DRAFT - ICT Project Guidance

System Default 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](#_Toc149732228)

[Synopsis 1](#_Toc149732229)

[Contents 2](#_Toc149732230)

[Introduction 6](#_Toc149732231)

[Purpose 6](#_Toc149732232)

[Context 6](#_Toc149732233)

[Structure 6](#_Toc149732234)

[Tiers 6](#_Toc149732235)

[Grouping By Qualities 7](#_Toc149732236)

[Qualities 7](#_Toc149732237)

[Content 8](#_Toc149732238)

[Prioritisation 8](#_Toc149732239)

[Exemptions 8](#_Toc149732240)

[Acceptance Criteria 8](#_Toc149732241)

[Quantitative Settings 9](#_Toc149732242)

[Quality Requirements 10](#_Toc149732243)

[ISO Defined Qualities 10](#_Toc149732244)

[Terminology Used 10](#_Toc149732245)

[Prioritisation 10](#_Toc149732246)

[Headings 10](#_Toc149732247)

[Project Specific System Qualities 11](#_Toc149732248)

[Scope 11](#_Toc149732249)

[Custom Developed Solution Qualities 13](#_Toc149732250)

[Scope 13](#_Toc149732251)

[Security 14](#_Toc149732252)

[Functionality 23](#_Toc149732253)

[Reliability 26](#_Toc149732254)

[Usability 32](#_Toc149732255)

[Performance 35](#_Toc149732256)

[Maintainability 36](#_Toc149732257)

[Portability 39](#_Toc149732258)

[Installed Solution Qualities 41](#_Toc149732259)

[Scope 41](#_Toc149732260)

[Security 42](#_Toc149732261)

[Reliability 45](#_Toc149732262)

[Maintainability 46](#_Toc149732263)

[Ministry Specific System Qualities 47](#_Toc149732264)

[Scope 47](#_Toc149732265)

[Processes 48](#_Toc149732266)

[Security 49](#_Toc149732267)

[Compatibility 51](#_Toc149732268)

[Usability 52](#_Toc149732269)

[NZ Education Sector System Qualities 54](#_Toc149732270)

[Scope 54](#_Toc149732271)

[Processes 55](#_Toc149732272)

[Security 56](#_Toc149732273)

[Compatibility 56](#_Toc149732274)

[Maintainability 56](#_Toc149732275)

[NZ Government Sector System Qualities 58](#_Toc149732276)

[Scope 58](#_Toc149732277)

[Processes 59](#_Toc149732278)

[Security 59](#_Toc149732279)

[Functionality 65](#_Toc149732280)

[Compatibility 66](#_Toc149732281)

[Usability 66](#_Toc149732282)

[Maintainability 67](#_Toc149732283)

[Portability 68](#_Toc149732284)

[NZ specific Default System Qualities 69](#_Toc149732285)

[Scope 69](#_Toc149732286)

[Privacy 70](#_Toc149732287)

[Default System Qualities 71](#_Toc149732288)

[Scope 71](#_Toc149732289)

[Security 72](#_Toc149732290)

[General 72](#_Toc149732291)

[Confidentiality 75](#_Toc149732292)

[Privacy 85](#_Toc149732293)

[General 85](#_Toc149732294)

[Functionality 87](#_Toc149732295)

[Completeness 87](#_Toc149732296)

[Compatibility 89](#_Toc149732297)

[Interoperability 90](#_Toc149732298)

[Usability 93](#_Toc149732299)

[Operability 93](#_Toc149732300)

[User Protection Error 96](#_Toc149732301)

[User Interface Aesthetics 96](#_Toc149732302)

[Accessibility 96](#_Toc149732303)

[TODO 98](#_Toc149732304)

[Reliability 109](#_Toc149732305)

[Performance 118](#_Toc149732306)

[Maintainability 124](#_Toc149732307)

[Portability 138](#_Toc149732308)

[Default Internal Requirements 144](#_Toc149732309)

[Conclusion 146](#_Toc149732310)

[Appendices 147](#_Toc149732311)

[Appendix A - Document Information 147](#_Toc149732312)

[Images 147](#_Toc149732313)

[Tables 147](#_Toc149732314)

[References 147](#_Toc149732315)

[Review Distribution 147](#_Toc149732316)

[Audience 148](#_Toc149732317)

[Structure 148](#_Toc149732318)

[Diagrams 148](#_Toc149732319)

[Terms 148](#_Toc149732320)

[Appendices B – ISO-25010 Qualities 149](#_Toc149732321)

[Delivery 149](#_Toc149732322)

[Security 149](#_Toc149732323)

[Confidentiality 149](#_Toc149732324)

[Integrity 149](#_Toc149732325)

[Non-Repudiation (of Action) and Accountability (by Whom) 149](#_Toc149732326)

[Authenticity 149](#_Toc149732327)

[Availability 149](#_Toc149732328)

[Privacy 150](#_Toc149732329)

[Functionality 150](#_Toc149732330)

[Functional Completeness 150](#_Toc149732331)

[Functional Correctness 150](#_Toc149732332)

[Functional Appropriateness 150](#_Toc149732333)

[Performance 150](#_Toc149732334)

[Time behaviour 150](#_Toc149732335)

[Resource Utilisation 150](#_Toc149732336)

[Capacity 150](#_Toc149732337)

[Compatibility 150](#_Toc149732338)

[Co-existence 150](#_Toc149732339)

[Interoperability 150](#_Toc149732340)

[Usability 150](#_Toc149732341)

[Appropriateness recognisability 151](#_Toc149732342)

[Learnability 151](#_Toc149732343)

[Operability 151](#_Toc149732344)

[User Error Protection 151](#_Toc149732345)

[User Interface Aesthetics 151](#_Toc149732346)

[Accessibility 151](#_Toc149732347)

[Reliability 151](#_Toc149732348)

[Maturity 152](#_Toc149732349)

[Availability 152](#_Toc149732350)

[Fault tolerance 152](#_Toc149732351)

[Recoverability 152](#_Toc149732352)

[Maintainability 152](#_Toc149732353)

[Modularity 152](#_Toc149732354)

[Reusability 152](#_Toc149732355)

[Analysability 152](#_Toc149732356)

[Modifiability 152](#_Toc149732357)

[Testability 152](#_Toc149732358)

[Portability 152](#_Toc149732359)

[Adaptability 152](#_Toc149732360)

[Installability 152](#_Toc149732361)

[Replaceability 152](#_Toc149732362)

## Introduction

BOSSCARD/ RAID: Background [], Objective, Options, Scope[In/Out], Stakeholders [Users], Constraints, Assumptions, Risks, Dependencies, Decisions, Deliverables.

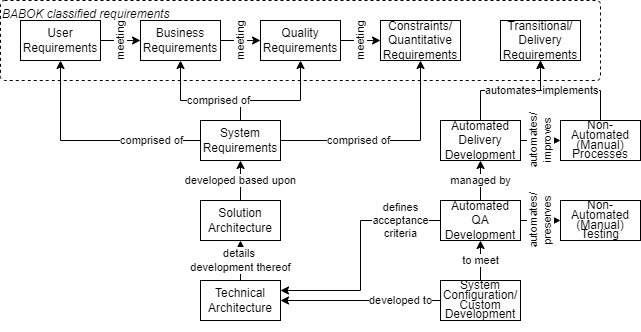
## Purpose

This document summarises the project’s key Qualitative Quality Requirements.

## Context

This set of requirements fits within the Business Analysis Body of Knowledge (BABOK) requirements classification system (Business, User, Functional, Quality, Constraints and Transition requirements.

The totality of the Functional Requirements, Quality Requirements and Quantitative Requirements are referred to as the “System’s Requirements”, the basis of the Solution Architecture Description document.



## Organisation

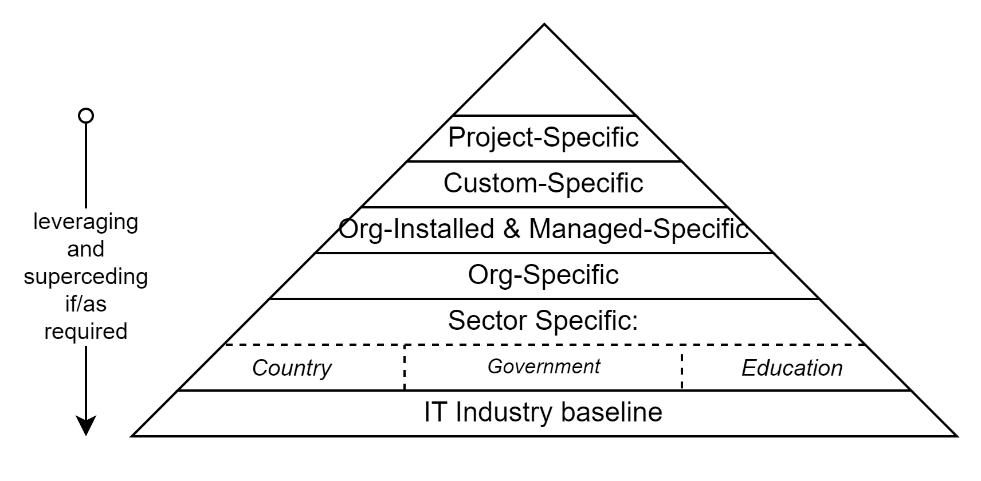
To minimise miscomprehensions as to expectations, the document’s requirements are organised and presented in a specific order, as described below.

