DRAFT - ICT Project Guidance

Default System Quality Requirements

Version:

0.1

Author:

Sky Sigal, Solution Architect

## Description

This document lists target Quality Requirements expected of services procured for this organisation. The requirements are developed and categorised following ISO-25010’s defined terminology.

## Synopsis

Requirements are developed to meet ISO-25010 defined categories for Quality Requirements, organised in a tiered, pyramidal manner to diminish the effort of RFx respondents to determine project specifics versus default quality expectations.

## Contents

[Description 1](#_Toc156204920)

[Synopsis 1](#_Toc156204921)

[Contents 2](#_Toc156204922)

[Document Context 5](#_Toc156204923)

[Background 5](#_Toc156204924)

[Default Baseline IT System Qualities 6](#_Toc156204925)

[Functional Suitability 6](#_Toc156204926)

[Functional Completeness 6](#_Toc156204927)

[Functional Correctness 10](#_Toc156204928)

[Functional Appropriateness 11](#_Toc156204929)

[Performance Efficiency 11](#_Toc156204930)

[Time Behaviour 11](#_Toc156204931)

[Resource Utilisation 12](#_Toc156204932)

[Capacity 12](#_Toc156204933)

[Compatibility 18](#_Toc156204934)

[Co-Existence 18](#_Toc156204935)

[Interoperability 18](#_Toc156204936)

[Usability 21](#_Toc156204937)

[Appropriateness Recognisability 21](#_Toc156204938)

[Learnability 33](#_Toc156204939)

[Operability 33](#_Toc156204940)

[User Protection Error 37](#_Toc156204941)

[User Interface Aesthetics 38](#_Toc156204942)

[Accessibility 38](#_Toc156204943)

[Reliability 40](#_Toc156204944)

[Maturity 41](#_Toc156204945)

[Availability 42](#_Toc156204946)

[Fault Tolerance 45](#_Toc156204947)

[Recoverability 45](#_Toc156204948)

[Security 51](#_Toc156204949)

[General 51](#_Toc156204950)

[Confidentiality 53](#_Toc156204951)

[Integrity 57](#_Toc156204952)

[Non-Repudiation 66](#_Toc156204953)

[Accountability 68](#_Toc156204954)

[Authenticity 69](#_Toc156204955)

[Maintainability 71](#_Toc156204956)

[General 71](#_Toc156204957)

[Modularity 72](#_Toc156204958)

[Reusability 73](#_Toc156204959)

[Analysability 73](#_Toc156204960)

[Modifiability 76](#_Toc156204961)

[Testability 78](#_Toc156204962)

[Portability 92](#_Toc156204963)

[Adaptability 92](#_Toc156204964)

[Installability 93](#_Toc156204965)

[Replaceability 95](#_Toc156204966)

[Regulatory 97](#_Toc156204967)

[General 97](#_Toc156204968)

[Privacy 98](#_Toc156204969)

[Sovereignty 100](#_Toc156204970)

[Appendices 101](#_Toc156204971)

[Appendix A - Document Information 101](#_Toc156204972)

[Images 101](#_Toc156204973)

[Tables 101](#_Toc156204974)

[References 101](#_Toc156204975)

[Review Distribution 101](#_Toc156204976)

[Audience 101](#_Toc156204977)

[Structure 101](#_Toc156204978)

[Diagrams 101](#_Toc156204979)

[Terms 101](#_Toc156204980)

[Appendices B – ISO-25010 Qualities 102](#_Toc156204981)

[Delivery 102](#_Toc156204982)

[Security 102](#_Toc156204983)

[Confidentiality 103](#_Toc156204984)

[Integrity 103](#_Toc156204985)

[Non-Repudiation (of Action) and Accountability (by Whom) 103](#_Toc156204986)

[Authenticity 103](#_Toc156204987)

[Availability 103](#_Toc156204988)

[Privacy 103](#_Toc156204989)

[Functionality 103](#_Toc156204990)

[Functional Completeness 103](#_Toc156204991)

[Functional Correctness 103](#_Toc156204992)

[Functional Appropriateness 103](#_Toc156204993)

[Performance 103](#_Toc156204994)

[Time behaviour 104](#_Toc156204995)

[Resource Utilisation 104](#_Toc156204996)

[Capacity 104](#_Toc156204997)

[Compatibility 104](#_Toc156204998)

[Co-existence 104](#_Toc156204999)

[Interoperability 104](#_Toc156205000)

[Usability 104](#_Toc156205001)

[Appropriateness recognisability 104](#_Toc156205002)

[Learnability 104](#_Toc156205003)

[Operability 104](#_Toc156205004)

[User Error Protection 104](#_Toc156205005)

[User Interface Aesthetics 104](#_Toc156205006)

[Accessibility 104](#_Toc156205007)

[Reliability 104](#_Toc156205008)

[Maturity 105](#_Toc156205009)

[Availability 105](#_Toc156205010)

[Fault tolerance 105](#_Toc156205011)

[Recoverability 105](#_Toc156205012)

[Maintainability 105](#_Toc156205013)

[Modularity 106](#_Toc156205014)

[Reusability 106](#_Toc156205015)

[Analysability 106](#_Toc156205016)

[Modifiability 106](#_Toc156205017)

[Testability 106](#_Toc156205018)

[Portability 106](#_Toc156205019)

[Adaptability 106](#_Toc156205020)

[Installability 106](#_Toc156205021)

[Replaceability 106](#_Toc156205022)

## Document Context

The development and organisation of the requirements defined in this document follow the guidance provided within *ICT Project Guidance – System Quality based Non-Functional Requirements*.

This document is the base document of a series of shorter tiered requirement documents that extend or supersede requirements inherited from lower documents such as this one.

The requirements within this document are organised following ISO-25010 quality headers.

The structuring of the requirements themselves follow guidance provided within the above document.

## Background

# 

# Qualities Based Non Functional Requirements

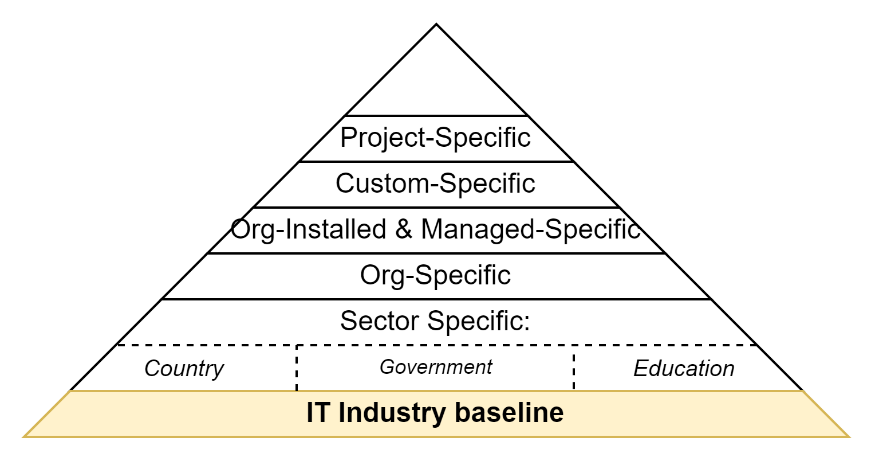


Figure : Default System Base Tier of Quality Requirements

Systems by default are expected to meet the following quality requirements.

This is the largest section of requirements, but it is expected that mature service providers meet these common requirements by default.

## Functional Suitability

*ISO-25010 Definition**: the degree to which a product or system provides functions that meet stated and implied needs when used under specified conditions. This characteristic is composed of the qualities listed below.*

Note:   
not to be confused with a solution’s Functional Requirements.

### Functional Completeness

IDO-25010 Definition: the degree to which the set of functions covers all the specified tasks and user objectives.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | | ID | Statement | Rationale | Fit Criteria | | Details | Response | Analysis |
|  | QR-DEF-FUN- COM-00 | Default/ Functionality/ Completeness | | Services MUST provide functionality to enable all the Capabilities listed in the Target Objectives:Capabilities. | A solution that does not cover all defined Capabilities is – by definition – Incapable of meeting defined objectives. | |  | Irrespective of the business capabilities on top of the following, mature systems will be capable of managing system specific information:  - Diagnostics - Errors Logging - Sessions - Session Operation Auditing - Users - User Grouping - [System] Roles  Less certain, but indicative of a capable design: - System Permissions - Group Roles - Group Role Allocation - Group Permissions to Group Role Allocation - Searching  - Uploaded Media management - Resource - Resource Metadata  etc. |  |  |
|  | QR-DEF-FUN- COM-00 |  | | Service analysis and functionality MUST address equally and regularly the needs of all key stakeholder groups, including the following stakeholder groups:  Business Owner,  Test Analyst,  Customer User  Business Specialist  Customer Support  Operations Specialist  Monitoring Specialist  Security Specialist  Maintenance Specialist Stakeholders  Infrastructure Specialist | Projects tend to fail more often when there is uneven emphasis on Business Owner expectations and/or Customer User SME expectations -- at the expense of other stakeholder requirements. | |  | Customer Support Stakeholders require documentation to provide simple, non-business specific tasks, as well as know whom to forward requests to for Business specific tasks,  Operations specialists require documentation on how to manage Users, Groups, Permissions, Workflows.  Maintenance Specialists require diagnostics tools  Security Specialists require auditing tools  C&A Specialists require secure development, deployment and operations practices in order to permit the solution to go and stay Live,  Infrastructure Specialists require configured automated compilation, packaging and deployment Pipelines, inclusive of Infrastructure as Code,  Test Analyst stakeholders require automation of their QA instructions. Business Owner Stakeholders require the development of reports on planning, progress, cost/benefits, risks, and service usage, issues and feedback. |  |  |
|  | QR-DEF- FUN- COM-00 | Default/ Functionality/ Information/ Non-Circumventing Security | | Services  MUST provide the functionality required by stakeholders to perform their responsibilities without breaching Security requirements. | A solution cannot implement best practice defence in depth if one or more stakeholder groups can have direct access to production data in a non-auditable manner.  Important:  It is illegal to provide access to data for purposes that are not disclosed in the system data use disclosure. | |  | Functionality is required by the following stakeholder groups: - Support specialists - Operations specialist - Maintenance specialists - Quality Assurance specialists - Developers  The functionality to perform their roles generally starts with providing authorised access to appropriate search functionality (filtering, ordering, paging) through - Diagnostic Logs &  Error Reports,  - Session &   Session Operations, - Groups, Resources,  Users, Roles &  Permissions |  |  |

### Functional Correctness

ISO-25010 Definition: the degree to which a product or system provides the correct results with the needed degree of precision.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  |  |  | Services’s systems MUST record date & time values to a minimum of the nearest UTC based millisecond or better. | Auditing records of changes to resources – even fast ones -- should be sequentially recorded. | Sighting: Available diagnostics and session audit records are recorded to the stated precision. | Use a trustable approach to round to the nearest acceptable value (*not* the lower or highest). |  |  |
|  |  |  | Services’s systems MUST record currencies to a minimum of the nearest hundredth of the used currency. | The system and organisation would lose users trust if operations that dealt with currencies did not eventuate in correct results. | Sighting: Available diagnostics and appropriate system records are recorded to the sUsztated precision. | Use a trustable approach to round to the nearest acceptable value (*not* the lower or highest). |  | Does the solution do any operation that involves currency?  Is there a chance that it might? |

Requirements: None

### Functional Appropriateness

ISO-25010 Definition: the degree to which the functions facilitate the accomplishment of specified tasks and objectives.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |

Requirements: None

## Performance Efficiency

*ISO-25010 Definition:* *the degree of performance relative to the amount of resources used under stated conditions. This characteristic is composed of the sub-qualities listed below.*

### Time Behaviour

ISO-25010 Definition: the degree to which the response and processing times and throughput rates of a solution, when performing its functions, meets requirements.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR-DEF-PRF-02 | Default/ Performance/ Time Behaviour | | Services MUST be capable of completing peak user requests within delays defined in the ’Target Objectives’. | Users become disconnected from systems that make them wait. |  |  |  |  |

### Resource Utilisation

*ISO-25010 Definition:* *the degree to which the amounts and types of resources used by a product or system, when performing its functions, meets requirements.*

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  |  |  | |  |  |  |  |  |  |

