovering gracefully to ensure continuous service delivery. The Supplier must describe resilience capabilities. How does the offered solution handle failures and ensure service continuity across environments?	**B**		
TEC-SLA-6	**Product Quality (ISO/IEC 25010)**	**Reliability**	Services must be self-contained with a single responsibility, enabling multiple instances to run in parallel in geo-redundant data centers. How does the offered solution support service redundancy and geo-redundancy?	**B**		

TEC Data Exchange

Nr.	Quality Dimension ISO25000)	Category (ISO25000)	Requirement	Classification	Extended Description	Supplier's compliance (drop down menu)	Supplier's response
TEC-DATA-1	**Data Quality (ISO/IEC 25012)**	**Data Centric IT Requirements**	The solution shall support data exchange, including both data collection and sharing. The Supplier shall ensure that the Customer can easily export and import their data in a standardized format. The solution shall support secure and automated access of data to the Customer's cloud platforms without impact on the performance of solutions in production.	**A**	The offered solution must provide functionality to import and export relevant data to the systems functionality and technical setup in an easy and secure manner. This so that it is possible to import and export data through secure and standardised formats.		
TEC-DATA-2	**Data Quality (ISO/IEC 25012)**	**Data Centric IT Requirements**	The Supplier is requested to describe the support for various methods for dataand metadata export: - Messaging: Transfer of data using asynchronous event-based protocols (publish-subscribe), such as Java Message Service, Apache Kafka, WebHooks or event streams. Central to the description are considerations on latency/real-time. - Remote Procedure Invocation: Transfer of data using synchronous queries (request-reply) to, for example, a REST API or methodologies such as ETL (Extract Transform Load) and ELT (Extract Load Transform). - File Transfer: Transfer of data using file transfer methods (e.g. JSON, XML, CSV, XLSX or column-based formats such as Parquet. etc.). Column-based formats are preferred for larger amounts of data. - Delta Share: For secure sharing of large data sets in real time.	**B**	The offered solution must provide standard-compliant APIs (e.g., REST, GraphQL) to enable interoperability with the Customer’s existing systems. How does the offered solution ensure seamless data exchange and compatibility with third-party platforms? See examples of integration methods (Enterprise Integration Patterns) at https://www.enterpriseintegrationpatterns.com/. Note that in Avinor, publish-subscribe and request-reply are the preferred patterns.		
TEC-DATA-3	**Data Quality (ISO/IEC 25012)**	**Data Centric IT Requirements**	The supplier is requested to describe which additional relevant data can be made available/exported from the solution, and in which format.	**B**			
TEC-DATA-4	**Data Quality (ISO/IEC 25012)**	**Data Centric IT Requirements**	The solution must support integration with external systems using HTTP-based protocols, such as REST, gRPC and SOAP, with a preference for REST. If the solution currently lacks the capability to integrate via HTTP-based protocols, would the supplier be willing to develop this functionality for the Customer? The supplier is requested to describe how the delivery of this functionality will be achieved.	**A**			
TEC-DATA-5	**Data Quality (ISO/IEC 25012)**	**Data Centric IT Requirements**	The solution must ensure reliable and secure data exchange with the Customer’s systems. This can be, but not limited to CRM, ERP or IoT systems. What mechanisms does the Supplier provide to ensure data integrity and confidentiality during cross-system communication?	**B**			