### Tiers

Requirements are organised according to layered Scopes -- each section expanding or superseding one or more requirements in a more general scope.

The requirements start with the smallest set of requirements, the Project-Specific, that build on top of more general Organisation requirements, which in turn are built upon Sectors-Specific requirements.

At the bottom are Baseline/Default industry standard requirements.



**Scoping as above is purposeful:** the delivery of projects is de-risked by avoiding developing requirements to define novel approaches to previously solved IT solutions, while being mindful of choosing ones that do not negatively impact the delivery of uniquely valuable business service features.

### Qualities

Within each domain tier, requirements are organised according to ISO standards based headers where applicable.



The ISO-\* quality model is the cornerstone of a Service quality evaluation system.

The quality model determines which quality characteristics will be considered when evaluating the properties of a software service.

The quality of a system is the degree to which the system satisfies the stated and implied needs of its various stakeholders, and thus provides value. Those stakeholders' needs (functionality, performance, security, maintainability, etc.) are precisely what is represented in the quality model.

## Requirement Attributes

### ID

Each requirement has a unique ID for unambiguous referencing later, from contracts and work items.

As is customary, the Quality Requirement starts with QR- before expressing succinctly what Tier and Category they belong to: QR-{Tier}-{Quality}-{number}.

### [Diagram] Title

Each requirement is provided a short title. The title is intended to be unique, while being both less opaque than an ID, and short enough that they could be used within diagrams.

Good practice dictates that requirements are SMART (Specific, Measurable, (pragmatically) Achievable, Relevant, Timely), developed in a CLEAR manner (Collaboratively, Limited scope, Evaluated, Appropriate, Resource Conscience) manner. Refer to the Appendices.

### Statement

A Requirement Statement is expected to be succinct, define its prioritisation, and developed by following SMART guidance.

#### Prioritisation

Requirement prioritisation is according to RFC-8174 defined terms. Their implication in the context of procurement is as below:

1. **MUST** - requirements expected to be deliver as defined.   
   If technically *unable* to (e.g.: because the service is a **SaaS**), propose a work-around.
2. **SHOULD** - requirements expected to be deliver as defined, but alternative means to obtaining an equivalent outcome are acceptable.
3. **MAY** - represents requirements that -- time and resources permitting – would be ‘nice to have’ but are not considered essential functionality for the final solution.

### Acceptance Criteria

While correctly developed Statements should define achievable measurable outcomes, the same outcomes are often spelled out as Fit/Acceptance Criteria.

Note:  
Quantitative requirements are Measurable in their own right, therefore do not include accompanying Fit statements.

### Details

Each Requirement includes a Details column to include information that may be useful but should not be part of the Statement.

### Questions and Response

RFx Respondents should review the Requirements Statement, Fit, Details and guiding Questions, to succinctly respond in the Response column as to how their proposed solution meets the intended outcomes.

### Exemptions

Not all solutions can reasonably meet all requirements that are marked as MUSTs.   
For example, proposed solutions may rely on the use of 3rd party SaaS service providers -- whom it is improbable will agree to modifying their service to meet project specific requirements. In such cases, it is up to the presenter to submit a work around that can meet the same obligations and/or objectives.

### Comment

The Comments column is reserved for evaluation purposes, capturing remarks about the Response provided by Respondents.

## Custom Development Quality Requirements

The requirements captured in this document define *what* outcomes are expected, attempting to avoid as much as reasonable defining *how* they expected, so that RFx respondents can respond with a solution that relies on either a custom developed system, a service or product, or a mix thereof.

While solutions that are purchased or subscribed to are not qualified to ensure they are maintainable, modular, and improvable at a code level, custom developed systems are held to a higher standard and are.

Hence -- in addition to the general quality requirements defined in this document -- custom developed systems must meet the obligations listed in the supplemental *Project Guidance – Definition – Custom Developed Solution Quality Requirements*.

# Quantitative Settings

TO FILL IN PER PROJECT – OR DO IT IN A SEPARATE DOCUMENT (I THINK THE SECOND OPTION IS MY PREFERENCE)

# Quality Requirements

The Business Analysts Book of Knowledge (BABOK) defines Quality Requirements as one of the 5 types of categories requiring defining.

## ISO Defined Qualities

ISO-25010 defines a list of system qualities considered valuable.

ISO-25012 defines a list of qualities defined valuable when assessing data within a system.

ISO-25022 defines a list of qualities that users expect to experience when using a system that contains information.

## Terminology Used

Specific terminology is used throughout this document, following guidance given in *ICT Project Guidance – Requirement Development*.

### Prioritisation

As per the Appendices, Requirements are Obligations.

The quality requirements outline the required or preferred capabilities of the solution by priority (Must, Should and Could).

1. **Must** - the respondent must propose a solution that, as a minimum standard, meets the requirements of the core functionality identified as “Must”.
2. **Should** - functional requirements that have been identified as “Should” are highly desirable functionality that should be included, or workarounds may be available for this functionality.
3. **Could** - represents requirements that are ‘a nice to have’ (time and resources permitting), but not considered necessary functionality for the final solution.

### Headings

# Project Specific System Qualities

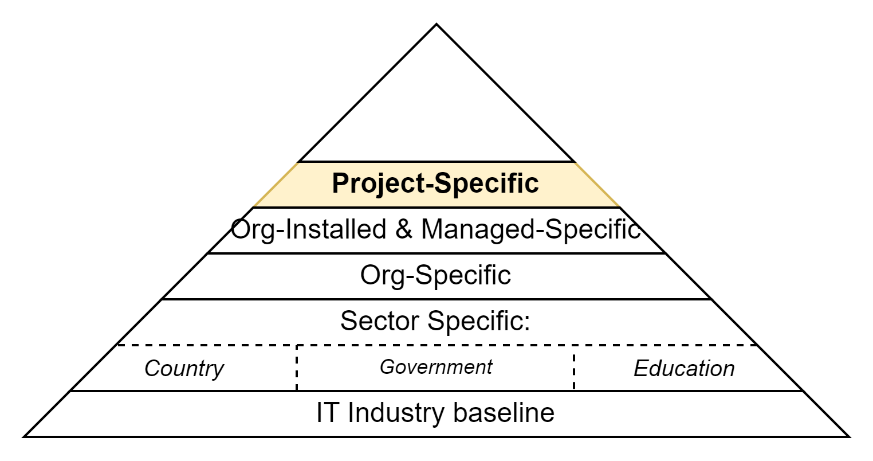


Figure 1: Project Specific Tier of Quality Requirements

The project has no Project specific Quality requirements beyond those defined further down for Education Domain, Government Domain and General systems later in this document.

## Scope

The following are the Requirements categories defined in this Tier:

|  |  |  |
| --- | --- | --- |
| Defined | Undefined (Inherited) | Details |
|  | * Accreditation * Security * Maintainability * Deliverability * Functionality * Usability * Reliability * Performance * Maintainability * Portability | In essence, if the service is capable of being accessible for productive use by the user base while meeting its Quantitative Requirements, and laws and regulations specific to either the Education Sector or Government sector, then requirements that would be common to any system (as per the Default System Qualities defined below), are good enough. |

# Organisation (NZ MOE) Specific (Hosted) System Qualities

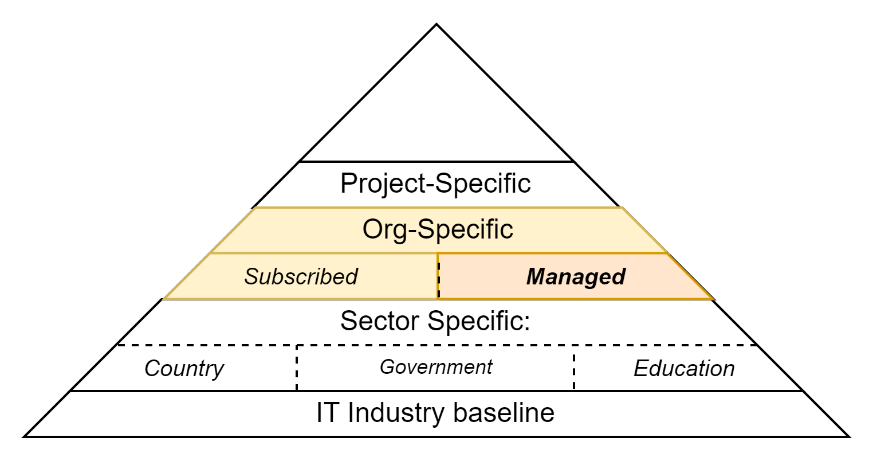


Figure 3: Organisation (NZ MOE) Specific Tier of (Managed) System Quality Requirements

This section lists qualities specific to licensed and procured services that are installed and management by the organisation -- as opposed to subscribed Software as a Service managed by others.