### Capacity

ISO-25010 Definition: the degree to which the maximum limits of the solution meet or exceed requirements.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR-DEF-PRF- 00 | Default/ Performance/ Capacity/ Time Behaviour/ Response Time | | Services’s APIs and User Interface MUST be capable of completing Peak surge requests and returning control to users within response times defined in the ’Target Objectives’. | Services must feel responsive to users, allowing them to be as efficient as they are capable. |  | Note:  completed User operations specifically means that the first operation has been actioned and completed on the server, and the next operation can be begun on the service client. All images, etc. in the response from the first operation should have completed loading by the time of beginning the actioning of the next operation. |  |  |
|  | QR-DEF-PRF- 00 | Default/ Performance/ Capacity/ Throughput | | Services MUST be capable of completing the requests of the peak user quantity defined in the ‘Target Objectives’ while meeting Responsivity targets. |  |  |  |  |  |
|  | QR-DEF-PRF- 00 | Default/ Performance/ Capacity/ Data Locking | | The application MUST NOT impede multiple (concurrent) users from using and maintaining the same data.  The system will be designed so that data locking does not exclusively lock data in such way that it prevents other business users from using the system in an efficient manner. | One user using data should not impede another user from using and maintaining that same data. Lock management will be designed to support concurrent access to data for read, update and delete operations. |  | Services does not open transactions at the beginning of requests and close them at the end. |  |  |
|  | QR-DEF-PRF- 00 | Default/ Performance/ Capacity/ Storage | | Services MUST be capable of persist the volume of information entrusted to it, for the full service lifespan of the system (see ‘Target Objectives’). | The information system should not physically delete information, instead keeping it for the lifespan of the system. |  | Services is expected to dynamically scale up and out as required to store the expected quantity of data required by the solution over its service lifespan. |  |  |
|  | QR-DEF-PRF- 00 | Default/ Performance/ Capacity/ Archiving | | Services MUST not physically remove archived data from the solution’s production data environment. | Archived data is production data at a specific point in time, and therefore has a relative value compared to production data. |  | Services archives records using logical state flag, as opposed to physical flags.  It is a logical error to misinterpret legislation to confuse removal from use, as meaning a physical removal. |  |  |
|  | QR-DEF-PRF- 00 | Default/ Performance/ Capacity/ Users & Resources | | Services MUST be able to manage the expected number of users and resources, described elsewhere. | Services SHOULD be capable of meeting expectations of users to access the system and manage information. |  | Services is capable of dynamically scaling up to manage the projected number of users and resource elements without change to the architectural design.  Please describe any concerns that the solution could not scale as required. |  |  |
|  | QR-DEF-PRF- 00 | Default/ Performance/ Capacity/ Throughput | | Services MUST be capable of handling – within max acceptable delays defined in the ‘Target Objectives’– the requests of the peak projected number of concurrent users. | Services SHOULD be capable of handling projected activity surges without frustration of end users, or becoming unavailable. |  | Services is capable of dynamically scaling horizontally to handle the requests of projected peak surge activity.  the solution ensures there are no bottle necks at various tiers (for example database accesses per second).  Note: completed User operations specifically means that the first operation has been actioned and completed on the server, and the next operation can be begun on the service client. All images, etc. in the response from the first operation should have completed loading by the time of beginning the actioning of the next operation. |  |  |
|  |  |  | |  |  |  |  |  |  |
|  | QR-DEF-PRF- 00 | Default/ Performance/ Resource Usage/ Background Operations | | Services’s capabilities, capacity and performance MUST NOT be negatively affected by background operations. | Users should not be affected by background batch, reporting or analysis operations. |  | Services is developed to ensure background operations do not negatively affect users, using a combination of one or more of the following:  command queues to handle tasks asynchronously,  using a limited number of background threads to process long running processes,  etc. |  |  |
|  | QR-DEF-PRF- 00 | Default/ Performance/ Resource Usage/ Background Operations/ Timing | | Services MUST process background operations when submitted (as opposed to running them outside of work hours). | Background operations should run when there are support and operations specialists to handle issues that might arise. |  | Parallel Multi-threading allows for faster completion that Serial operations, providing processing have plenty of opportunity to complete before the beginning of the next business day |  |  |
|  | QR-DEF-PRF- 00 | Default/ Performance/ Capacity/ Background/ Multi-threaded | | Services MUST process background operations across a configurable amount of threads to not impact end users | Parallel Multi-threading allows for faster completion that Serial operations, providing processing have plenty of opportunity to complete before the beginning of the next business day |  | Services processes background activity in a paged, multiple threading manner. |  |  |
|  | QR-DEF-PRF- 00 | Default/ Performance/ Timing/ Background Tasks | | Services MUST process background processes throughout the day. | Processing background tasks after hours is common – but illogical to run important tasks when no support, operations, or security specialists are working. |  | Services processes background activity as a separate service account running a separate process, accessing the same database. |  |  |

## Compatibility

*ISO-25010 Definition:* *the degree to which a product, system or component can exchange information with other products, systems or components, and/or perform its required functions while sharing the same hardware or software environment. This characteristic is composed of the sub-qualities listed below.*

### Co-Existence

ISO-25010: the degree to which a product can perform its required functions efficiently while sharing a common environment and resources with other products, without detrimental impact on any other product.

Requirements: None

### Interoperability

ISO 25010 Definition: the degree to which two or more systems, products or components can exchange information and use the information that has been exchanged.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  |  | | Default/ Compatibility/ Interoperability/ IdP | Services’s services MUST be integrated with mutually agreed 3rd party IdPs using current standards. | The service must avoid persisting Personal Credentials -- whether plaintext, encrypted, hashed – and prefer relying on an external dedicated service to perform this specialist task. |  | It is a security hazard to persist user passwords in a system. |  |  |
|  | QR- DEF- COM- 00 | Default/ Compatibility/ Interoperability/APIs | | The service MUST permit the extraction of the vast majority of system managed resources, metadata and relationships via APIs. | The primary purpose is to avoid vendor lock in.  At end of service lifespan, the system’s data must be extractable, transformable, for import into the service’s replacement.  The APIs should be specific to the task, REST-ful,  preferably Queryable.   Preferably adhering to domain specific standards if they are available.  SAML’s unwarranted complexity for HTTP/S based systems put delivery timelines unnecessarily at risk, while increasing deployment and maintenance coordination requirements and associated costs. | APIs are available for:  - System Roles - Users - Groups - Group Roles - User Roles in Groups - Reference Data - Resources (Records and Media) - User Roles to Resources | Use APIs: extracting data from databases introduces security (unauditable etc.) and data validation errors,  The APIs must be specific to importing, managing and extracting data, and not be simply reused UX (e.g. limited to looking at one group/tenant at a time) or Reporting APIs (hopefully provided secure aggregated views, but this is insufficient to extract data into another system for Business Continuity purposes). |  |  |
|  |  | Default/Compatibility/Interoperability/OAuth2 | | The service MUST use the OAuth2 protocol to authorise 3rd party services to use the service’s APIs. |  |  | Note that OAuth2 is an *Authorising* protocol, not *an Authentication* protocol.  Note also that the protocol leaves it up to implementors to mutually agree on if and how to transmit information about the actual user of the remote service, for auditing reasons. |  |  |
|  |  | Default/ Compatibility/ Interoperability/OIDC | | The service MUST use OIDC as the protocol used to authenticate users. | SAML’s unwarranted complexity for HTTP/S based systems put delivery timelines unnecessarily at risk, while increasing deployment and maintenance coordination requirements and associated costs. | Sighting: Report that OIDC is used to authenticate users. | Note that while OIDC is built upon OAuth2 protocol, the methodology is implemented slightly differently by each IdP. |  |  |
|  |  | **Default/ Compatibility/ Interoperability/MTA** | | Custom code services MUST be integrated via SMTP to a provided Mail Transfer Authority (MTA). | The service is required to notify users, including those not currently using the system. |  | The integration is expected to either via SMTP or a REST-ful API endpoint. |  |  |
|  |  | **Default/ Compatibility/ Interoperability/ Data warehouse** | | Services’s services MUST be capable of having key information extracted for pickup by or direct publishing to APIs of, a data warehouse. | Disjointed system information limit the development of holistic insights to inform business decisions. | Data can be exported via system APIs, for transmitting to a provided target for subsequent pickup. | The common approach is to allow an ETL service invoke a system’s APIs to collect information to deposit in a location for pickup by the Data warehouse. |  |  |

## Usability

ISO-25010 Definition: the degree to which a product or system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use. This characteristic is composed of the sub-qualities listed below.