Nr.	Quality Dimension ISO25000)	Category (ISO25000)	Requirement	Classification	Extended Description	Supplier's compliance (drop down menu)	Supplier's response
TEC-DATA-6	**Data Quality (ISO/IEC 25012)**	**Data Centric IT Requirements**	The supplier shall document factors influencing API scalability and performance to ensure that the proposed solution is capable of handling the required data exchange volumes. The supplier shall document how the solution supports flexible and efficient data extraction, including how the Customer can configure the time, frequency and content, as well as the interfaces and mechanisms used for extraction of large amounts of data for analysis and reporting purposes. Any limitations, such as paging, rate limiting, throttling and volume limitations, and how these affect data extraction and analysis, shall be described. The Provider shall also describe how the solution supports incremental data extraction based on changes after a given point in time, including handling and identifying updated and deleted data in the event of large amounts of data or high frequency of change, without the need for complete data extraction.	**A**			
TEC-DATA-7	**Data Quality (ISO/IEC 25012)**	**Data Centric IT Requirements**	How does the Supplier ensure API performance and scalability? The supplier is requested to describe how the delivery of this functionality will be achieved.	**B**			
TEC-DATA-8	**Data Quality (ISO/IEC 25012)**	**Data Centric IT Requirements**	The supplier is asked to describe how the data that the solution will process can be documented as a product, meaning the datasets included in the system, the metadata that is part of the datasets, and how these are available to Avinor. The documentation shall cover all information elements, including unique and stable identifiers, business keys, relationships, cardinality, and unambiguous and sufficiently descriptive data definitions, including the meaning of values, status codes, and classifications. The data model and documentation shall be kept up to date as changes are made, and changes from previous versions shall be clearly documented.	**B**			
TEC-DATA-9	**Data Quality (ISO/IEC 25012)**	**Data Centric IT Requirements**	The supplier is asked to describe how the solution supports the handling of master data, if applicable.	**B**			
TEC-DATA-10	**Data Quality (ISO/IEC 25012)**	**Data Centric IT Requirements**	The supplier is asked to describe how the solution supports various needs for timeliness of integrations (e.g., periodic batch jobs or near real-time).	**B**			
TEC-DATA-11	**Data Quality (ISO/IEC 25012)**	**Data Centric IT Requirements**	The supplier is asked to describe how the solution supports data governance. This, by presenting different roles and responsibilities (e.g., CRUD) for managing data in the solution and ensuring data quality (for example managing duplicate or missing data, etc.)	**B**			
TEC-DATA-12	**Data Quality (ISO/IEC 25012)**	**Data Centric IT Requirements - Sesar SWIM**	The proposed solution must support integration with Sesar SWIM (System Wide Information Management), enabling the exchange of aeronautical, meteorological, and flight-related data in compliance with Sesar SWIM standards. This includes compatibility with SWIM Yellow Profile and support for SWIM-enabled services used at airports. How does the proposed solution ensure compliance with Sesar SWIM standards and facilitate seamless data exchange with relevant stakeholders, such as air navigation service providers and airlines?	**A**			

Nr.	Quality Dimension ISO25000)	Category (ISO25000)	Requirement	Classification	Extended Description	Supplier's compliance (drop down menu)	Supplier's response
TEC-DATA-13	**Data Quality (ISO/IEC 25012)**	**Data Centric IT Requirements - LUFTHAVN**	The supplier is requested to describe the capabilities of the proposed solution for streaming data in real-time to another system or data platform. Preferred protocols are MQTT and AMQP. If the solution does not have the capability to stream data in real time, the supplier shall develop this functionality for the Customer	**B**			
TEC-DATA-14	**Data Quality (ISO/IEC 25012)**	**Data Centric IT Requirements - LUFTHAVN**	The proposed solution should be able to integrate with Avinor's Geographic Information Systems (GIS) to ensure effective management and visualization of geographical data. The supplier should describe how the solution architecture meets this requirement.	**B**	Avinor's Geographic Information System (GIS) is built on ESRI's ArcGIS software (www.esri.com). The central component of Avinor's GIS is ArcGIS Enterprise. Together with geographic data stored in centralized geodatabases, this platform enables the creation and distribution of map-based web services, web applications, field apps, and desktop solutions throughout Avinor. Additionally, Avinor extensively utilizes FME from Safe Software (www.safe.com) for ETL processes, data transfer, and quality control involving geographic data. ArcGIS offers a comprehensive set of APIs, including JavaScript, .NET, and Python. The supplier is requested to describe how the solution can integrate maps from external map services. Furthermore, the supplier is asked to specify which map formats the solution supports, as well as how map data is updated and maintained.		

TEC Documentation Requirements

Req. Ref.	Quality Dimension ISO25000)	Category (ISO25000)	Requirement (EN)	Classification	Supplier's compliance (drop down menu)	Supplier's response
TEC-DOC-1	Product Quality (ISO/IEC 25010)		The Supplier shall deliver a document plan, outlining all documents expected to be delivered to the Customer throughout the project, updated with scheduled delivery dates for each piece of documentation. The customer should have the ability to make changes to the document plan. The final approval of the document plan should be made by the customer.	A		
TEC-DOC-2	Product Quality (ISO/IEC 25010)	Compatibility	The Supplier shall provide complete system documentation, including a detailed architecture overview of the solution.	A		
TEC-DOC-3	Product Quality (ISO/IEC 25010)	Compatibility	The Supplier shall document all interfaces and APIs, clearly identifying any proprietary technologies.	A		
TEC-DOC-4	Product Quality (ISO/IEC 25010)	Compatibility	Documentation of all integrations implemented shall be submitted before commissioning of the system.	A		
TEC-DOC-5	Product Quality (ISO/IEC 25010)	Usability / Interaction Capability	A user manual in Norwegian and/or English should be provided for super users and end users, according to the configurated solution delivered to Avinor.	B		
TEC-DOC-6	Product Quality (ISO/IEC 25010)	Reliability	The Supplier shall be responsible for maintaining and consistently updating all documentation to align with system upgrades for the duration of the system's lifecycle.	A		