**Note:**  
Whereas SaaS require less Maintenance costs, there are still many services and capabilities that already exist, therefore do not need custom development, but are not yet available for subscription/SaaS.

## Scope

The following are the Requirements categories defined in this Tier:

|  |  |  |
| --- | --- | --- |
| Defined | Undefined (Inherited) | Details |
| * Security * Usability * Maintainability * Portability | * Privacy Deliverability * Functionality * Reliability * Performance | All systems, whether for government, education or other purposes, are required to abide by national laws and regulations that are applicable to all persons. |

## Security

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | o**General** o**Confidentiality** þ**Integrity** o**Non-Repudiation** o**Accountability** o**Authenticity** | | | |  |  |  |  |  |
|  | **Integrity** | | | |  |  |  |  |  |
|  | QR- INS-SEC- 00 | Organisation/ NZMOE/Hosted/ Installed/ Security/ Integrity/ Information/ Configuration | Integration Configuration MUST be encrypted if it cannot be persisted in a secure storage. | Contributes to the obligation of implementing  Defence in Depth. |  |  |  | Connection strings to services (datastores, etc.) that are persisted in the configuration files of a system are a risk if the device becomes accessible to a miscreant.   Important: Where encryption is not possible, the credential must be identified in the project’s risk registry. |  |
|  | QR- INS-SEC- 00 | Organisation/ NZMOE/ Hosted/ Installed/ Security/ Integrity/ Information/ Configuration/ Handling | The solution 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- INS-SEC- 00 | Organisation/ NZMOE/ Hosted/ Installed/ Security/ Integrity/ Certificate/ Lifespans | The solution 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. |  |  |  | The solution includes automated mechanisms to regularly commission and deploy new certificates, at every deployment.  The solution 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- INS-SEC- 00 | Organisation/ NZMOE/ Hosted/ Installed/ Security/ Integrity/ Service Accounts | The solution’s 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- INS-SEC- 00 | Organisation/ NZMOE/ Hosted/ Installed/ Security/ Integrity/ Service Accounts | Each Connection to Services Dependencies, in each Environment category (e.g. ST, UT, PR), in each Network Domain (Test, Production) MUST use an individual service account. | Service Accounts should be provided the least access so that if they are compromised only one dependency service is compromised. |  |  |  | The naming pattern will follow an organisation specific naming scheme (e.g.: ‘{from}-{to}-svc’, such that a single channel’s service account may be named similar to: ‘myproject-someservicesapis-svc’) |  |
|  | QR- INS-SEC- 00 | Organisation/ NZMOE/ Hosted/ Installed/ Security/ Integrity/ WAF | The solution MUST be protected by Firewalls and Web Access Firewalls (WAF)s. | Firewalls limit the surface of attach to a single (web) port, and WAFs analyse web traffic for abnormal behaviour and intrusion. |  |  |  | The solution uses a Firewall to only allow traffic from clients to the service via ports 80 (for HTTP) and 443 (for HTTPS).  The solution’s WAF must be configurable to permit media containing malware through if the service is capable and configured to inspect media uploads for malware (this configuration permits a better user experience due to more informative error messages, compared to a general WAF generated error). |  |
|  | QR- INS-SEC- 00 | Organisation/ NZMOE/ Hosted/ Installed/ Security/ Integrity/ Information/ At Rest/ Data Backups | Production Data Backups MUST be separated from Non-Production Data environments.  Access to Production Data, whether in a PROD data system or a backup, must be restricted to only service accounts. | Backups are production data – just from a point in time in the past – and should be protected as completely as production data. |  |  |  | Backups are encrypted  Access to Backups is limited to Deployment Service accounts  Backup Restoration operations are accessible to Operations Specialists. |  |

## Reliability

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | o**General** o**Maturity** o**Availability** o**Fault Tolerance** o**Recoverability** | | | |  |  |  |  |  |

## Maintainability

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | o**General** þ**Modularity** o**Reusability**  o**Analysability** o**Modifiability** o**Testability** | | | |  |  |  |  |  |
|  | **Modularity** | | | |  |  |  |  |  |
|  |  | Organisation/ NZMOE/ Hosted/ Installed/ Maintainability/ | Services MUST be accompanied with sufficient documentation to successfully support system users, as well as operate and maintain service components. | Delivery stakeholders are not expected to remain available for the service's lifespan.  In order to ensure their knowledge is not lost, documentation is required. |  |  |  | Better yet, in addition to written documentation, automated tests that demonstrate how the system works are far more valuable over the full service lifespan. |  |

# Organisation (NZ MOE) Specific (Subscribed) System Qualities

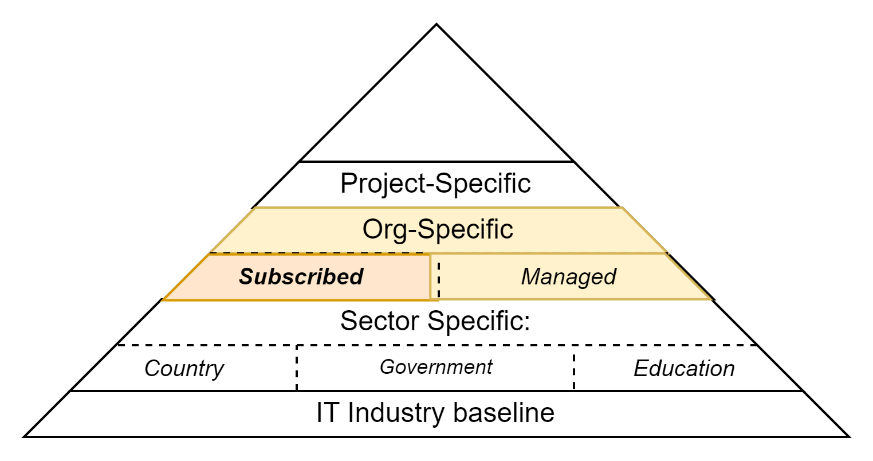


Figure 4: Organisation Specific Tier of System Quality Requirements

The Ministry of Education imposes few additional quality requirements beyond general Education Sector tier requirements.

## Scope

The following are the Requirements categories defined in this Tier:

|  |  |  |
| --- | --- | --- |
| Defined | Undefined (Inherited) | Details |
| * Security * Usability * Processes | * Accreditation * Deliverability * Functionality * Reliability * Performance * Maintainability * Portability * Maintainability | Systems in the Education Sector are mandated to comply with statements within the Education Act that are specific to digital services.  Additionally, systems are to use national education infrastructure services. |

## Processes

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | þ**General** | | | |  |  |  |  |  |
|  | **General** | | | |  |  |  |  |  |
|  | QR-MOE-COM- 00 | Organisation/ NZMOE/ Managed/ Processes/ Governance/ ATO | The delivery of the solution to a Prod Data environment MUST adhere to the organisation’s processes. | The ministry is obligated by regulation to ensure services obtain an Authority to Operate (ATO) by the Chief Digital Officer (CDO) before deployment to a Prod Data environment, requiring refreshing every 2 years. |  |  |  | The CDO takes advice on whether to do this from the Change Authority Board (CAB).  CAB ensures the service is:  - secure,  - supportable,  - operable,  - maintainable.  CAB does by ensuring  - security specialists have verified the solution’s data meet its obligations, system’s design, implementation, and deployment meets security obligations (see NZISM),  - support services have accepted an Application Support Guide (ASG),  - operations services have accepted an operations manual,  - Maintenance services have accepted development, quality assurance, deployment, backup and restoration documentation. |  |