### Appropriateness Recognisability

ISO-25010 Definition: the degree to which users can recognize whether a solution is appropriate for their needs.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | | | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR-DEF-USA-APP-00 | | Default/ Usability/ Appropriateness/ |  | |  |  |  |  |  |
|  | QR- DEF- USA- 00 | | Default/ Usability/ ----/ Configurability | Services’s mutable system configuration values MUST be configurable via a Service Client User Interface. | | Mutable system configurations must be configurable by the automated deployment process, and in extremis, by Operations Specialist intervention until the next system deployment. |  | Services’s mutable system settings are presented on a System Configuration view. |  |  |
|  | QR- DEF- USA- 00 | | Default/ Usability/ Learnability/ Training | Services MUST be intuitive enough to not require users to undergo training to use the solution. | | The cost of training becomes a cost born by the sponsor.  It is inappropriate that a sponsor must bear an additional cost on to resolve an in adequacy in usability that was already paid to vendors to resolve in the first place. |  | The number of users of the system makes it cost prohibitive to make them undergo training.  Even for internal users, the cost of training becomes a cost born by the sponsor.  It is inappropriate that a sponsor must bear an additional cost to resolve an inadequacy in usability that was already paid to vendors to resolve in the first place.  Services may provide a digital help system that is readily available to both unauthenticated and authenticated system users. |  |  |
|  | QR- DEF- USA- 00 | | Default/ Usability/ Operability/ ??? | Services MUST be operable by the widest range of users. | |  |  | Services follows AoG mandated rules for Usability & Accessibility  Services uses graphics suitable for visually impaired users.  Services uses culturally appropriate graphics.  The style sheet allows for dynamic resizing of the interface in order to make text more easily readable.  The HTML is decorated with ARIA tags to make it easier to read by blind readers. |  |  |
|  | QR- DEF- USA- 00 | | Default/ Usability/ Operability/ Malware Detection | Services MUST protect users from downloading malware by inspecting uploaded media for malware. | | The reputation of the organisation is dependent on users trusting its services to do them and their group or organisation no harm. |  | Services uses a 3rd party service to inspects media uploaded by end users.  Services can handle checking multiple files in one operation.  Services does not persist media that is infected.   Services can rely on an external WAF to do this but preferably performs checks itself. |  |  |
|  | QR- DEF- USA- 00 | | Default/ Usability/ Operability/ User Management | Services MUST not require centralised management to manage users, groups or permissions. | | Users closest to work are in the best place to make decisions of whom they wish to work with. |  | Services allows appropriate users other than centralised specialist staff (e.g., support specialists & business support specialists) to manage users, groups, obligations, permissions, roles. |  |  |
|  | QR- DEF- USA- 00 | | Default/ Usability/ Operability/ Web Browsers | Services MUST be operable from the widest range of current common browsers. | | Services must be accessible and productive from the devices commonly used by both service provider stakeholders and service consumers. |  | Services is accessible via the latest web capable devices (desktop, laptop, tablet, mobile).  Services is to remain accessible from the latest 3 automatically released versions of the 3  most used browsers (Edge, Chrome, Safari), on web capable desk and mobile devices. |  |  |
|  | QR- DEF- USA- 00 | | Default/ Usability/ ???/ Localisation | All UX text and images other than user submitted media MUST be translatable to multiple languages. | | The system must be accessible to more than just English language speakers. |  | Services is capable of using language packs to localize the user interface's images and text.  Services’s text and images are managed in language-culture packs  Different cultures may use different imagery  Services SHOULD be capable of handling the different orientation of text in different cultures |  |  |
|  | QR- DEF- USA- 00 | | Default/ Usability/ ???/ Localisation/ Layout | The UX SHOULD be able to be different depending on the culture | | In addition to changing text and images, some cultures may desire different layout. |  | Services’s service client interface can reference different style sheets depending on the presentation culture. |  |  |
|  | QR- DEF- USA- 00 | | Default/ Usability/ Operability/ Search/ Flexibility | The Solution MUST provide the means to search for records in a case-insensitive, accent-insensitive, culture phonetically aware manner. | |  |  | For example, en-NZ and mi-NZ pronounce ‘wh’ differently. Māori words have macrons that English speakers may not attempt to include, etc.  Note that providing an effective search diminishes the reliance and effort required to develop a deeply nested Menu, which is especially problematic on mobile interfaces. |  |  |
|  | QR- DEF- USA- 00 | | Default/ Usability/ Operability/ Search Synopsis | Services MUST provide a generalised means to search the solution for Synopsis records of users and resources, returned in a filtered and paged manner. | | Services are to allow users to easily develop, persist and re-find stored information.  Note:  Paging is a required precaution against DOS resource consummation attacks. |  | Services search service is universal in that it searches across all key elements of the system.  Services search is text based.  Services search may be filtered by textually entered constraints, rather than by use of secondary controls (e.g., one can type a date range, rather than have to use two different date controls).  Results are returned as Synopsis records, summarising key information of the found records (much as Google makes summaries of web pages)  Synopsis records provide links to the source record being summarised. |  |  |
|  | QR- DEF- USA- 00 | | Default/ Usability/ Operability/ Default/ Usability/ Operability/ Reportability/ Reports | Services MUST be capable of developing user refined and filtered Reports on Diagnostics, Errors, Sessions, Users, Groups, User submitted Resources, User submitted Resource Usage, System Resource usage (CPU) and System Responses. | | Decisions as to how to spend resources are aided by reports demonstrating current conditions.  Decisions are often done by governance boards whose members do not access the system, or its views (refer to a requirement defined elsewhere in this catalogue, defining that Reports must be printable). |  | Services may leverage 3rd party analysis and reporting services that have access to a duplicate read-only database for reporting purposes only.  The reporting database is separate from the production system to ensure complex reporting operations do not negatively affect system performance. |  |  |
|  | QR- DEF- USA- 00 | | Default/ Usability/ Operability/ Reportability/ Channels | Services MUST be capable of developing both on screen and printed versions of reports. | | Although a need that is diminishing in a digital era, there is still value in having physically distributable artefacts of information. |  | Services generates reports that are for screen display, that include a link to the same information, prepared for printing.  Note: The currently preferred solution is to link to print ready PDF documents, rather than using web print-specific CSS tags (they rarely produce better than rudimentary results). |  |  |
|  | QR-DEF-USA-00 | | Default/ Usability/ Operability/ Alerts/ Abnormal Behaviour | Services MUST be capable of alerting subscribed stakeholders to abnormal behaviour | | Alerting operations and/or security specialists early can allow them to defend a system against manual or automated access to data. |  | Services SHOULD be able to notice abnormal activity by time, volume, source, illogical flows that may indicate automated searching for authorisation or validation weaknesses.  A WAF, separate from this solution can be used to fulfil most or all these tasks. |  |  |
|  | QR- DEF- USA- 00 | | Default/ Usability/ Operability/ Alerts/ Errors | Services MUST be capable of alerting subscribed users of errors | | Errors should be flagged to stakeholders who can analyse error reports and action any required resolution of the logged problem. |  |  |  |  |
|  | QR- DEF- USA- 00 | | Default/ Usability/ Operability/ Error Protection/ Meaningful Messages | The system MUST inform the end user of a failure that caused the request to not be successfully completed.  The application displays a generic plain English message to the user advising there has been a unexpected failure.  Messages are sanitised of PII or confidential credentials before persistence or presentation. | | Informing users of the category of the error may help inform conversations they may have with support services. |  | The   solution catches, logs, sanitizes & reports exceptions and stack traces, for errors including the following:  Network failure  3rd party service failure  Data storage exceptions  Application exceptions  User Authentication failure  Resource location failure  A unique identifier (UUID) is developed for the report, which is referenced when notifying the end user that an error has occurred, so they can refer to it if they ask for assistance from support specialists. |  |  |
|  | QR- DEF- USA- 00 | | Default/ Usability/ Operability/ Error Flow | In the event of an error the solution MUST provide the instructions describing the correct steps for a user or system. | | Informing users what to do next may help users continue with their intended or alternately achievable tasks. |  | Services presents information to the user on how to proceed. |  |  |
|  | QR- DEF- USA- 00 | | Default/ Usability/ ???/ Documentation | Services MUST be accompanied with sufficient documentation for all components to be deployed, maintained and operated by revolving resources over the solution’s service lifespan. | | Developers and testers not expected to stick with the project for the service's lifespan.  In order to ensure their knowledge is not lost, documentation is required.  Better yet, automated tests that demonstrate how the system works should be developed prior to beginning work items. |  | Developers can rely on automated tests to understand functionality developed by others, rather than having to rely on outdated and poorly maintained documents describing components that should be regularly evolving.  Documentation is electronically stored, preferably within a wiki.  Documentation can be made open and public, because developers do not access to configuration secrets, and therefore run less of a risk of including within documentation compromising information. |  |  |
|  | QR- DEF- USA- 00 | | Default/ Usability/ UI Aesthetics/AoG | Services MUST meet All of Government (AoG) UI design guidelines. | | Reusing AoG aesthetic guidelines improves recognisability and decreases the effort required to learn to use a solution's services. |  | Services service client interface can be skinned to align with the aesthetics of this organisation, and/or AoG directives. |  |  |
|  |  | | Default/ Usability/ ???/ User Voice/System | Services MUST provide a means to collect and display User Rating and Feedback of the system, its Features and its Resources. | |  |  | To improve the service during the whole service lifespan, Stakeholders and Users must be able to express their approval or disapproval of the service. |  |  |
|  | QR- DEF- USA- 00 | | Default/ Usability/ ???/ User Feedback/ Features | Services MUST provide a means to collect and display User Rating and Feedback of the system’s Features. | |  |  | To improve the service during the whole service lifespan, Stakeholders and Users must be able to express their approval or disapproval of individual features. |  |  |
|  | QR- DEF- USA- 00 | | Default/ Usability/ ???/ User Feedback/ Resources | Services MUST provide a means to collect and display User Rating and Feedback of Records and Resources within the system. | |  |  | To improve the service during the whole service lifespan, Stakeholders and Users must be able to express their approval or disapproval of records and resources made available by the service. |  |  |

### Learnability

ISO-25010 Definition: the degree to which a solution enables the user to learn how to use it with effectiveness, efficiency and in the case of an emergency.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR-DEF-USA-LRDN-00 | | Default/ Usability/ Reconisability/ Learnability/ DNS | The system MUST be configurable to be discoverable via predictable paths following guidance on DNS naming strategies. | Users should be able to find the service using predictable URL patterns. | URL for different environments (ST, UT, PR, etc.) of the service follow organisation guidance for DNS naming conventions. |  |  | While DNS installation is an implementation detail, it is important to know whether a SaaS can accommodate customer specific DNS names or not (e.g.: can only host the service as a subdomain: mycorp.ourservice.tld) |
|  |  | |  |  |  |  |  |  |  |

No Requirements.

### Operability

ISO-25010 Definition: the degree to which a product is easy to operate, control and appropriate to use.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR- DEF- USA- 00 | Default/ Usability/ ----/ Mobile PWA | ‘Custom Code’ interfaces MUST be web and mobile capable web pages, preferably following Progressive Web App (PWA) Single Page Application (SPA) development patterns. | Services must be accessible via the most prevalent devices (mobile).  Services must take advantage of the devices and sensors available in a device to provide a better user experience (based on location, etc.) |  | Services user interface is separate from the service.  Services user interface is developed using the most current recommended development practices in order to provide the longest use. |  |  |
|  | QR- DEF- USA- 01 | Default/ Usability/ Learnability/ Layout | Services SHOULD use standard UX layout approaches. | Use of standard graphical and behavioural design patterns improves usability and decreases input errors. |  | the solution uses a common CSS framework such as Bootstrap, etc. |  |  |
|  |  | QR-DEF-USA-00 | Default/Usability/Operability/Operability/Copy/Understandable | The System’s Instructions (interface text, alerts, warnings, notifications, etc.) MUST be easy to understand by non-technical users. | Clarity of instructions on how to use the system improves efficiency while reducing full service-lifespan support costs. |  |  |  |
|  | QR-DEF-USA-00 | Default/ Usability/ Operability/ Meaningful Error Messages | Services MUST present informative specific error messages that explain the cause and user available remaining options. | Clarity of instructions on how to use the system improves efficiency while reducing full service-lifespan support costs. |  | Informing users of the category of the error may help inform conversations they may have with support services.  Consider providing each error message with its own GUID that can be referenced in support calls.  Consider ensuring error messages are presented along with an actionable Primary Action (OK, etc).  Avoid causing users uncertainty and frustration from generic undescriptive system HTTP errors. |  |  |
|  | QR- DEF- USA- 00 | Default/ Usability/ Operability/ Search/ Generalised | Any custom service client element of the solution MUST provide a generalised means to search the solution for Synopsis/SummaryItem records of users and resources, returned in a queryable, filtered and paged manner.  Free form text-based search capabilities (as opposed to requiring dropdowns to filter) are a real benefit. | Services are to allow users to easily develop, persist and re-find stored information. |  | Note: Paging is a required control as a precaution against DOS resource consummation attacks. |  |  |
|  | QR-DEF-USA-00 | Default/ Usability/ Operability/ Universality | Services MUST by default handle Unicode, UTF-8 transmission, and UTC datetimes. | Services must persist and transmit universal data. |  | The database is developed to persist Unicode.  UTF-8 Character set encoding is used in transmission between components  Validation allows Māori macrons and other variants (ā, ē, ō, etc.)  Search is case insensitive, can handle omissions of Macrons, and/or variations in spelling (‘wh’ / ‘f’). |  |  |
|  |  | Default/ Usability/ Operability/ RoleMgmt/ Self-Reliant | Services MUST not rely on 3rd party services to provide the means to manage users, groups, permissions or roles. | Systems may integrate with other services for non-core functionality, but must be self-reliant fore core functionality. |  | Users closest to work are in the best place to make decisions of whom they wish to work with.  The system may be *informed* by information received from another service (AD, AAD, IdP), but the system must be able to manage these services on its own (with its own API and GUI views, etc).  *Note: It is an antipattern to not include management of core system entities, expecting to save money by relying on a shared enterprise service.* |  |  |
|  | QR-DEF-USA-00 | Default/ Usability/ Operability/ Disclosures/Custom | The Service GUIs MUST permit linking to one or more Disclosure statements: - tracking statement, - personal information and data collection statement - etc. | Solutions must disclose to end users intentions, etc. |  |  |  |  |

### User Protection Error

ISO-25010 Definition: the degree to which a solution protects users against making errors.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | | | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR- DEF- USA- 00 | | Default/ Usability/ Validation/ ServerSide | Services tier MUST validate all input at the Service Facade. | | Services must protect the data quality using validation -- irrespective of the UI used. |  | Services must use a common validation approach irrespective of the Service Client used.  *Note that the solution service client repeats the validation to provide a better user experience.* |  |  |

### User Interface Aesthetics

ISO-25010 Definition: the degree to which a user interface enables pleasing and satisfying interaction for the user.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | | | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR- DEF- USA- 00 | | Default/ Usability/ Aesthetics/ Branding | Services MUST be brandable with  - org logo,  - org name, - org subtitle | | Services must be recognisable to be trusted. |  |  |  |  |

### Accessibility

ISO-25010 Definition: the degree to which a solution can be used by people with the widest range of characteristics and capabilities to achieve a specific goal in a specified context of use.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | | | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR-DEF-USA- 00 | | Default/ Usability/ Accessibility/ WCAG | Service Graphical User Interfaces (GUI) MUST meet WCAG 2.2 standards to an Level AA or higher. | | Services must be usable by visually impaired users. | Sighting of a report summarising the score of the system, and it’s achieving a Level AA or better. | The organisation of data for WCAG impacts other positive outcomes. Notable succinctness of interfaces, organised repeated layout patterns, etc.  Note:  WCAG 2.0 is an ISO standard: ISO-40500. |  |  |
|  | QR- DEF- USA- 00 | | Usability/ Accessibility/ Print | Services MUST be capable of developing both on-screen and independently developed printed versions of resources.  Note: Print artefacts must not include navigation, status and context screen artefacts. | |  |  | Although a need that is diminishing in a digital era, there is still value in having physically distributable artefacts of information.  Note: It is common that Resources are developed using print-focused style sheets, but based on current limits with this approach, it is recommended that resources are developed into print specific formats (e.g., PDF) for better quality print artefacts. |  |  |
|  | QR- DEF- USA- 00 | | Usability/ Accessibility/ Universal Design | Universal Design Principles MUST be adhered to when developing custom interfaces. | |  |  | Universal Design is the design and composition of an environment so that it can be accessed, understood and used to the greatest extent possible by all people regardless of their age, size, ability or disability. If an environment is accessible, usable, convenient and a pleasure to use, everyone benefits. |  |  |
|  | QR- DEF- USA- 00 | | Usability/ Operability/ Provisioning/ Users/ JIT | Services MUST be capable of processing IdP issued identy tokens to create Users Just In Time (JIT). | |  |  | The creation of system users should not require manual provisioning tasks.  Note: The assignment of Roles requires more steps. |  |  |