## Security

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | þ**General** þ**Confidentiality** þ**Integrity**  o**Non Repudiation** o**Accountability** o**Authenticity**  o**Availability** | | | |  |  |  |  |  |
|  | **General** | | | |  |  |  |  |  |
|  |  | Organisation/ NZMOE/ Managed/ Security/ General/ | The solution’s services MUST have processes in place to detect and manage vulnerabilities. |  |  |  |  | Note: Vulnerabilities are not to be confused with Attack attempts.  Questions: How often are application level vulnerability scans conducted?  Are these independently performed or verified?  Please provide a copy of the latest report(s).  As a Service (additionally):  Are regular network penetration tests conducted, and if so, how often?  Are these independently conducted?  Please provide a copy of the latest report(s). |  |
|  | QR-MOE-SEC- 00 | Organisation/ NZMOE/Organisation/ NZMOE/ Managed/ Security/ General/ Incidents | The solution MUST support Ministry endorsed security incident processes. | Appropriate subscribed stakeholders must be made aware of security incidents in order to ascertain the risk to their business concerns and determine whether it is appropriate to inform end users. |  |  |  | the solution includes a means of informing appropriate subscribed stakeholders, within stated response delays, keep them informed of progress towards resolution, inform them when resolution is achieved, deliver a summary report.  In the event of a security incident within the solution, processes exist (and are accessible and fit for purpose) to support recovery as applicable.  Note: Solution design with the successful vendor will include creation of a security incident classification matrix and different classes of security incident will be assigned to the incident resolution requirements defined in the ‘Target Objectives’. |  |
|  | QR-MOE-SEC-00 | Organisation/ NZMOE/ Managed/ Security/ Integrity/ Cloud Provider | The solution MUST use MOE Cyber Security team Accredited cloud providers. | As described under the Government Sector Requirements defined below, Cloud First is an AoG mandated directive, but the cloud provider used to meet this obligation must be accredited.  The solution must be accreditawithout having to accredit the underlying cloud provider as well. |  |  |  | MOE accredited cloud providers include: - Azure - AWS |  |
|  | Confidentiality | | | |  |  |  |  |  |
| J | QR- MOE- SEC-00 | Organisation/ NZMOE/ Managed/ Security/ Confidentiality/ External IdP/ ESL | The solution MUST be capable of using standard protocols to connect to the sector's Education Sector Logon (ESL) service. | This organisation's default identity service is Education Sector Logon (ESL). |  |  |  | Some Identity Protocols are not standardized. The solution is capable of being customised to meet an IdP’s small variations to standard protocols (version, validation, etc.). |  |
|  | Integrity | | | |  |  |  |  |  |
|  | QR- MOE- SEC- 00 | Organisation/NZMOE/Managed/ Security/ Integrity/ External Roles Management | The solution MAY be able to sync Roles with a ministry provided Role Management Service. | This organisation's default identity service for ministry and sector workforce is the Education Sector Logon (ESL) service. |  |  |  | ESL can assign Roles to a User per Provider. | This pattern is flawed.  Role management should be organised per organisation.  Not centrally trying to control roles in other organisation. |
|  | QR-MOE-SEC- 00 | Organisation/ NZMOE/ Managed/ Security/ Integrity/ Session/ Duration/ Variable | The solution MUST enable configuration of the duration of a Session (e.g., 20minutes to 30 days) | A user should not be required to unnecessarily sign back often, interfering with their work. |  |  |  | This may be handled internally or external via the integrated Identity Provider. |  |
|  | QR-MOE-SEC-00 | Organisation/ NZMOE/ Managed/ Security/ Integrity/ Media/ Validation |  |  |  |  |  |  |  |

## Compatibility

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | | Comments | | | Details |  |
|  | o**General** o**Co-Existence** þ**Interoperability** o**…** | | | |  | |  | | |  |  |  |
|  | **Interoperability** | | | |  | |  | | |  |  |  |
|  | QR- MOE- COM- 00 | Organisation/ NZMOE/ Managed/ Compatibility/ Interoperability/ IdP/ ESL | Services **MUST** be capable of modifying the use of standard authentication protocols, to connect to the sector's Education Sector Logon (ESL) service (an IdP), which may have small variations to standards. | This organisation's default identity provider service (IdP) is the Education Sector Logon (ESL). |  |  | | |  | |  |  |
|  | QR- MOE- COM- 00 | Organisation/ NZMOE/ Managed/ Compatibility/ Interoperability/ Sector SoR | The system MUST integrate with organisation or sector systems of record as required to meet project specific outcomes. | The system must not duplicate the collection of records that are already available via integration with authoritative sources. |  |  | | |  | | Systems to consider whether are relevant or not the delivery of the service:  FIRST: The System of Record for Education Providers (Schools)  NSI: the System of Record for Learners (Students)  ENROL: The system of Record for the association of Learners to Providers  Learner Record System: The system of Record for Learner progress and achievement (currently a function of the Te Rito service).  OCH: The sector’s Repository of Learning Resources (media). |  |
| J | QR-MOE-COM- 00 | Organisation/ NZMOE/ Managed/ Compatibility/ Interoperability/ Datawarehouse | The system’s key data MUST be exported for collection by a data warehouse. | The organisation’s data warehouse permits Reports being generated from consolidated Views composed of data from multiple systems. |  |  | | |  | | A data extraction process should extract information that is placed in a location that is accessible for collection by the data warehouse. |  |

## Usability

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | o**General** o**Appropriateness** o**Learnability**  o**Operability** o**User Protection Error**  þ**User Interface Aesthetics** o **Accessibility** | | | |  |  |  |  |  |
|  | **User Interface Aesthetics** | | | |  |  |  |  |  |
| J | QR- MOE- USA- 01 | Organisation/ NZMOE/ Managed/ Usability/ Standards/ Web Interfaces | Custom Code that has a web based Graphical User Interface (GUI) MUST follow the organisation’s UI Style Guidance. | Interfaces by the same organisation must be recognisably from the same organisation. |  |  |  | This requirement is separate but should not interfere with adhering to the obligation that user interfaces need to meet Government mandated Web Standards so that they are accessible to impaired users. |  |

## Performance

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | o**Time Behaviour** þ **Capacity** | | | |  |  |  |  |  |
|  | **Capacity** | | | |  |  |  |  |  |
|  | QR-MOE-PRF-00 | Organisation/ NZMOE/ Managed/ Performance/ Capacity/ Scalability/ Horizontal | The solution must have the ability to scale up or down on a single node. | To increase or decrease volume or business throughput on the service it should be possible for memory, CPU, disk space and other components within a node, to be replaced or upgraded without the need to replace that server or node. |  |  |  | Scaling vertically (up/down) means adding resources to (or removing resources from) a single node, typically involving the addition of CPUs, memory or storage to a single computer. |  |
|  |  |  | The solution MUST be able to scale horizontally by adding or subtracting adding more nodes to/from a system | To ensure the solution can grow/shrink as more users are added/subtracted without its performance being negatively impacted. |  |  |  | Scaling horizontally means adding nodes to (or removing nodes from) the system, typically involving the addition of servers, computers, or routers to a distributed software application. An example might involve scaling out from one web server to three. |  |

# Sector (NZ Education) Specific System Qualities

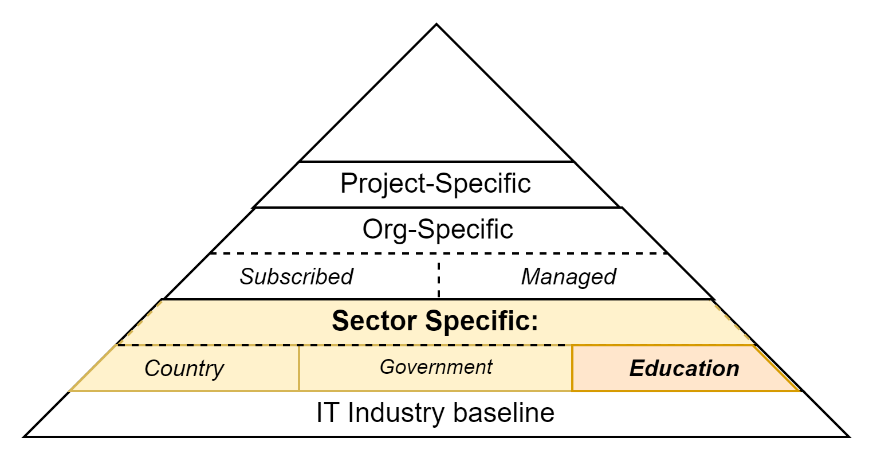


Figure 5: Sector (NZ Education) Specific Tier of System Quality Requirements

The education sector imposes few additional quality requirements beyond general all-of-government requirements defined later within this document.

## Scope

The following are the Requirements categories defined in this Tier:

|  |  |  |
| --- | --- | --- |
| Defined | Undefined (Inherited) | Details |
| * Accreditation * Security * Maintainability | * Deliverability * Functionality * Usability * Reliability * Performance * Maintainability * Portability | Systems in the Education Sector are mandated to comply with statements within the Education Act that are specific to digital services.  Additionally, systems are to use national education infrastructure services. |

## Processes

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | o**General** þ**Accreditation** | | | |  |  |  |  |  |
|  | **Accreditation** | | | |  |  |  |  |  |
| J | QR-EDU-ACC- 00 | NZEDU/ Accreditation | Services MUST comply with current legislation obligations:  NZ Education Act. | The solution is subject to the same laws that govern any other aspect of the country.  Specifically, but limited to, the following considerations:  Education Act: National Identifiers must not be used as natural keys, or round-tripped outside the system. |  |  |  |  |  |
|  | QR-EDU-ACC- 00 | NZEDU/ Quality Assurance | The solution’s functionality and qualities MUST be quality assured before significant change releases. | Business and support specialists should have confidence that the solution automates testing to support a quicker delivery of confidence to system certifiers and accreditors. |  |  |  |  |  |

## Security

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | o**General** o**Confidentiality** o**Integrity**  o**Non-Repudiation** o**Authenticity** o**Accountability** o**Accessibility** | | | |  |  |  |  |  |

## Compatibility

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | o**General** o**Co-Existence** þ**Interoperability** | | | |  |  |  |  |  |
|  | **Interoperability** | | | |  |  |  |  |  |
|  | QR-EDU- COM- 00 | NZEDU/ Compatibility/ Interoperability/ | Education sector related Resources MUST be exportable in international and current education sector protocols. | For improved interoperability and whole sector usability, information must be shared using education sector appropriate and endorsed formats and protocols | Consider:  CASE  SCORM  cmi5  LTI  NZSIF  Common Cartridge |  |  |  |  |

## Maintainability

*Digital deliverables must permit the organisation meaningfully participating in maintenance and improvement of digital deliverables received.   
Note that the organisation’s digital capabilities are limited compared to a development services provider.*

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | | Response | Comments | | Details |  |
|  | o**General** o**Modularity** þ**Reusability** o**Analysability** o**Modifiability** o**Testability** | | | | |  |  | |  |  |  |
|  | **Reusability** | | | | |  |  | |  |  |  |
|  | QR- EDU- MAIN- 00 | NZEDU/ Maintainability/ Reusability/ Standards and Patterns | Custom Code MUST align and leverage organisation standards and patterns. |  |  | |  | |  | 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 |  |
|  | QR-EDU-MAIN-00 | NZEDU/ Maintainability/ Change Notification | Feature changes to the solutions MUST be communicated to subscribed Stakeholders. | Uses should be able to prepare for changes to the system. |  | |  | |  | The system notifies users of system changes. |  |

# Sector (NZ Government) System Qualities

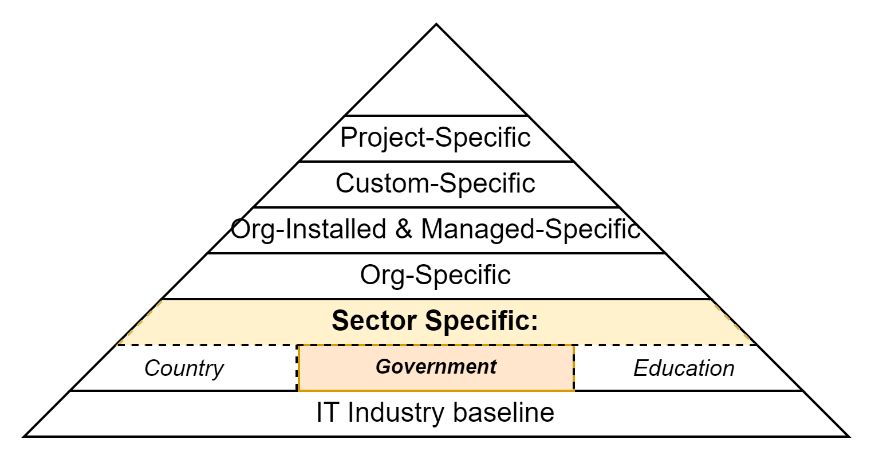


Figure 6: Sector (NZ Government) Specific Tier of System Quality Requirements

Governments agencies are subject to the same laws and regulations as any other organisation, while also being obligated to must adhere to a small set of regulations to ensure they operate to a higher level of accessibility, transparency and accountability than regular organisations.

## Scope

The following are the Requirements categories defined in this Tier:

|  |  |  |
| --- | --- | --- |
| Defined | Undefined (Inherited) | Details |
| * Accreditation * Security * Maintainability * Usability | * Privacy * Deliverability * Functionality * Reliability * Performance * Maintainability * Portability | Government agencies are mandated to deliver certain outcomes while adhering to certain constraints.  For example, Accreditation is a activity mandated for all NZ government agency services before they are made available to consumers.  Additionally, the system is mandated to adhere to NZISM.  Furthermore, the system is mandated to be Cloud hosted in a cloud optimised manner (i.e., avoiding IaaS). |

## Processes

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | o**General** þ **Security** | | | |  |  |  |  |  |
|  | QR-GOV-PRO- 00 | NZGovt/ Processes/ CISCO | The delivery of any government offered solution to production data environments MUST follow the NZISM defined Certification and Accreditation Process. | This Agen |  |  |  | The Certification Authority of this agency is the Chief Information Security Officer (CISO). |  |
|  |  |  |  |  |  |  |  | Refer to AoG Principles, which outline data and information handling constraints. |  |

## Security

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | | Response | | Comments | Details |  |
|  | þ **General** þ **Confidentiality** þ **Integrity** o**Non-Repudiation** o**Accountability** o**Authenticity** o**Availability** | | | | |  |  | |  |  |  |
|  | **General** | | | | |  |  | |  |  |  |
|  | QR-DEF-SEC- 00 | NZGovt/ Security/ General/ Accreditation | The solution MUST complete and achieve security Certification and Accreditation (C&A) by the agency prior to production implementation. | The process incorporates:  - Security Risk  Assessment - Security Risk  Management  Assessment - System Security   Plan  The controls defined  within the   System Security Plan  must be mappable to  an acceptable detailed  control catalogue  (including the latest  NZISM version). | |  | |  |  | The solution has previously achieved C&A from another organisation and what artefacts are available to advance through this process as rapidly and cost effectively as possible. |  |
|  | QR-GOV-SEC-00 | NZGovt/ Security/ General/ Data Classification | The solution’s information  MUST be rated. | The rating informs the minimum level of controls and mitigations a government system must implement. | |  | |  |  | The solution information must be rated under either Policy and Privacy classification (UNCASSIFIED, IN-CONFIDENCE, SENSITIVE) or National Security classification (RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET)  See: [Classifications | Protective Security Requirements](https://protectivesecurity.govt.nz/classification-system/overview/classifications/#:~:text=Classifications%20are%20divided%20into%20two,international%20relations%20of%20New%20Zealand.) And [Classification Examples (protectivesecurity.govt.nz)](https://protectivesecurity.govt.nz/assets/Classification/Classification_Examples.pdf) |  |
|  | **Integrity** | | | | |  |  | |  |  |  |
|  | QR-GOV-SEC- 00 | NZGovt/ Security/ Integrity/ Physical Security Controls | 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. | |  | |  |  | The solution’s environments are hosted within an ISO-27001, Level2+ based data facility, which limits, monitors and audits physical and virtual access to devices.  The solution 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 | NZGovt/ Security/ Integrity/ Data/ Location | Data classified as RESTRICTED or higher MUST be persisted in New Zealand, and if not available, Australia. |  | |  | |  |  | Not to be confused with Data Sovereignity |  |
|  | QR-DEF-SEC- 00 | NZGovt/ Security/ Integrity/ NZISM | The solution design MUST implement NZISM recommended security and risk mitigations controls appropriate to the system's NZ government data classification, as defined in the ’Target Objectives’. | A system must apply applicable NZISM recommended safety and risk mitigation controls to safely persist user provided data. | |  | |  |  |  |  |
|  | QR- GOV- SEC- 00 | NZGovt/ Security/ Integrity/ NZISM | The solution MUST implement all Security Controls defined within the Default System Qualities section as part of its implementation of NZISM. | NZ Govt agencies are obligated to implement NZISM defined Controls  appropriate to the information's highest security classification, as defined in the ’Target Objectives’. | |  | |  |  | Other than declaring the relationship to the mandated implementation of applicable NZISM controls, this requirement does not introduce more requirements than the common best practice ones previously outlined under Default System Qualities.  Namely: - Defence In Depth - Firewall & WAF   (intrustion detection) - Infra  scalability,  (Horiz.+Vert) - Encryption in  Transit - Encryption at  Rest - Credential  protection - AuthN via IdP - AuthZ applied - Auditing of  Activity - Sanitizing  Diagnostics  Logs and  Error Reports - Monitoring &  Alerting - Hardening   (OS, Services)  Reference: [http://www.gcsb.govt.nz/publications/th e-nz-information-security-manual](http://www.gcsb.govt.nz/publications/the-nz-information-security-manual)  <https://protectivesecurity.govt.nz/home/information-security-management-protocol/new-zealand-government-security-classification-system/> |  |
|  | QR-GOV-SEC-00 | NZGOVT/ Integrity/Data/In Transit/SENSITIVE | The solution MUST transit data in accordance with its data classification. |  | |  | |  |  | For data classified as SENSITIVE the following applies:  Information must be marked SENSITIVE.  All SENSITIVE information transmitted across public networks, including the Internet, within NZ or across any networks overseas must be encrypted using a system approved by GCSB (see SE-012). |  |
|  | **Confidentiality** | | | | |  | |  |  |  |  |
| X | QR-GOV-SEC- 00 | NZGovt/ Confidentiality/ Information/ In Transit/ Encryption | The solution MUST protect communication in transit between devices. | NZISM mandates that systems must utilise specified controls specific to the system’s security classification, (as defined within the ‘Target Objectives’). | |  | |  |  | Note this is the same requirement as previously defined under Default System Security quality requirements – only adding that the task is mandated by NZISM for all Government offered services. |  |
|  |  |  |  |  | |  | |  |  |  |  |
|  | **Integrity** | | | | |  | |  |  |  |  |
|  |  |  |  |  | |  | |  |  |  |  |
|  | QR-DEF-SEC- 00 | NZGovt/ Security/ Integrity/ Client Credentials | The solution MUST not deploy credentials to external clients. | Credentials that are deployed and persisted outside a system’s infrastructure are compromised. | |  | |  |  | The solution avoids using integration approaches that require the installation of certs on service clients. |  |
|  | QR-GOV-SEC- 00 | NZGovt/ Integrity/ Information/ At Rest/ Encryption | The solution MUST protect user-generated information at rest. | Information MUST be stored and transmitted as per the GCSB New Zealand Information Security Manual (NZISM) v2.4 (or later versions) controls to meet the requirements specified for data with a security rating as per the ‘Target Objectives’. | |  | |  |  | This is the same requirement as previously defined under Default Security quality requirements, explaining that it is mandated for Government offered services. |  |
|  | QR-GOV-SEC- 00 | NZGovt/ Security/ Integrity/ Information/ At Rest/ Sensitive Configuration Parameters | The solution 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-GOV-SEC- 00 | NZGovt/ Integrity/ Data Classification | The solution MUST use NZISM recommended security and risk mitigations controls appropriate to the system's NZ government data classification, as defined in the *’Custom Code’*. | A system must apply applicable NZISM recommended safety and risk mitigation controls to safely persist user provided data. | |  | |  |  | The solution adheres to NZISM security controls.  References:  <https://protectivesecurity.govt.nz/home/information-security-management-protocol/new-zealand-government-security-classification-system/> |  |