## Reliability

*ISO-25010 Definition:* *Degree to which a system, product or component performs specified functions under specified conditions for a specified period of time. This characteristic is composed of the sub-qualities listed below.*

### Maturity

ISO-25010 Definition: the degree to which a solution needs for reliability, under normal operation.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR-DEF-REL- 00 | Default/ Reliability/ Maturity/ Supported Technologies | | Services language, framework and components MUST be accreditable as supportable technologies. | Services must be developed using a language and framework that decreases the number of errors in a system. |  | Services is developed using components that this organisation's accreditation and security specialists do not raise as risks. |  |  |
|  | QR-DEF-REL- 00 | Default/ Reliability/ Maturity/ Development Language | | Services SHOULD be developed using a compiled language. | Compilers can prevent errors by pre-compilation that are not discoverable by scripts languages which can only discover them during run-time. |  | Services is built with a compiled language to limit the number of bugs that make it to a production environment.  Services development team uses strict compilation flags to find and force the fixing of errors early. |  |  |
|  | QR-DEF-REL- 00 | Default/ Reliability/ Maturity/ Development Framework | | Services MUST use a development Framework that is usable on multiple platforms. | No OS has complete dominance of the market and it is virtually certain that a solution has to be capable of running on different OSs. |  | Services is built in on a common framework, such as:  .NET Core (as opposed to the older Windows specific .NET Classic Framework)  Java (with reservations due to Oracle's licensing costs). |  |  |
|  | QR-DEF-REL- 00 | Default/ Reliability/ Maturity/ Single Point of Failure | | Services MUST be designed to minimise the number of Single Points of Failure. | If a component of the system fails (e.g., caching) the system must be resilient enough to continue to function until the issue can be addressed. |  | Services is capable of working if caching is unable to work.  The number of connections to the database is minimised per request. |  |  |

### Availability

ISO-25010 Definition: the degree to which a service is available and operable to service consumers when required for use.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR-DEF-REL- 00 | Default/ Reliability/ Availability/ Horizontally Scalable | | Services MUST be capable of supporting the projected number of concurrent and absolute users as defined in the *Target Quality Objectives* table, by dynamically scaling horizontally based on the CPU being consumed at higher than a specified %, for longer than a specified duration, scaling down later based on another CPU % value. | The system must be capable of running economically when not in demand, while not compromising its ability to meet projected peak demand. |  |  |  |  |
|  | QR-DEF-REL- 00 | Default/ Reliability/ Availability | | Services MUST meet the availability expectations defined in the ‘Target Objectives’. | The system must be capable of operating during the hours users are most expected to use the system, meeting the demand, throughput and response criteria listed in the ’Custom Code’.  In the case of a planned or unplanned outage, the solution must be able to be fLreturned to a functionality state in the shortest amount of time. |  | Services is deployed to cloud infrastructure that has a higher uptime SLA than the one described within the ‘Target Objectives’.  Services is protected by a WAF to limit DoS attack traffic.  Services is horizontally scalable to handle surges of demand.  The number of connections to the database is minimised per request to diminish QR-DEF-REL-00 the chance of the database becoming a bottleneck.  Services uses caching to limit the number of threads required to communicate across tiers to the database to diminish the chance of it becoming a bottleneck.  Complex queries for reporting are delegated to a separate reporting database.  The database is backed up regularly for DR restoration.  Services is deployed using Infrastructure as Code, so that a new production environment can be re-developed quickly after a Disaster.  Services is accompanied with an automated DR recovery solution. |  |  |
|  | QR- DEF- REL- 00 | Default/ Reliability/ Availability/ Scheduled Downtime | | Users MUST be given notice in-system (as a banner for example) as to when solution capabilities and components will be rendered inaccessible, and for how long (while continuing to meet MTD expectations). |  |  | Users require foreknowledge, and Support specialists require foreknowledge as to when users may inquire as to why a service is no available. |  |  |
|  | QR-DEF-REL- 00 | Default/ Reliability/ Availability/ Restart | | The process of restarting or recovering after a service or component outage or failure MUST NOT require needing to restart the underlying infrastructure of the services. | Minimises the downtime experienced by users by simplifying the process of restarting the solution and automating it to make it more efficient for support staff. |  | Services restarts itself after a system reset upon the first request.  The deployment pipeline has a final step to invoke the service and wake it up, ensuring the first user is not faced with a longer than usual delay. |  |  |

### Fault Tolerance

ISO-25010 Definition: the degree to which a solution operates as intended despite the presence of hardware, software or user faults.

Requirements: None

### Recoverability

ISO-25010 Definition: the degree to which, in the event of an interruption or failure, a solution can recover the data directly affected and re-establish the desired system state.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR-DEF-REL- 00 | Default/ Reliability/ Recoverability/ Backups | | Services MUST include a regular and fully automated backup and restoration process strategy that meets Response Point Objective Time (RPO) and Response Time objectives (RPT) targets as defined in the ‘Target Objectives’. | Upon corruption of PROD data, data should be restored from backups. |  | Services data is backed up in full every day.  Services data is backed up incrementally at an interval that satisfies the constraints defined in the ‘Target Objectives’.  Services backups are kept for a delay defined in the ‘Target Objectives’.  Backups are kept in a resource group separate to the production data's resource group.  Backups are taken, restored and accessed only by the deployment pipeline's agent (to remain in conformance of ISO-27001 requirements). |  |  |
|  | QR-DEF-REL- 00 | Default/ Reliability/ Recoverability/ Geo Resilience | | Services design SHOULD be ensure it is resilient against unavailability of infrastructure in the default area. | Regional network failures may make services in other countries temporarily unavailable. |  | Services is developed using Infrastructure as Code so can create a new environment in a new location, if directed to. |  |  |
|  | QR-DEF-REL- 00 | Default/ Reliability/ Recoverability/ Transactions | | All change request operations SHOULD be committed within a single end of request Transaction. | Failure in mid request can lead to only half the information being committed, leading to difficult to trace errors. |  | Services attempts to ensure that write operations are committed within a transaction so that all operations either occur together, or don't.  Services is developed using an ORM to handle requests (as they generally are wrapped in transactions).  Services collects and holds a request's write operations and only triggers them at the end of the request to limit hard to trace/resolve "half/writes". |  |  |
|  | QR-DEF-REL- 00 | Default/ Reliability/ Recoverability/ Offline | | Services MUST not be made unavailable for longer than the Maximum Tolerable Downtime (MTD) defined in the ‘Target Objectives’. | The system must not be made unavailable for use for longer than necessary. |  | Recommended approaches include: Automating delivery pipelines, using Infrastructure as Code, Database schema as Code, Automated database backup restoration to permit – in the case of a Disaster – the recreation of a completely new environment within the delay stated within the ‘Target Objectives’. |  |  |
|  | QR-DEF-REL- 00 | Default/ Reliability/ Recoverability/ Scheduled Downtime | | Stakeholders and users MUST be given notice as to when solution capabilities and components will be rendered inaccessible. | Users require foreknowledge, and Support specialists require foreknowledge as to when users may inquire as to why a service is no available. |  | Services notifies end users as to upcoming events that will take the service offline.  System Notifications are available as interface banners, and/or alerting subscribed stakeholders. |  |  |
|  | QR-DEF-REL- 00 | Default/ Reliability/ Recoverability/ Scalability/ Users | | Services MUST be capable of supporting the projected number of concurrent and absolute users as defined in the ‘Target Objectives’. | Services must remain accessible through the service's expected lifetime.  The system must be capable of running economically when not in demand, while not compromising its ability to meet projected peak demand. |  | Services dynamically scales horizontally based on the CPU being consumed at higher than a specified %, for longer than a specified duration.  Services dynamically scales back down based on the CPU consumption falling lower than a specified % for longer than a specified duration. |  |  |
|  | QR-DEF-REL- 00 | Default/ Reliability/ Recoverability/ Fault Tolerance | | Services MUST trap unexpected errors and capture relevant information in permanent records. | Services must record error reports for later analysis by operations specialists. |  | Services creates error records and persists them to facilitate analysis later, the solution’s error records storage is filterable and searchable error records are given a unique UUID, which is shared with the system user, for later sharing and discussion with Customer Support specialists. |  |  |
|  | QR-DEF-REL-13 | Default/ Reliability/ Recoverability/ Recoverability | | Services MUST be able to recover from unexpected behaviour. | Services must be capable of continuing to perform, even if it encounters an unexpected error – just log it for later analysis, conditionally alert operations specialists, and continue. |  | Services traps all unexpected logical and component errors, alerts subscribed stakeholders, and resets state to allow for handling subsequent requests. |  |  |
|  | QR-DEF-REL- 00 | Default/ Recoverability/ Recoverability/ MTD | | Services MUST be capable of meeting the Maximum Tolerable Downtime (MTD) specified in the ‘Target Objectives’. | The reputation of the organisation is associated to the ability of end users being confident that the service they used will be available when needed – and if it goes down, that it is a both a rare occurrence, and that the service re-becomes available in an acceptable amount of time. |  | Services cloud provider’s SLAs, combined with the solution’s fully automated DR recovery process ensure that the stated MTD is achievable. |  |  |
|  | QR-DEF-REL- 00 | Default/ Recoverability/ Recoverability/ DR | | Services MUST meet be able to recreate a new environment and be operational within the delay specified in the ‘Target Objectives’. | Cloud infrastructure reduces but does not eliminate the chance of having to recreate a new environment. |  | Services uses automation to recreate environments as needed, including restoring data from backups, within short delays. |  |  |

## Security

*ISO-25010 Definition: the degree to which a product or system protects information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization. This characteristic is composed of the qualities listed below:*

Security is the practice of maintaining the confidentiality, privacy, integrity and accountability of data changes by controlling authorised access, use and disclosure, while preventing unauthorised use, disruption, modification or destruction.

Note:  
Availability is a *related to Security (see CIA) but is defined elsewhere, under*Reliability*.*

### General

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR-DEF-SEC- 00 | Default/ Security/ Integrity/ Controls/ OWASP | | Services MUST implement the Top Ten Application Security Risks recommended mitigations controls of the Open Web Application Security Project (OWASP)'s recommended mitigation of the latest. | Decrease risk by following the advice of a reputed source of current knowledge regarding web application vulnerabilities. |  | Services service and client systems are expected to be hardened against:  - code injection - broken  authentication - sensitive data  exposure - broken   access controls - security  misconfiguration - cross site  scripting (XSS) - cross site  request forgery  (CSRF) - insecure  deserialization - using  components   with known  vulnerabilities - insufficient  logging and  monitoring |  |  |
|  | QR-DEF-SEC-INTE-00 | Default/ Security/ Integrity/ Defence in Depth | | Services MUST apply recommended risk mitigations to keep the system’s information secure. | Contributes to a defence in depth approach to slowing the progress of attackers. |  | Personnel Training  ISO-27001 Level 2+ Cloud Service Provider,  Physical access restrictions,  Firewall route protection,  WAF for active intrusion and DoS protection, monitoring, and alerting subscribed specialists.  Encrypted communication channels between devices  Dynamically horizontally scalable infrastructure to handle sustained peek requests,  Access to all UI operations and APIs endpoint are protected by authentication, authorisation and auditing.  Encrypted datastores  Service Accounts for dependency services are managed by 3rd parties.  Credentials required for access to integrated dependency services are persisted in specialised encrypted storage.  Network, Device, and OS hardening. |  |  |