## Functionality

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | o**General** o **Completeness** þ **Correctness** o**Appropriateness** | | | |  |  |  |  |  |
|  | **Functional Correctness** | | | |  |  |  |  |  |
|  | QR- GOV-  FUN- 00 | NZGovt/ Functionality/ Correctness/ ??? | Functionality MUST be provided to permit adherence to Regulation applicable to Government Agencies. | All NZ Government agency services must adhere to regulation defined within:   * Public Records Act 2005 * Official Information Act 1982 * Education Act |  |  |  | In addition to constraints common to all services provided within New Zealand, defined under the *New Zealand Default System Qualities* tier, Functionality is required to adhere to regulation governing - Provide User Interface links as per NZ WAG  - Leaving archived System Data within Systems  - Transmitting a learner’s National Student Number (NSN) between services  - Providing Search and Reporting capabilities to contribute to Requests for Information (ROI)s. |  |

## Compatibility

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | o**General** o**Co-Existence** o**Interoperability** | | | |  |  |  |  |  |

## Usability

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | o**General** þ **Appropriate Recognisability** o**Learnability** o **Operability** o **User Error Protection** o**User Interface Aesthetics** þ **Accessibility** | | | | |  |  |  |  |  |
|  | **Appropriateness Recognisability** | | | | |  |  |  |  |  |
|  | QR-GOV- USA- 00 | NZGovt/ Usability/ Recognisability/ NZ WAG | | Web Interfaces within the solution MUST meet NZ Government Web Standards - Web Usability Standards. | All NZ Government web services MUST use similar branding layout and structure. |  |  |  |  | The solution meets NZ GWS WUG obligations.  For example, the service client has a Home Page, Navigation, Copyright notice, etc. |
|  | **Accessibility** | | | | |  |  |  |  |  |
|  |  | NZGovt/ Usability/ Languages | | The solution MUST be accessible to users in all of the national spoken languages. | New Zealand citizens use one or both of the two spoken national languages (the third being a visual language, used by hearing impaired citizens):  - en-NZ (NZ English)  -mi-NZ (NZ Māori) |  |  |  |  | Providing public services in both languages is mandated. |
|  | QR-GOV-USA- 00 | NZGovt/ Usability/ Accessibility/ WAS | | Solution Web Interfaces MUST meet NZ Government Web Accessibility Standards | All NZ Government web services must be accessible by impaired users. |  |  |  |  | This requirement is no more than that previously defined for Default Systems (i.e., MUST meet WCAG 1.1 at Level AA). |

## Maintainability

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | o**General** þ**Modularity** o**Reusability** o**Analysability** o**Authenticity** o**Modifiability** o **Testability** | | | |  |  |  |  |  |
|  | **Modifiability** | | | |  |  |  |  |  |
|  | QR-GOV-MAI- 00 | NZGovt/ Maintainability/ Modifiability/ AoG/ Cloud-First | The solution MUST installed in a Cloud. | To meet AoG Regulations. |  |  |  | The objective is for a SaaS based solution before a PaaS based one, before a CaaS based one, before IaaS.  ‘Organisation Managed’ Physical or Virtual resources are not acceptable solutions. |  |
|  | **Testability** | | | |  |  |  |  |  |
|  | (No Tier specific requirements. See next Tier down the pyramid) | | | |  |  |  |  |  |

## Portability

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | o **General** o **Adaptability** o **Installability** o **Replaceability** | | | |  |  |  |  |  |

# Sector (NZ) specific System Qualities

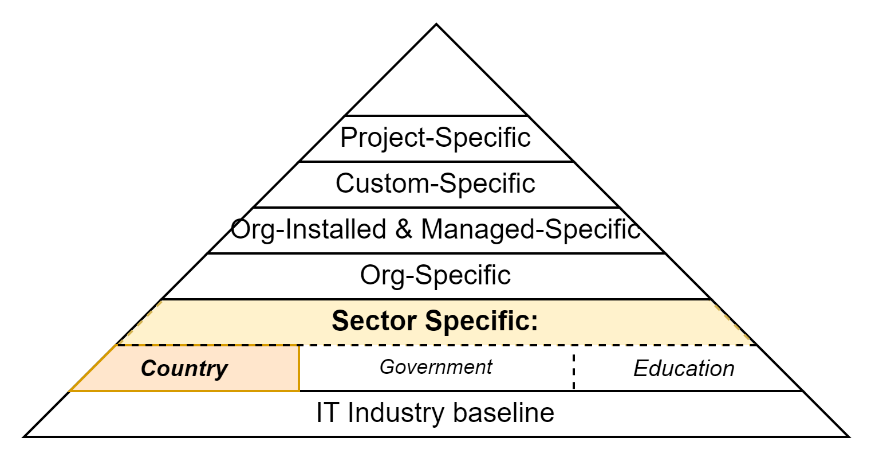


Figure 7: Sector (NZ) specific Tier of System Quality Requirements

The following are New Zealand specific requirements that override the underlying Default tier’s common baseline requirements.

## Scope

The following are the Requirements categories defined in this Tier:

|  |  |  |
| --- | --- | --- |
| Defined | Undefined (Inherited) | Details |
| * Privacy | * Security * Deliverability * Functionality * Usability * Reliability * Performance * Maintainability * Portability | All systems, whether for government, education or other purposes, are required to abide by national laws and regulations that are applicable to all persons. |

## Privacy

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | þ **General** | | | |  |  |  |  |  |
|  | **General** | | | |  |  |  |  |  |
| J | QR- NZ- PRI- 01 | NZ/ Regulation/ Privacy Act 1993 | The solution MUST adhere to the applicable Acts outlined under the ‘Target Objectives’. | The solution must meet NZ legal obligations before being accreditable to be delivered as a service by this organisation. |  |  |  | This requirement is the same as the requirement defined under Default System Qualities, but explicit in naming NZ applicable laws. NZ Laws applicable to all systems offered within New Zealand include:  Privacy Act 1993  Education Act  Note that additional NZ Laws specific to Government Agencies are covered within the Government Domain Requirements section above (e.g.: Public Records Act, Official Information Act). |  |
|  |  | NZ/ Security/ Integrity/ Data/ Sovereignty/ Māori | The Solution MUST persist Māori data in New Zealand.  If that is not reasonably possible, permission must be granted to the service to persist Māori data in Australia. |  |  |  |  | See: [Te Mana Raraunga](https://www.temanararaunga.maori.nz/) |  |

# Default Baseline IT System Qualities

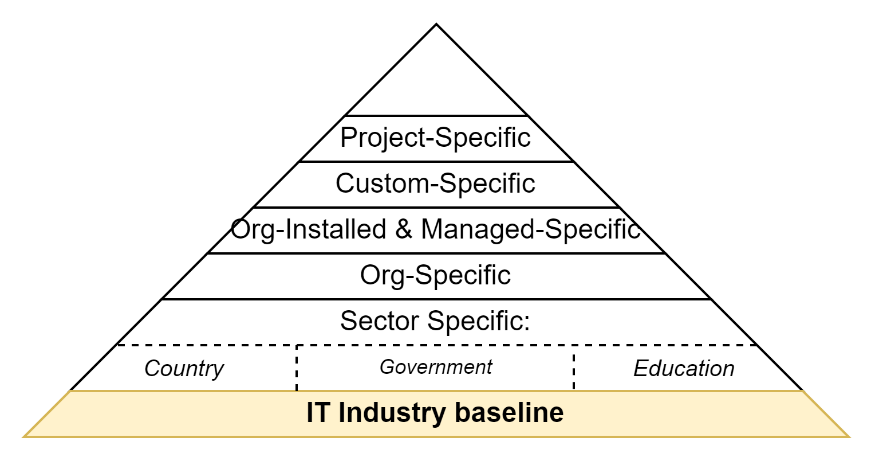


Figure 8: Default System Base Tier of Quality Requirements

Systems by default are expected to meet the following quality requirements.  
Requirements specific to specific involved sectors (Country, Government, Education) are defined in those tiers, earlier in the document.