### Confidentiality

ISO-25010 Definition: the degree to which the solution ensures data is accessible only by those authorised to do so.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR-DEF-SEC- 00 | Default/ Security/ Integrity/ Access/ Physical | | Any location where Production data is persisted MUST adhere to ISO-27001 level 2+ constraints on physical access. | Systems can be secured, but users should not be able to directly access, clone or remove physical or virtual hard drives which contain production data or backups of production data, especially if the access is not audited. |  | Services environments are hosted within an ISO-27001, Level2+ based data facility, which limits, monitors and audits physical and virtual access to devices.  Services is hosted within an accredited cloud provider.  Physical and virtual media devices containing production data are not removed from their environment, and when disposed of are sanitised first then disposed of securely |  |  |
|  | QR- DEF- SEC- 00 | Default/ Security/ Integrity/ Access/ Non Users | | Direct access to system data MUST not be permitted by any person who is not an Authenticated, Authorised and Audited User. | In depth protection cannot be successfully applied if a group of users are permitted to circumvent physical and/or logical controls. |  | Access to system data, production as well as non-production data is restricted.  This applies to non-prod environment devices and data as non-prod data environments are meant to test and demonstrate the controls applicable in a production data environment.  Diagnosis of issues should be via diagnostic tracing, not circumventing data access controls.  The granting access to data storage is given only to deployment service accounts, and must exclude physical or virtual access by: - Developers,  - Test analysts,  - Stakeholder analysts,  - Operations specialists - Maintenance specialists.  The Functionality required for these stakeholders to perform their jobs without breaching this requirement must be provided for by the solution (i.e. diagnostics tracing, and error recording, both accessible by filtered searching, etc). |  |  |
|  | QR-DEF-SEC- 00 | Default/ Security/ Integrity/ Information/ In Transit/ Encryption | | Services MUST protect information between devices crossing network boundaries by encrypted channels, falling back to encrypted messages where not possible with common processes. |  |  | Services channel encryption is achieved using TLS based HTTP (HTTP/S) communication between all internal and external components.  Services encrypts any other channel (e.g., database connections use the secure flag).  Message Encrypting is appropriate if channel encryption is not achievable.  Digital signatures may be relevant on a case-by-case basis when messages pass through tiers which remove or replace channel encryption (e.g., corporate firewalls). |  |  |
|  |  |  | | Unsecured communication to services MUST not be accepted, redirecting to secure equivalents. | Users type addresses into browsers without prepending with HTTPS, defaulting to HTTP. | Sighting: Invocations to service endpoints using insecure HTTP are not accepted.  For better user experience, they should be redirected to the same endpoint | Redirection is a configuration done at the server level, not the application installed within it. |  |  |
|  | QR-DEF-SEC- 00 | Default/ Security/ Integrity/ Information/ Credentials/ Clear Text | | Credentials MUST not be transmitted or persisted in clear text. | Even if the overall datastore is encrypted, or the transmission channel and message within are encrypted, credentials SHOULD not be transmitted in clear text. |  | Where technically feasible, the solution is integrated with external services without transmitting clear text credentials.  Channels pass through devices and services (e.g.: WAFs) that may strip off encryption, log traffic and message contents, before re-attaching new encryption. This becomes a source of data leakage, and therefore risk. |  |  |
|  |  |  | |  |  |  |  |  |  |
|  |  |  | |  |  |  |  |  |  |

### Integrity

ISO-25010 Definition: the degree to which the solution prevents unauthorised access, modification of systems and the information they manage.

Integrity builds upon Confidentiality in that in addition, changes to data and resources are controlled by permission.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | | | ID | | Statement | | Rationale | | Fit Criteria | | Details | | Response | Analysis |
| QR-DEF-SEC-CONF- 00 | | Default/ Security/ Confidentiality/ Permission Based | | | The system MUST protect Resources by only permitting Authorised Users. | | Protection of Resources by access controls contributes to a Defence in Depth strategy. | |  | | While the permission system can be Role based, it is our experience that systems are more flexible if they are Permission based, (using Roles as logical groupings of Permissions, assignable to Users). It is also our experience that systems are more flexible if Roles are not System based, but Group based (Accountable, Contact Person, Member, Guest, etc.) and Resource based (Creator, Contributor, Reviewer, Approver, Maintainer, etc.). | |
|  | QR-DEF-SEC-00 | | Default/Security/Confidentiality/Public Users | | | The system MUST permit non-authenticated public users having access to some Resources. | |  | |  | | While most Resources are non-public, there may be a benefit to permit public non-authenticated access to some records. | |  |  |
|  | QR-DEF-SEC-INTE-00 | | Default/ Security/ Integrity/ Least Privilege | | | Services MUST anonymous Public Users to the least privileges while still being permitted to view publicly accessible Views. | | Systems always have areas of views accessible to public users to provide information and or functionality to authenticate to the system. | | Sighting: An unauthenticated public User can access some Views of the system. | | A public area will at least contain a link to one or more public IdPs.  A public area may contain self-help documentation, etc. | |  | Can public unauthenticated users view some system Views?  Is access to and operations upon these view audited? |
|  | QR-DEF-SEC- 00 | | Default/ Security/ Integrity/ Required Privilege | | | Services MUST allow operators and business service administrators to attribute to or invite end users the least amount of privilege needed to perform their tasks. | | Avoid the risk of unauthorised unpermitted activity (accidental or otherwise). | | Sighting: documentation of the system permission to role matrix, the role given to system operators, business service support specialists, and new users. | | Roles can be System, Group or Resource Roles.  Roles are logical bundles of Permissions.   It is preferable to Invite users to roles than allocate them, as the workflow permits them accepting Responsibilities associated to Permissions before they Accept the Invitation to the Role. | |  |  |
|  | QR-DEF-SEC- 00 | | Default/ Security/ Integrity/ Information/ At Rest/ Encryption | | | Services MUST protect user-generated information at rest. | |  | |  | | Databases are encrypted.  Blob storage is on encrypted storage.  Diagnostic trace files on encrypted storage.  Note:  encryption at rest depends on the data information security classification specified in the ‘Target Objectives’, so in case the Data Classification rises during development, the database chosen SHOULD be able to be encrypted at database, table, or column granularity if needed. | |  |  |
|  | QR-DEF-SEC- 00 | | Default/ Security/ Integrity/ External Identity Provider Services | | | Services MUST use external Identity Provider Services to persist User Credentials. | | The less secrets maintained in a solution, the less attack surface the system has to defend. | |  | | Services can use current protocols to connect to external identity providers (OIDC, OAuth, SAML).  Services is capable of authenticating both UI and API security principles (users). | |  |  |
|  | QR-DEF-SEC- 00 | | Default/ Security/ Integrity/ External PII Management Services | | | Services SHOULD persist Personally Identifiable Information (PII) in an external specialised and hardened storage service. | | The less PII information maintained in a solution, the less attack surfaces a solution has. | |  | | Services sources PII data from an external PII service.  PII data cloned to the system's user profile is limited in scope.  Cloned PII data is persisted in an external data store separate from the system's primary database.  Note:  A key reason PII information is persisted separately is to minimise risk of data leakage when data is copied to a reporting database and/or data warehouse. | |  |  |
|  | QR-DEF-SEC- 00 | | Default/ Security/ Confidentiality/ Sanitisation | | | Services MUST sanitise diagnostics and audit records of confidential credential and other secrets. | | Persisting credentials in audit or diagnostics records allows Operations and/or Support Specialists access to confidential information they should not have. | |  | | the solution ensures that diagnostics and audit messages are scrubbed of confidential and/or personally identifiable information prior to being persisted. | |  |  |
|  | QR-DEF-SEC- 00 | | Default/ Security/ Integrity/ Information/ In Transit/ Clear Text Credentials | | | Services MUST not transmit clear text credentials. | | Even if the channel and message within are encrypted, credentials SHOULD not be transmitted in clear text. | |  | | Where technically feasible, the solution is integrated with external services without transmitting clear text credentials. | |  |  |
|  | QR-DEF-SEC- 00 | | Default/ Security/ Integrity/ Information/ At Rest/ Encryption/ Sensitive Configuration Parameters | | | Services MUST encrypt any persisted sensitive configuration information. | | If configuration secrets cannot be persisted elsewhere than in the system configuration files, databases or similar, they must deter tampering by being rendered cost prohibitive to read or modify.  Note:  Such variables must be registered on the project's risk register. | |  | | Configuration credentials are persisted in secure key storage services.  Access to production key storage services is restricted to the automated deployment pipeline agent’s service account.  Configuration credentials and settings which cannot be sourced from a separate secure storage service are encrypted in the system's configuration files.  Credentials that are persisted in the system's config file, but cannot be encrypted, are recorded in the project's risk registry. | |  |  |
|  | QR-DEF-SEC- 00 | | Default/ Security/ Integrity/ Information/ At Rest/ Encrypted/ Sensitive Configuration Parameters/ Setting | | | Services MUST use deployment automation to automatically source configuration credentials from confidential storage services and inject them into config files. | | Code repositories are not secure as they can be copied, duplicated for use anywhere. Credentials in source code repositories are compromised credentials as code repositories are not secure. | |  | | Configuration credentials are not sourced from source control, and instead are sourced from secure storage services.  The automated deployment agent injects the retrieved credentials into the deployed system's configuration files.  The configuration credentials are encrypted within the config file. | |  |  |
|  | QR-DEF-SEC- 00 | | Default/ Security/ Integrity/ Information/ At Rest/ Source Code | | | Code repositories used for Custom Code MUST be protected from committing any security credentials or environment specific information. | | Source code is used for production environments, therefore must be protected from becoming a means by which a nefarious person can discover a way to bypass a solution's security controls. | |  | | Code Branch Policies are effective against checking in bugs, but not effective against checking in confidential credentials.  Project members with write access to code repositories must be trained as to the importance of not committing credentials and reporting when such an error has happened. | |  |  |
|  | QR-DEF-SEC- 00 | | Default/ Security/ Integrity/ Information/ At Rest/ Source Code/ Contamination | | | If credentials and/or environment specific properties are checked in, steps must be taken to:  remove the credentials from the code repository and  rotate the credentials so the information is no longer a potential risk. | | Environments, whether production or non-production environments, must be protected.  Publicly accessible source code must not become a means of discovering means to bypass a solution's security controls.  Note:  Until the source code repository is cleansed the incident must be registered on the project's risk register. | |  | |  | |  |  |
|  | QR-DEF-SEC- 00 | | Default/ Security/ Integrity/ Certificate Lifespans | | | Services MUST limit the duration of certificates to short lifespans, as per the ‘Target Objectives’. | | The shorter the duration certificates are used, the less time bad actors have to crack the certificates. | |  | | Services includes automated mechanisms to regularly commission and deploy new certificates, at every deployment.  Services ensures that deployments are done frequently (approximately every fortnight), regardless of new features having been developed or not, to ensure certs are rotated often (no more than 90 days). | |  |  |
|  | QR-DEF-SEC- 00 | | Default/ Security/ Integrity/ Service Accounts | | | Services components MUST run under individual service accounts, either developed by automation or by the organisation's operation specialists. | | Use of a single service account, creates a single point of failure that if compromised provides access to multiple components. | |  | | Where technically feasible, service accounts are automatically developed.  If deploying to Azure, consider Microsoft Secure Identities (MSI).  Service accounts are distinct per tier.  Service account credentials are securely deployed by the automated delivery pipeline to service consumers. | |  |  |
|  | QR-DEF-SEC- 00 | | Default/ Security/ Integrity/ Client Credentials | | | Services MUST not deploy credentials to external clients. | | Credentials that are deployed and persisted outside a system’s infrastructure are compromised. | |  | | he solution avoids using integration approaches that require the installation of certs on service clients. | |  |  |
|  | QR-DEF-SEC- 00 | | Default/ Security/ Integrity/ Information/ At Rest/ Logs | | | Solution audit, debug and access logs MUST be protected from tampering | |  | |  | |  | |  |  |
|  | QR-DEF-SEC- 00 | | Default/ Security/ Integrity/ Production Data | | | Production Data MUST not be accessible outside of the Production Environment and Production data backup environment. | | The less people who have access to information the less chance of data being divulged by accident or intent. | |  | | It is illegal to access production data when not disclosed on the data use disclosure. | |  |  |
|  |  | |  | | |  | |  | |  | |  | |  |  |

### Non-Repudiation

ISO-25010 Definition: the degree to which actions or events can be proven to have taken place so that the events or actions cannot be repudiated later.

Non-Repudiation (of Action) and Accountability (by Whom)

are associated in that non-repudiation defines the degree to which the solution can prove that actions have been taken, and accountability is being able to associate the non-repudiable (audited) activity to a specific user.

In essence, it’s the subject of Auditing the changes permitted as per the *Integrity* section above.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR-DEF-SEC- 00 | Default/ Security/ Non-Repudiation/ Permanency | | Services MUST permanently store Session Operation audit record to later correctly ascertain the process by which system or user data was changed. | Discovery of irregular activity may be months or years after the event, or happen sporadically over a long duration, so records should be kept for the duration of the solution.  Services must audit the activity of authenticated users as well as unauthenticated public users, because irregular activity can start before authentication occurs, and when they sign in, their identity be associated to all their pre-sign in activity as well.  Services must audit the activity of any background service agents (batch operations, etc.). | Sighting: There is an Session Operations table that can be reported on.  Affirmation: There is no functionality to delete entries. | Services audits operations, how and where the solution keeps these records in order to keep the solution performant, and whether the solution’s audit records are queryable when required. |  | Is there a Session Operations table?  Does it record or reference the User who made the Operations?  Are the records light to persist records without undue consumption of storage?  Are the records ever deleted? |
|  | QR-DEF-SEC- 00 | Default/ Security/ NonRepudiation/ Sessions/ Multiple | | Services MUST allow multiple concurrent Sessions per user. | A user may be signing in from a mobile device at the same time as using a desktop or laptop device.  A user may be using two different browser types on the same system.  A user may be using a browser in both normal and Private mode. | Sighted: A user can sign in via two different browsers and/or devices.  Diagnostics tracing and Session Operation auditing will shows two concurrent Sessions associated to the same user, distinguishable by different BrowserType/Client IP information. | Diagnostics and Session Operation auditing records of Anonymous Users who have not yet signed in will appear to be the same user (Anonymous) with many different concurrent Sessions.  Note that IPs change multiple times when a mobile user drives through multiple cells, and a single mobile user may appear as multiple different Sessions. |  | Is the system tracing and auditing unaudited Users?  Is the Diagnostics tracing and/or Session records keeping track of IP/browser type? |

### Accountability

ISO-25010 Definition: the degree to which the actions of an entity can be traced uniquely to the entity.

Non-Repudiation (of Action) and Accountability (by Whom)

are associated in that non-repudiation defines the degree to which the solution can prove that actions have been taken, and accountability is being able to associate the non-repudiable (audited) activity to a specific user.

In essence, it’s the subject of tying Auditing to specific authenticated system Users – noting that it doesn’t make an assumption that a system User is a correctly identified external user (see *Authenticity*, later).

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR-DEF-SEC- ACC- 00 | Default/ Security/ Accountability/ Sessions/ Authenticated User | | Services MUST record or reference the system user identity in all session audit records. | For accountability reasons, Operations that change resources must be resolvable back to the User who made the changes. | Sighting: A report generated from the Session Operations table shows Users Creating, Modifying, Removing records. | All Operations – not just CRUD ones - should be traced and audited.  This might include but are not limited to resource workflow Status changes, commenting, approvals, etc. |  | Is there a Session Operations view or report?  Does it show the User making changes?  Does it show different kinds of Operations, not just CRUD?  Does it show View operations (which can be used to inform decisions, based on better understanding how far information has already propagated)? |
|  | QR-DEF-SEC- ACC- 00 | Default/ Security/ Accountability/ Sessions/ Anonymous User | | Services MUST record or reference the system user identity in all session audit records. | Auditing of multiple attempts to login is a relevant reason to audit actions of even unauthenticated users.  A session's user may be anonymous until authenticated.  The act of Authentication does not change the session, it just clarifies who is operating the Session. |  | Services tracks anonymous users through the process of authentication, ongoing until session termination or timeout. | Custom? | Are unauthenticated users tracked and their operations audited?  How does the auditing change once they identify themselves? |

### Authenticity

ISO-25010 Definition: the degree to which the identity of a subject or resource can be proved to be the one claimed

In essence it builds upon Accountability, associating system users to actual users.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR-DEF-SEC- AUTH-00 | Default/ Security/ Authenticity/ IdPs | | Services MUST correctly ascertain the identity of system users using agreed as acceptable external Identity Providers (IdPs). | The basis of both Authorisation and Non-Repudiation of actions is based on correct Authenticating of users.  Agreed accepted user identity providers implement 2FA or similar approaches to improve identification based on age verification, device ownership, evidence of authority, etc. | Sighting: Users are authenticated via an external integrated Identity Provider.  OIDC is the protocol used. | The complexity of SAML as the basis of integration and authenticating Users is to be avoided in preference of OIDC. Use OAuth 2+ for authenticating services using the system’s APIs. |  | Is an external IdP used?  Is OIDC used? |
|  |  |  | | Authentication of users MUST NOT use in-system authentication system unless previously mutually agreed as being architecturally appropriate. | Risk of systems being compromised significantly increased when Usernames and Passwords are persisted in systems whose purpose is not specifically and only securing credentials. | Sighting Users are authenticated via an external integrated Identity Provider and there is no option to use an in-system approach to authenticate users unless mutually agreed. | There are valid scenarios where the use of an internal IdP are required -- for example, public consumer IdPs often have Terms and conditions specifying a minimum age, making them unsuitable for young learners – but this must be mutually accepted as being the only reasonable course of action. |  | Is an external IdP used?  Is OIDC used?  Are all target Users able to use the external IdP?  Is there a suitable external IdP (eg: young learner friendly) that can be used instead? |

## Maintainability

*ISO-25010 Definition: the degree of effectiveness and efficiency with which a product or system can be modified to improve it, correct it or adapt it to changes in environment, and in requirements. This characteristic is composed of the sub-qualities listed below.*

### General

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Code Repository | ‘Custom Code’ MUST be maintained and accessible in an ‘Organisation Managed’ code repository. | Code written for this organisation must be analysable for code security and quality. |  | Custom code is any code required (integration, deployment, etc.) and does not include SaaS logic.   A GitHub based repository is expected unless agreed otherwise |  |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Source Control | ‘Custom Code’ developed for the solution MUST be persisted in an ‘Organisation Managed’ distributed source code repository accessible by this organisation. | Vendor support may be appreciated and contracted, but vendor lock-in is not desired as the only option. |  | Services uses an ALM managed repository for configuration, scripts, etc. required to configure a new environment and deploy the solution’s code to it. |  |  |
|  | QR-DEF-MNT- TEST- 00 | Default/ Maintainability/ ALM | The technical management of the delivery of ‘Custom Code’ MUST be managed and operated within ‘Organisation Managed’ services. | The organisation must be able to participate in the development and delivery of the service, to contribute, as well as learn how to participate in its Support, Operation and Maintenance. |  | Consider using an Application Lifecycle Management (ALM) suite as they decrease or even remove the complexity and cost and delays of integrating common development tools (Work Item Management and Kanban Boards, Code Repositories and automated deployment pipelines). |  |  |

### Modularity

ISO-25010 definition: the degree to which a solution is composed of discrete components such that a change to one has minimal impact on others.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |

Note:  
This category is applicable to Custom services, and not SaaS services.

Requirements: None.

### Reusability

ISO-25010 definition: the degree to which an asset can be used in more than one system or reused to build other assets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |

Note:  
This category is applicable to Hosted services, and not SaaS services.

Requirements: None.

### Analysability

ISO-25010 definition: the degree of effectiveness and efficiency with which it is possible to assess the impact of a solution, a change, a failure, or determine what requires change.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | | | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | | QR- DEF-USA- UAE- 01 | Default/ Usability/ UPE/ Notifications/ Change | | Upcoming changes to the service that require the service being temporarily unavailable MUST be communicated to the users prior to the downtime. | To decrease avoidable support costs, Users should be to prepared for changes to the system. | Sighting:  Notifications should be displayed *within* the system to all users, with the configurable option of the notification being transmitted via email to subscribed users.  In-system notifications should be able to be removed once seen on a per-user basis (i.e., not remain a permanent distracting banner message).  System Operators and/or Maintainer specialists Roles can be configured to have the Permission required to post a notification.  When a system is taken offline, the system should redirect to a Status page describing why the service is not available, and when it is expected to re-established. | Note: This may be a Transitional Requirement. |  | Is the notification in-system?  Is the notification also sent externally to the system?  Using a webpage to list changes done in the past and upcoming changes in the future. |
|  | QR-DEF-MAIN-ANAL- 00 | | | Default/ Maintainability/Analysability/ Status Page | When the service is intentionally made unavailable the solution MUST instead redirect users to a temporary status page. | Let users know why a service is not available, and when to expect it being restored. | Sighted:  When the service is intentionally made unavailable a replacement status page is shown in its place.  The sighted status page lists the reasons Why the service is not available.  The sighted service page states When service is expected to be returned. |  |  | Is the text of status page template based?  Is the template text of the status page editable?  Can changes be deployed without taking down the system? |
|  | QR-DEF-MNT- 00 | | | Default/ Maintainability/ Analysability/ Reportability/ Alerting | Services SHOULD be capable of alerting subscribed stakeholders of atypical/abnormal activity that warrants investigation. | Abnormal/atypical activity should be flagged for review by the appropriate user. |  | Services analyses activity for atypical activity and can alert subscribed stakeholders.  Performance issues  Security issues  Abnormal Behaviour issues  Errors  3rd party solutions may be used (eg: WAF). |  |  |
|  | QR-DEF-MNT- 00 | | | Default/ Maintainability/ Analysability/ Reportability/Queryable **Reports** | Services MUST be capable of developing user refined queryable paged & filtered Reports on Diagnostics, Errors, Sessions, Operations, Users, Groups, Role Allocations, Permission Allocation, User submitted Resources, User submitted Resource Usage, System Resource usage (CPU) and System Responses.  3rd party analysis and reporting services may use a duplicate read-only reporting database. | Decisions as to how to spend resources are aided by reports demonstrating current conditions.  Decisions are often done by governance boards whose members do not access the system, or its views (refer to a requirement defined elsewhere in this catalogue, defining that reports must be printable). |  |  |  |  |

### Modifiability

ISO-25010 definition: the degree to which a solution can be effectively and efficiently modified without introducing defects or degrading operational quality.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | | | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | |  | QR-DEF-SEC-AUTH-00 | | Default/ Security/ Authenticity/ System | Services MUST be configurable to be hosted and discoverable under a custom domain name. |  | The default approach is to host a service as a subdomain of an organisation’s domain (e.g.: [https://*ourservice.ourorg.tld*](https://ourservice.ourorg.tld)). |  | While DNS names, certificate development, and routing are external to the service, the service’s behaviour must not conflict with these exterior configurations. |  |
|  | | QR-DEF-MAIN-MOD-00 | Default/ Maintainability/Modifiability/IdP Service | | The service MUST be configured to use a preferred 3rd party standards based IdP (AAD, B2C, etc.) |  |  | Can the service be integrated with AAD for internal users?  Can the service be integrated with an OIDC compliant IdP or broker to authenticate external users? |  |  |
|  | | QR-DEF-MNT- 00 | Default/ Maintainability/ Modifiability/ MTA | | The system MUST be capable of being configured to use an external specific email service (MTA) AND specify who is sending the email (e.g., “noresponse”). | Systems must have the capability of notifying users who inclusive of users who not currently using the system. |  | Does the system send email?  Is it configurable?  The MTA is expected to be an organisation managed one.  It will be expected to be DMARC compliant.  It will be expected to be sent from a *noresponse* account within a sub domain under the service’s domain name.  E.g.: *“mail.ourservice.ourorganisation.tld”* |  |  |