## Scope

The following are the Requirements categories defined in this Tier:

|  |  |  |
| --- | --- | --- |
| Defined | Undefined | Notes |
| * Delivery * Security * Privacy * Functionality * Usability * Reliability * Performance * Maintainability * Portability | * Processes | Accreditation is Government agency concern, defined under Government Domain requirements. |

## Functionality

Table 4: Default System Functionality Quality Requirements

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | | Details |  |
|  | o**General** þ **Completeness** o**Correctness** o**Appropriateness** | | | | |  | |  |  |  |
|  | Completeness | | | | |  | |  |  |  |
|  | QR-DEF-FUN- 00 | Default/ Functionality/ Completeness | The solution 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. |  |
|  |  |  | 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- 00 | Default/ Functionality/ Information/ Non-Circumventing Security | The solution  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 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 |  | |  |  |

## Security

Table 2: Table of Default System Security Quality Requirements

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | þ **General** þ **Confidentiality** þ **Integrity** þ **Non-Repudiation** þ **Accountability** þ **Authenticity** þ **Availability** | | | |  |  |  |  |  |
|  | General | | | |  |  |  |  |  |
|  | QR-DEF-SEC-00 | Default/Security/Integrity/SOC 2 | Services MUST have a SOC 2 |  |  |  |  | SOC 2 is independently audits of:  **- Security:**  - Firewalls  - Intrusion  Detection  (WAF)  - Networks **- Availability:**  - Perf monitoring  - Site failover   - DR   - Security  incident  handling  **- Processing  Integrity:**  - Quality  Assurance  - Processing  monitoring  - network  **- Confidentiality:**  - Encryption  - Access Control  - Network  - Firewalls  **Privacy:**  - Access control  - 2FA  - Encryption |  |
|  | Integrity | | | |  |  |  |  |  |
|  | QR-DEF-SEC- 00 | Default/ Security/ Integrity/ Defence in Depth | The solution MUST apply recommended risk mitigations to keep the system’s information secure if a tier, layer or component is breached. | 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. |  |
|  | 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). |  |
|  |  | Default/Security/Integrity/Accreditation/ISO-27001, Level 2+ |  |  |  |  |  |  |  |
|  | 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. |  |  |  | The solution’s environments are hosted within an ISO-27001, Level2+ based data facility, which limits, monitors and audits physical and virtual access to devices.  The solution 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 |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Confidentiality | | | |  |  |  |  |  |
|  | QR-DEF-SEC- 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. |  |
|  | **Integrity** | | | |  |  |  |  |  |
|  | QR-DEF-SEC- 00 | Default/ Security/ Integrity/ Least Privilege | The solution MUST allow solution and business administrators to attribute to end users the least amount of privilege needed to perform their tasks. | Avoid the risk of unauthorised activity (accidental or otherwise). |  |  |  |  |  |
|  | QR-DEF-SEC- 00 | Default/ Security/ Integrity/ Information/ In Transit/ Encryption | The solution MUST protect user-submitted information in transit between devices by encrypted channels, falling back to encrypted messages where not possible with common processes. |  |  |  |  | The solution’s channel encryption is achieved using TLS based HTTP (HTTPS) communication between all internal and external components.  The solution 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). |  |
|  | QR-DEF-SEC- 00 | Default/ Security/ Integrity/ Information/ At Rest/ Encryption | The solution 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/ 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. |  |
|  | QR-DEF-SEC- 00 | Default/ Security/ Integrity/ External Identity Provider Services | The solution 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. |  |  |  | The solution can use current protocols to connect to external identity providers (OIDC, OAuth, SAML).  The solution is capable of authenticating both UI and API security principles (users). |  |
|  | QR-DEF-SEC- 00 | Default/ Security/ Integrity/ External PII Management Services | The solution 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. |  |  |  | The solution 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 | The solution 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 | The solution 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 | The solution 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 | The solution 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 | The solution’s source code repository 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 | The solution 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. |  |  |  | The solution includes automated mechanisms to regularly commission and deploy new certificates, at every deployment.  The solution 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 | The solution’s 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 | The solution 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. |  |
|  | QR-DEF-SEC- 00 | Default/ Security/ Integrity/ Controls/ OWASP | The solution 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. |  |  |  | The solution’s 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 |  |
|  | **Non-Repudiation** | | | |  |  |  |  |  |
|  | QR-DEF-SEC- 00 | Default/ Security/ Non-Repudiation/ ??? | The solution MUST permanently store Session audit records of all operations in order to correctly ascertain the process by which information 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.  The solution 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.  The solution must audit the activity of any background service agents (batch operations, etc.). |  |  |  | The solution 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. |  |
|  | **Accountability** | | | |  |  |  |  |  |
|  | QR-DEF-SEC- 00 | Default/ Security/ Accountability/ Sessions/ Multiple | The solution 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. |  |  |  | The solution allows for a user to have multiple distinct sessions.  the solution allows users to open multiple concurrent sessions from multiple devices |  |
|  | QR-DEF-SEC- 00 | Default/ Security/ Accountability/ Sessions/ User | The solution MUST record the system user identity in all session audit records. | Note:  a session's user may be anonymous until authenticated. The act of Authentication does not change the session, it just clarifies who is in operating in the session. |  | Custom? |  | The solution tracks anonymous users through the process of authentication, ongoing until session termination or timeout. |  |
|  | **Authenticity** | | | |  |  |  |  |  |
|  | QR-DEF-SEC- 00 | Default/ Security/ Authenticity/ IdPs | The solution MUST correctly ascertain the identity of system users using external Identity Providers. | The basis of allowing access to users is knowing who they are. |  |  |  | The solution relies on external IdPs to authenticate users.  Please describe how the solution authenticates system "super users". |  |
|  | **Availability** | | | |  |  |  |  |  |
|  |  | | | |  |  |  |  |  |

## Privacy

Table 3: Default System Privacy Quality Requirements

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | þ **General** | | | |  | |  |  |  |
|  | General | | | |  |  |  |  |  |
|  | QR-DEF-PRV- 00 | Default/ Privacy/ Laws | The solution MUST adhere to the applicable laws of the country. | The solution must meet legal obligations before being accreditable to be delivered as a service by this organisation. |  |  |  |  |  |
|  | QR- DEF- PRV- 00 | Default/ Privacy/ PI/ Scope & Use | Services MUST inform and request the consent from end users as to the scope and purpose for which Data is collected by the system. | The requirement is a prerequisite for being able to implement Privacy regulations in most locations which the system is to be used. |  |  |  |  |  |
|  | QR-DEF-PRV- 00 | Default/ Privacy/ PI/ Minimum | The solution 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. |  | The solution actively avoids requesting non-essential PII information.  The solution 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-PRV- 00 | Default/ Privacy/ Correction | The solution MUST allow users to self-correct their own information. | Users know themselves best. |  | The solution allows users to change or request changes to the PII information imported from an external PII service. |  |  |  |