### Testability

ISO-25010 definition: the degree to which test criteria can be established, and determination of whether the solution meets them.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR-DEF-MAIN-TEST-00 | Default/ Maintainability/Testability/ Test Environments | The Service MUST be dynamically testable in a series of non-production data environment. | The service must be testable before being released, without putting production data at risk.  Environments can be expensive so should be able to be removed when not needed. | One or more environments.  The environments must not be provisioned with production data – only data specific to testing needs.  The environments must be regularly destroyed & rebuilt.  Depending on the environments are managed by different domain services (e.g., AAD).  The environments must be discoverable using predicable DNS names, following organisation naming patterns. | The use of Production Data in a non-disclosed manner is illegal, putting the organisation at risk of both reputational and financial damage. |  | Domains to look for temporary development include:  Non Prod Data Env: - Build Test (BT) - Dev Test (DT) - System Test (ST) - User [SMS] Test (UT) --------------------------Non Prod, but External  User Accessible: - Training (TR) - API/Integration Test (IT) --------------------------Prod Data Env: - Pre Prod (PP) - PROD (PR) |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Testability/ Test Data | The Service MUST be tested using Non-Production Data created for testing purposes. | The use of data to prepare testing material is illegal unless explicitly included in the service’s Data Use Disclosure statement.  Testing a service, including its security, must not require compromising the security of the services’ data. |  | This includes extracting any portion of production data -- even if sophisticated anonymisation or obfuscation technique is employed.  A recommended approach is to develop Personas to represent Users, and develop data suitable to test both desired and non-desired use cases.  As for the number of records, it is recommended to use a minimum of 42 in most tables, so that developing List views – and paging is configured for 20 entries per page – the data is sufficient to demonstrate the presentation of both complete and incomplete pages. |  |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Documentation/SelfHelp | Maintained current Documentation for users to self help themselves MUST be made available to Users from the first deployment. |  |  |  |  |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Documentation/Support | Maintained current Documentation to support the service MUST be made available to operations specialists from the first deployment. |  |  |  |  |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Documentation/Operation | Maintained current Documentation to operate the service MUST be made available to maintenance specialists from the first deployment. | Undesired: Documentation is not available from the start.  Documentation is not maintained current over the service’s lifespan. |  |  |  |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Documentation/Maintenance | Documentation to maintain the service MUST be maintained current before deployment. |  |  |  |  |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Documentation/Location | Documentation (Support, Operate, Maintain, Monitor, Deployment) MUST be made available in an ‘Organisation Managed’ digital repository. |  |  |  |  |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Analysability/ Error Logging | Exceptions MUST be permanently logged to an appropriate data store and make the information accessible to a system administrator role. | Ensure adequate exception logging to support discovery and diagnosis of errors by appropriate support persons.  A unique Identifier of the error must be presented to the user to ease discussions with Support Services. |  | Preferably the solution permits Configuration of a default setting, logging asynchronously (fire/forget) to a remote API endpoint, potentially an agreed SIEM service. |  |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Analysability/ Auditing | The system MUST capture the appropriate level of audit information for all transactions that read, create, update or delete data.  Technical and business users reading audit trail data can determine, for all transactions that read, created, updated or deleted. | Technical and business users should be able to determine:  What was viewed or changed  By whom  When |  | Services auditing logs are protected from tampering, by using data store service within an ISO-27001 compliant data warehouse that logs access to physical resources and access to virtual hard drives is limited and audited to prevent tampering  Note:  Signage of the audit log entries is not implemented in this system. |  |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Analysability/ Capabilities | Services services and service client interfaces MUST support filtering and sorting capabilities using a case insensitive, accept sensitive, culture. | Any user interface must assist users in finding appropriate information in a manner that produces the highest chance of finding the correct information, no matter the culture. |  | Services service client interfaces provide a means to search across items, whether AutoComplete is offered, present Summaries of matching records, whether they can be sorted by one or more fields, can be used effectively on both mobile and desktop interfaces (i.e., avoid using table layout strategies better suited to desktop interfaces than mobile devices, etc.)  Note:  Consider matching or improving on Latin\_1\_General\_CI\_AS |  |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Analysability/ Search Tools | Services MUST include capabilities of filtering, searching case-insensitively, accent-insensitively, sorted paged diagnostics, error and audit records. | Support specialists must have the tools to find records to diagnose user and system activity. |  | Services makes system records searchable in an efficient manner, using filtering criteria & response paging. |  |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Reportability/ Monitoring | Services MUST include a means of monitoring key metrics. | Metrics are required to be collected in order to compare abnormal behaviour against. |  | Services monitors:  Performance issues  Security issues  Abnormal Behaviour issues  Errors |  |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Capacity/Diagnostics trace message storage | Services MUST keep diagnostics trace messages for a configurable duration of time. | Diagnostics trace messages can be voluminous. Being not required for operations, auditing or archiving purposes, they can be purged as needed to keep storage requirements within reason. |  | Services diagnostics trace messages are kept for a configurable duration (by default 31 days).  Services PROD environment’s diagnostic trace messages are conserved even if the environment is destroyed and rebuilt (e.g., using Infrastructure as Code invoked by an automated deployment).  Services diagnostics messages are copied to a target area available to an organisation’s SIEM system to import. |  |  |
|  | QR-DEF- MNT- 00 | Default/ Maintainability/ Analysability/ Metric Collection | Services MUST collect and make available key metrics for reports. | Collecting metrics provides information required to direct effort towards continual improvement of the service rendered. |  | Average & Max Duration of Transactions  Average & Max Volume of Transactions  Average & Max Transactions per Session  Transactions to Dynamically allocated Hosts  Average & Max Number of Sessions per User  Average & Max Number of Resources accessed per Session  Include collecting metrics for developing the following ascending/descending lists:  Resources collaborated on per User  Feedback per User  Resources Flagged  Users Flagged  User's Resources Flagged  Storage used per User  Storage used per Group |  |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Testability/ Automated | Services MUST perform all testing of configuration or customisation by automation. | Resources, whether permanent resources or contractors, leave with their knowledge of systems.  Documentation of evolving systems are hard to keep current.  The only effective way to ensure quality assurance knowledge lasts the length of the service lifespan, and is rapid enough to not delay deployments of environments, functionality and data is to automate all testing. |  | Services capabilities, functionality and qualities are tested by automation initiated by the delivery pipeline.  Services automated pipeline tests the following:  external system (database, identity provider, caching, malware detection, etc.) integration testing,  API service facade authorisation, access and functionality integration testing  automated smoke testing,  automated quick, high-level functionality testing,  automated longer, in-depth, functionality testing. |  |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Modularity/ Reference based | Services customisation SHOULD align with and leverage organisation standards and patterns.  Deviations must be recorded as Project Decisions. | The risk of delivery failure is reduced by:  reusing where possible  aligning with Ministry and AoG design and data principles and standards  proven reference architectures for custom development  development standards  use of available environment services (reusing enterprise systems, including IdPs, as malware validation, smtp services, etc.)  data management standards  deployment standards, practices and guidelines |  | The system's database schema is specific to this application.  The system deploys data to data warehouses via API (not SQL).  The schema of the DTOs used meets data management standards.  Uses deployment standards, practices and guidelines. |  |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/Modifiability/ Configurable Features | Custom Code based solutions MUST and others SHOULD be configurable to enable and disable different functionality depending on user group. | Certain features are required to be released in stages, starting with only a subset of users. |  | Certain features are required to be released in stages, starting with only a subset of users.  Services allows the dynamic disabling of features that are in the code base, but not ready for use by end users.  Services allows for the dynamic association of features to certain groups of users, for A-B feature testing. |  |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/Modifiability/ Loosely coupled | Custom Code based solutions MUST and others SHOULD be developed using loosely coupled systems and components. | Services SHOULD allow modification to one component or group of functionality with the least chance of affecting other parts of the solution. |  | Services is developed as a loosely coupled set of systems, components, logical domains.  Consider describing the use of external 3rd party subscriptions services for Identity services, PII storage services, confidential storage services, structured and unstructured storage services, caching, malware detection, content validation, etc.  Consider describing using DDD for system component development.  Consider describing using SOLID development patterns. |  |  |
|  |  | Default/ Maintainability/ Modifiability/ API Versioning | Externally accessible APIs and associated DTOs MUST be versioned. | Maintainability requires that changes to DTOs does not cause force breaking contracts with established integrated systems. |  |  |  |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/Modifiability/ Web Standards | ‘Custom Code’ MUST be developed and maintained to current & maintained Web Standards. | Services is more maintainable and secure when the standards used are mainstream and current. |  | The Solution’s Service Client Interface is developed using current web standards.  HTML5+  CSS Levels 4+  All W3C Modules  Document Object Model level 3+  ECMA Script 5.1+  Services service client does not rely on platform or browser extensions (eg:  ActiveX Adobe Flash, Flex or AIR Microsoft Silverlight, Microsoft ClickOnce, SmartClients, Java or JavaFX, Embacadero DataSnap, etc.) |  |  |
|  | QR-CUS-MNT- 00 | Default/ Maintainability/ Analysability/ Status Reporting | Custom Code solutions MUST be able to develop both web interface and printable reports of the status of key aspects of the system. | Senior stakeholders are not always users of the system yet require reports on which to base decisions. |  | Services has web view interfaces and associated printed reports to describe key aspects of at least the following key elements of the solution:  User Concerns:  Users (# of users, # of new and leaving users, etc.)  Groups (# of groups, # of new and closing groups, etc.)  Resource Concerns:  Resources (# of resources, # of new, retired resources, etc.)  Resource Collections (# of groups, activity metrics, etc.)  Support Concerns:  User Feedback (#ratings, # comments, etc.)  Support Tickets (#open, #closed, etc.)  Security Concerns  Security Events: (# of reviewable events, reviewed events, issues, etc.)  Operations Concerns:  Unexpected behaviour (# of errors, # of resolutions, # of reviewed and discounted events, etc.)  Infrastructure Concerns:  Environments (# of environments)  Services  Costs (per month, new, closed)  Development Concerns:  Issues, Bugs (# of open/closed issues, # of open/closed requests, # of open/closed bugs, etc.)  Work Item velocity |  |  |

## Portability

*ISO-25010 Definition:* *the degree of effectiveness and efficiency with which a system, product or component can be transferred from one hardware, software or other operational or usage environment to another. This characteristic is composed of the sub-qualities listed below.*

### Adaptability

ISO-25010 definition: the degree to which a solution can effectively and efficiently be adapted for different and evolving hardware, software, or environments.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR- DEF- POR- ADAP- 00 | Default/ Portability/ Adaptability/ Settings/ API | | Services mutable system settings MUST be configurable by API. | Whether Rented, Bought or Built,  Deployment specialists must be able to configure deployed system components via APIs invoked by automation  pipelines.  Automation protects against loss of IP at the end of the delivery phase -- when resources leave -- while also reducing deployment documentation requirements. | APIs exist to configure the following mutable settings:  - System Branding - System Settings - Reference Data - System Roles - Users - Groups - Group Roles - Role allocation | System settings are set by an automation pipeline step after any compilation, testing and deployment steps, but prior to dynamic reference data provisioning and testing steps.  Mutable Settings are persisted in the services datastores (as opposed to immutable Configurations that are can only be changed by redeployment). |  | Is the system’s settings configurable?  By API or GUI only?  What are the key areas that can be configured [by API][by automation]: - System Branding - System Settings - Reference Data - System Roles - Groups - Group Roles - Role allocation |
|  | QR- DEF- POR- ADAP-00 | Default/ Portability/ Adaptability/ Configurability/ GUI | | Services mutable system settings MUST also be configurable by GUI. | Operations specialists may be required to change a system setting before the next scheduled release (which will re-apply the setting via API). | Interfaces exist for configuring:  - System Branding - System Settings - Reference Data - System Roles - Users - Groups - Group Roles - Role allocation - Workflow steps | Mutable Configurations include:  - Appearance - Branding - Reference Data - System Roles - User Grouping - Group Roles - Workflow steps |  | Is the system configurable by GUI? |

### Installability

ISO-25010 definition: the degree of effectiveness and efficiency in which a solution can be successfully installed/uninstalled in a specified environment.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  |  |  | |  |  |  |  |  |  |
|  | QR-DEF-POR- INST- 03 | Default/ Portability/ Installability/ Automated Environment Creation & Deployment | | Services MUST be able to deploy settings and provision new environments solely by automation. | Upon a disaster, a solution must be able to be rebuilt quickly from scratch using:  Infrastructure as Code,  Data base schema as Code,  Automated Backed up data.  Automated Data Restoration.  Automated Migration of Data to other systems (either drop/pickup areas, or APIs of external Data warehouse, SIEMs, etc.) |  | If the system is custom developed, the automation pipeline would involve compilation, static testing, packaging deploying, configuring and integrating.  the solution uses an automated pipeline to recreate environments from scratch and deploys logic and data to them.  the solution can be deployed purely by automation to a new environment of any choice (including BT, DT, ST, UT, PP, IT, PROD, etc.).  the solution’s credentials are persisted external systems for safe management.  the solution is deployed to non-PROD environments, such as DevTest (DT), System Test (ST), User Test (UT), Integration (INT) for external clients to test their API integration.  Note: Refer to the Delivery View for proposed environments. |  |  |
|  | QR-DEF-POR- 00 | Default/ Portability/ Installability/ Automated Integration Deployment | | Services testing processes COULD include deploying agreed 3rd party API clients. | In order to verify that API changes do not break remote key Service Clients, consider validating the changes by connecting to the API as intended. |  | NRN: Unit-testing and integration testing are performing the same functionality. This requirement is not required. |  |  |
|  | QR-DEF-POR- 00 | Default/ Portability/ Installability/ CustomCode/CrossOS | | ‘Custom Code’ MUST be operating system agnostic. | While installation automation scripting may be obligated to be OS dependent, any custom code used to develop extensions to a platform service must be as portable to different operating systems as the service itself. | *Note:* ‘Custom Code’ *is defined in this document’s appendices.* | ‘Custom Code’ should be developed using cross-OS platform & frameworks (.NET Core, Python, etc.) preferably deployable to managed platforms (e.g.: PaaS) that remove the need to know the underlying OS. |  |  |

### Replaceability

ISO-25010 definition: the degree to which a solution can replace another system for the same purpose in the same environment.

Note:  
this category is difficult to complete in a default manner, without knowing the specific purpose of the service.   
However, a number of general catch-all requirements are provided below.  
  
Note also that this this Category is not the same but complementary to Compatibility/Interoperability which covers the system’s integration requirements, including those needed for end of service business continuity reasons.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR-DEF-POR-REP- 00 | Default/ Portability/ Replaceability/ Integrations | IF the solution’s service(s) is/are replacing an existing service, it MUST be able to integrate with the existing service’s required integrated services. | If delivery is dependent on changes to the integration approach, it becomes dependent on other services being able to be changed, which they may not be. | Services can be integrated using the same channels, same protocols. | Note: being able to integrate using current approaches does not preclude the integration actually being done a new way if more secure, more maintainable, or more performant.  Integrations to check for include but are not limited to: - Directory Services (AAD) - Systems of record - Notifications (email) - Reporting - BI & Analysis - Data warehouse |  |  |
|  | QR-DEF-POR-REP- 00 | Default/ Portability/ Replaceability/ Functionality | IF the solution’s service(s) is/are replacing an existing services, it MUST be able to automate the delivery of the same business outcomes as the service it is replacing. | Avoid the risk of this project becoming dependent on other services being modified to continue to work after this new service is implemented.  Avoid replacing like-for-like by focusing too much on the same functions, rather than outcomes. | Compare the business outcomes deliverable by the service being replaced and its replacement. | Consider comparing at capabilities for managing: - Users - System Roles - Groups - User Group Roles – Resources - Media |  |  |

## Regulatory

ISO-25010 does not include a Regulatory section, which would be an appropriate section to outline legal obligations, including Accessibility, Privacy, Data, Record Keeping and Disclosure.

### General

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | # | | ID | | Statement | | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR-DEF-REG-PRV- 00 | | Default/ Regulation/ Privacy/ Regulation | | Services MUST adhere to the applicable regulations of the country(s) in which it is intended to be available from. | | Offering services that do not comply is illegal, putting the organisation’s reputation at risk, as well at risk of incurring costly fines. | | Services is assessed as being compliant with the applicable regulations of target countries, including: - System Accessibility - System Usability - System Security - Data  Classification - Data Use  - Data Retention - Personal Info  - Privacy - Finance - Official  Information  Requests  Is there an Accessibility report showing existing compliance? | Regulations exist to ensure Users  - can still use a system if they are visually impaired  - Not be tracked across systems - Are disclosed why their data is being collected - What it will be used for (note that it never includes ‘Be used for Testing Purposes’). - Who it will be shared with - how long it will be kept for - how to or who to contact to correct personal information - can opt out of using the system |  | Does the service meet Usability Standards?  Does the service meet Accessibility standards?  Does the system disclose Tracking/Cookie information and make it customisable?  Does the system disclose data collected, purpose, who it is shared with, how long it is made available before being removed from access?  Does the system disclose how to update PI information? |

### Privacy

All countries this service will be available from have laws -- including ones specific to Privacy Personal and Financial Information -- to comply with.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | # | | ID | | Statement | | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR-DEF-REG-PRV-00 | | Default/ Regulation/ Privacy/ Tracking | | Services MUST permit users to opt out of being tracked for any purpose other than for the correct behaviour of a service. | |  | | Sighting: Either only essential cookies are round tripped between server and client, or the user is shown a dialogue to opt-in to tracking. | Strictly necessary cookies are Same-Site cookies, that include: Session Cookies, Common categories of tracking cookies include: - Performance - Functionality - Preference - Third party Targeting  Note that if the cookies are purely for SameSite functional purposes on this site only, no confirmation is required by end users. |  | Are cookies that are not strictly necessary to the site’s use being sent?  If so, do end users have the means of selecting which cookies they accept? |
|  | QR-DEF-REG-PRV- 00 | | Default/ Regulation/ Privacy/ PI/ Minimum | | Services MUST collect the minimum amount of PII to meet its functionality expectations. | | The more PII information maintained in a system, the more tempting it is, and the more damage can occur from it being accidentally or intentionally leaked. | |  |  |  | Services actively avoids requesting non-essential PII information.  Services imports the user’s Given Name (for notifications), Display Name (for rendering views), and identity email credential (for notifications).  The Given and Display Name can be updated by the end user.  The PII is persisted in a secure data store that is separate from the production data. |
|  | QR-DEF-REG-PRV- 00 | | Default/ Regulation/ Privacy/ Correction | | Services MUST allow users to self-correct their own information. | | Aside from the legal obligations in some countries (e.g., NZ),  Users know themselves best, so this improves Data Quality. | | This implies the system provides user accessible GUIs for this, with changes submitted for review.  Alternatively, it implies providing a contact point (e.g., an email address) for requesting changes.  Services allows users to change or request changes to the PII information imported from an external PII service. |  |  | Can Users change information about themselves?  Can the system provide a means to review and reject or accept changes?  Can the solution provide an email address to write to request these changes? |

### Sovereignty

Most countries this service will be available from have or are developing data sovereignty regulations requiring adherence to.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | # | | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  | QR-DEF-REG-SOV- 01 | | Default/ Regulation/ Sovereignty/ Data Storage Location | | Services MUST persist data in the country closest to consumption – preferably the country itself. | Asides from Performance advantages, certain countries (e.g., NZ, Europe) already have or are developing and will have Data Sovereignty regulations that will exist during the system’s lifespan. | The data can be persisted in a specified country.  Backups of the data can be done in a specified country. |  |  | Is the data persisted in only one country (e.g. the USA)? |

Appendices

Appendix A - Document Information

### Images

[Figure 8: Default System Base Tier of Quality Requirements 19](#_Toc156204546)

### Tables

### References

*ICT Project Guidance – Requirement Development*

*Project Guidance – Definition – Custom Developed Solution Quality Requirements*

**There are no sources in the current document.**

### Review Distribution

The document was distributed for review as below:

|  |  |
| --- | --- |
| Identity | Notes |
| Russell Campbell, Project Manager |  |
| Sandy Britain, Enterprise Architect |  |
|  |  |

### Audience

The document is technical in nature, but parts are expected to be read and/or validated by a non-technical audience.

### Structure

Where possible, the document structure is guided by either ISO-\* standards or best practice.

### Diagrams

Diagrams are developed for a wide audience. Unless specifically for a technical audience, where the use of industry standard diagram types (ArchiMate, UML, C4), is appropriate, diagrams are developed as simple “box & line” monochrome diagrams.

### Terms

Refer to the project’s Glossary.

##### ‘Custom Code’

: all information required to develop, deploy, configure, integrate, provision any aspect of the service, excluding proprietary information such as Software as a Service (SaaS).

##### Custom Deliverables

: Code & Documentation.

Prod Data Environments: environments that contain production data that includes confidential information.

##### IT

: acronym for Information, using Technology to automate and facilitate its management.

##### ICT

: acronym for Information & Communication Technology, the domain of defining Information elements and using technology to automate their communication between entities. IT is a subset of ICT.

Non-Prod Data Environment: *all* other environments (BT, DT, ST, UT, PP, TR, etc.) than the Prod environment.

##### Organisation Provided

: if the organisation that is procuring the service has a service, then it must be used, unless mutually decided otherwise. If the organisation does not have the service, governance can mutually agree to use an alternate service until the organisation provides one to which it can be moved.

##### Proprietary Code

: code that indirectly or directly belongs to and is controlled by a vendor distinct from the organisation purchasing the development of the solution (the Ministry). Does not include code used to develop a SaaS.

##### SaaS

: *Software as a Service*, a managed service rented via a subscription account.

Appendices B – ISO-25010 Qualities

ISO-25010 defines Headers and sub headers, each with their individual descriptions.

These are as listed below.

### Delivery

While *Installability* is a quality defined under *ISO-25010/Portability* (see further down), the subject of Delivery wider, and called out first, with its own section.

### Security

Security is defined in ISO-25010 as the practice of maintaining the confidentiality, privacy, integrity and accountability of data changes by controlling authorised access, use and disclosure, while preventing unauthorised use, disruption, modification or destruction.

ISO-25010 recommends considering the following qualities and their descriptions when considering a solution:

#### Confidentiality

: the degree to which the solution ensures data is accessible only by those authorised to do so.

#### Integrity

: the degree to which the solution prevents unauthorised access, modification of systems and the information they manage.

#### Non-Repudiation (of Action) and Accountability (by Whom)

: are associated in that non-repudiation defines the degree to which the solution can prove that actions have been taken, and accountability is being able to associate the non-repudiable (audited) activity to a specific user.

#### Authenticity

: defines the degree to which the identity of a user can be claimed.

#### Availability

: a prerequisite for Security but is treated separately, under Reliability.

Note:  
Security and Privacy risk assessments, and matching Statement of Applicability listing required controls for the solution will be conducted during the solution’s design phase.  That process will further augment the security requirements listed below.

### Privacy

Privacy is not a defined ISO-25010 concern, but since the last edition, has become a first-class quality.

### Functionality

#### Functional Completeness

: …

#### Functional Correctness

: …

#### Functional Appropriateness

: …

### Performance

Efficiency, throughput, capacity, response time and resource consumption for Online Transaction Processing (OLTP) and background processes.

The system's ability to complete defined volumes of computer assisted Business Transactions (online and background operations) within acceptable times and with an acceptable consumption of resource.

ISO-25010 recommends considering the following qualities and their descriptions when considering a solution:

#### Time behaviour

: is the degree to which the response and processing times and throughput rates of a solution, when performing its functions, meets requirements.

#### Resource Utilisation

: is the degree to which the amounts and types of resources used by a product or system, when performing its functions, meets requirements.

#### Capacity

: is the degree to which the maximum limits of the solution meet or exceed requirements.

### Compatibility

#### Co-existence

: …

#### Interoperability

: …

### Usability

Usability is how easy and efficient it is for an end user to use the solution correctly, accurately, and safely.

It also ensures constancy with other organisation applications.

It is sometimes called system ergonomics, accessibility and ease of use.

ISO-25010 recommends considering the following qualities and their descriptions when considering a solution:

#### Appropriateness recognisability

: is the degree to which users can recognize whether a solution is appropriate for their needs.

#### Learnability

: is the degree to which a solution enables the user to learn how to use it with effectiveness, efficiency and in the case of an emergency.

#### Operability

is the degree to which a product is easy to operate, control and appropriate to use.

#### User Error Protection

: is the degree to which a solution protects users against making errors.

#### User Interface Aesthetics

: is the degree to which a user interface enables pleasing and satisfying interaction for the user.

#### Accessibility

: is the degree to which a solution can be used by people with the widest range of characteristics and capabilities to achieve a specific goal in a specified context of use.

### Reliability

Reliability of a solution is - a request being processed by that system according to agreed business logic and a valid response being returned by the system in the time expected. The time expected is influenced and constrained by the performance requirements of the system.

Fault tolerance is defined as the immunity of the system in the event of an unexpected internal or external fault. This is evaluated in the context of the likelihood of the fault, the severity of the fault and resulting impact on end users.

*Recoverability* is a subset of *Reliability* andis the ability to re-establish the normal functioning of a system after a significant external event, such as a disaster. A disaster implies total loss of access or use of the system by end users (e.g., production) where the outage has, or will, extend beyond the Maximum Tolerable Downtime (MTD).

The MTD and ‘normal functionality’ are agreed between IT (or the vendor) and the business owner of the system in the Service Level Agreement (SLA).

*Recoverability* uses activities such as data protection, Disaster Recovery (DR), and Business Continuity Planning (BCP) to ensure the recoverability of systems

ISO-25010 recommends considering the following qualities and their descriptions when considering a solution:

#### Maturity

: is the degree to which a solution needs for reliability, under normal operation.

#### Availability

: is the degree to which a solution is operational and accessible when required for use.

#### Fault tolerance

: is the degree to which a solution operates as intended despite the presence of hardware, software or user faults.

#### Recoverability

: is the degree to which, in the event of an interruption or failure, a solution can recover the data directly affected and re-establish the desired system state.

### Maintainability

Maintainability is the ability to maintain the system efficiently: find and remove faults, improve performance, carry out modifications and infrastructure upgrades. It is also known as modify-ability, enhancement, fault detection, isolation and repair.

Traceability is the ability to retain details of specified business, transactional, and system activity and data changes, including normal, abnormal, and error conditions with selective control. It is also called auditability and audit trail.

ISO-25010 recommends considering the following qualities and their descriptions when considering a solution:

#### Modularity

: is the degree to which a solution is composed of discrete components such that a change to one has minimal impact on others.

#### Reusability

: is the degree to which an asset can be used in more than one system or reused to build other assets.

#### Analysability

: is the degree of effectiveness and efficiency with which it is possible to assess the impact of a solution, a change, a failure, or determine what requires change.

#### Modifiability

: is the degree to which a solution can be effectively and efficiently modified without introducing defects or degrading operational quality.

#### Testability

: is the degree to which test criteria can be established, and determination of whether the solution meets them.

### Portability

ISO-25010 recommends considering the following qualities and their descriptions when considering a solution:

#### Adaptability

: is the degree to which a solution can effectively and efficiently be adapted for different and evolving hardware, software, or environments.

#### Installability

: is the degree of effectiveness and efficiency in which a solution can be successfully installed/uninstalled in a specified environment.

#### Replaceability

: is the degree to which a solution can replace another system for the same purpose in the same environment.