## Compatibility

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | TODO | | | |  |  |  |  |  |
|  | Co-Existence | | | |  |  |  |  |  |
|  | Compatibility | | | |  |  |  |  |  |
|  | QR- DEF- COM- 00 | Default/ Compatibility/ Interoperability/ ??? | The service MUST permit extraction of records via APIs. | At end of service lifespan, the system’s data must be extractable, transformable, and loading into the service’s replacement. |  |  |  | Extracting data from databases introduces security (unauditable etc.) and data validation errors, |  |
|  |  | Default/ Compatibility/ Interoperability/ IdP | 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. |  |  |  |  |  |
|  |  | **Default/ Compatibility/ Interoperability/ Data warehouse** | Services **MUST** be capable of having its key information published to a data warehouse. |  |  |  |  | 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. |  |
|  |  | **Default/ Compatibility/ Interoperability/ Malware Detection Service** | Custom Code services MUST be integrated with 3rd party malware detection services. |  |  |  |  | Applying defence in depth principles, the service should not depend on an external WAF to catch malware.   In built malware services are able to be rerun on persisted media at a configurable cycle, catching malware that was uploaded before the malware signatures were updated. |  |
|  |  | **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/SDKs | Exposed APIs MUST be with delivered with Software Developed Kits (SDKs) demonstrating their use, delivered in a state invokable from a Command Line Interface (CLI) or pipeline automation. | It is important to provide information on how the services available APIs can be invoked from a delivery pipeline. |  |  |  | Upon agreement, Postman scripts may be acceptable. |  |
|  | QR-DEF-MAIN-00 | Default/ Compatibility/ Interoperability/ SCIM | The solution MUST be able to be provisioned with users, groups and roles via an API -- preferably one that is Standards based. |  |  |  |  | A protocol (SCIM or equivalent) can be used to provision and deprovision groups, users and users within the solution.  *Note: these APIs are in addition to the base APIs provided to manage users, groups, etc.* |  |
|  |  | Default/ Compatibility/ Interoperability/ Querable APIs | REST APIs MUST be offered in a ‘queryable’- in a standards based approach manner. | Providing Queryability to REST APIs, permitting Filtering, Sorting, Merging, Projection and Paging -- for no extra effort -- decreases development complexity, effort, cost, while improving modularity and reuse. |  |  |  | Using OData, and optionally GraphQL.  Remove DoS attacks by applying recommended logical controls (e.g.: applying limits to the number of records that can be returned in one Page: 100). |  |
|  |  | Default/ Compatibility/ Interoperability/ Bae APIs | Custom services MUST appropriately expose all core functionality externally via APIs. | The design is in accordance with API-First design principles. |  |  |  | Core functionality is expected to include:  Diagnostics  Errors Reports  Settings  Sessions  Session Operations  Session Devices  Users  User Profile/Preferences  Groups  Organisations  Group Responsibilities, Obligations, Permissions  Roles  User Role Assignments  User Permission Assignments  Group Workflows,  Resource Metadata,  Resource Rights,  Resource Roles  Resource Responsibilities, Obligations, Permissions |  |

## Usability

Table 5: Default System Usability Quality Requirements

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | o**General** o **Appropriate Recognisability** o**Learnability** þ **Operability** þ **User Error Protection** þ **User Interface Aesthetics** þ **Accessibility** | | | |  |  |  |  |  |
|  | Operability | | | |  |  |  |  |  |
|  | 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 | The solution 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. | The solution’s purpose is 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 | The solution MUST by default handle Unicode, UTF-8 transmission, and UTC datetimes. | The solution 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/ Management/ Self-Reliant | Services **MUST** not rely on 3rd party services 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 an 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 | | | |  |  |  |  |  |
|  | QR- DEF- USA- 00 | Default/ Usability/ Validation/ ServerSide | Services tier **MUST** validate all input at the Service Facade. | The solution must protect the data quality using validation -- irrespective of the UI used. |  |  |  | The solution 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 | | | |  |  |  |  |  |
|  | 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. |  |  |  |  | Does the service permit system branding?  Does the service permit tenancy branding? |
|  | Accessibility | | | |  |  |  |  |  |
|  | QR-DEF-USA- 00 | Default/ Usability/ Accessibility/ WCAG | Service Graphical User Interfaces (GUI) SHOULD meet WCAG 2.2 standards to an Level AA or higher. | Services must be usable by visually impaired users. |  |  |  | The organisation of data for WCAG impacts other positive outcomes. Notable succinctness of interfaces, organised repeated layout patterns, etc. Note also that  WCAG 2.0 is also referred to as ISO-40500. | What level of WCAG compliance is the service currently able to achieve? |
|  | 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. | Does the service currently develop print specific outputs?  Are they based on web style style-sheets or print-specific formats (e.g.: PDF?) |
|  | 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 | The solution 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. |  |
|  | Recognisability | | | |  |  |  |  |  |
|  | QR- DEF- USA- 01 | Default/ Usability/ Recognisability/ Layout | The solution 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- 02 | Default/ Usability/ Recognisability/ NZ WAG | Any custom UX element of the solution MUST meet NZ Government Web Standards - Web Usability Standards. | All NZ Government web services MUST use similar branding layout and structure. |  |  |  | The solution meets WGAG Level AA.  For example, the service client has a Home Page, Navigation, Copyright notice, etc. |  |
|  | QR- DEF- USA- 00 | Default/ Usability/ Recognisability/ BREAD Interfaces | The solution’s custom interfaces MUST be developed according to Browse/Read/Edit/Delete (BREAD) design patterns to improve usability. | Using a commonly recognised pattern throughout a system improves usability and decreases navigation and data entry error. |  |  |  | The solution uses a common Search/Browse functionality to navigate to Resource specific View/Edit/Add/Delete Views. |  |
|  | 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. | The solution must be accessible via the most prevalent devices (mobile).  The solution must take advantage of the devices and sensors available in a device to provide a better user experience (based on location, etc.) |  |  |  | The solution’s user interface is separate from the service.  The solution’s user interface is developed using the most current recommended development practices in order to provide the longest use. |  |
|  | QR- DEF- USA- 00 | Default/ Usability/ ----/ Configurability | The solution’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. |  |  |  | The solution’s mutable system settings are presented on a System Configuration view. |  |
|  | QR- DEF- USA- 00 | Default/ Usability/ Learnability/ Training | The solution 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.  The solution may provide a digital help system that is readily available to both unauthenticated and authenticated system users. |  |
|  | QR- DEF- USA- 00 | Default/ Usability/ Operability/ ??? | The solution MUST be operable by the widest range of users. |  |  |  |  | The solution follows AoG mandated rules for Usability & Accessibility  The solution uses graphics suitable for visually impaired users.  The solution 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 | The solution 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. |  |  |  | The solution uses a 3rd party service to inspects media uploaded by end users.  The solution can handle checking multiple files in one operation.  The solution does not persist media that is infected.   The solution can rely on an external WAF to do this but preferably performs checks itself. |  |
|  | QR- DEF- USA- 00 | Default/ Usability/ Operability/ User Management | The solution 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. |  |  |  | The solution 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 | The solution MUST be operable from the widest range of current common browsers. | The solution must be accessible and productive from the devices commonly used by both service provider stakeholders and service consumers. |  |  |  | The solution is accessible via the latest web capable devices (desktop, laptop, tablet, mobile).  The solution 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. |  |  |  | The solution is capable of using language packs to localize the user interface's images and text.  The solution’s text and images are managed in language-culture packs  Different cultures may use different imagery  The solution 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. |  |  |  | The solution’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 | The solution MUST provide a generalised means to search the solution for Synopsis records of users and resources, returned in a filtered and paged manner. | The solution’s purpose is to allow users to easily develop, persist and re-find stored information.  Note:  Paging is a required precaution against DOS resource consummation attacks. |  |  |  | The solution’s search service is universal in that it searches across all key elements of the system.  The solution’s search is text based.  The solution’s 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 | The solution 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). |  |  |  | The solution 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 | The solution 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. |  |  |  | The solution 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 | The solution 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. |  |  |  | The solution 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 | The solution 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. |  |  |  | The solution presents information to the user on how to proceed. |  |
|  | QR- DEF- USA- 00 | Default/ Usability/ ???/ Documentation | The solution 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 | The solution 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. |  |  |  | The solution’s service client interface can be skinned to align with the aesthetics of this organisation, and/or AoG directives. |  |
|  |  | Default/ Usability/ ???/ User Voice/System | The solution 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 | The solution 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 | The solution 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. |  |

## Reliability

Table 6: Default System Reliability Quality Requirements

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | | Comments | Details |  |
|  | o **General** þ**Maturity** þ**Availability** þ**Fault Tolerance** þ**Recoverability** | | | |  |  |  | |  |  |
|  | **Maturity** | | | |  |  |  | |  |  |
|  | QR-DEF-REL- 00 | Default/ Reliability/ Maturity/ Supported Technologies | The solution’s language, framework and components MUST be accreditable as supportable technologies. | The solution must be developed using a language and framework that decreases the number of errors in a system. |  |  | |  | The solution 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 | The solution 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. |  |  | |  | The solution is built with a compiled language to limit the number of bugs that make it to a production environment.  The solution’s development team uses strict compilation flags to find and force the fixing of errors early. |  |
|  | QR-DEF-REL- 00 | Default/ Reliability/ Maturity/ Development Framework | The solution 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. |  |  | |  | The solution 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 | The solution 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. |  |  | |  | The solution is capable of working if caching is unable to work.  The number of connections to the database is minimised per request. |  |
|  | **Availability** | | | |  |  |  | |  |  |
|  | QR-DEF-REL- 00 | Default/ Reliability/ Availability/ Horizontally Scalable | The solution **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 | The solution 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. |  |  | |  | The solution is deployed to cloud infrastructure that has a higher uptime SLA than the one described within the ‘Target Objectives’.  The solution is protected by a WAF to limit DoS attack traffic.  The solution 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.  The solution 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.  The solution is deployed using Infrastructure as Code, so that a new production environment can be re-developed quickly after a Disaster.  The solution 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. |  |  | |  | The solution 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** | | | |  |  |  | |  |  |
|  |  |  |  |  |  |  | |  |  |  |
|  | **Recoverability** | | | |  |  |  | |  |  |
|  | QR-DEF-REL- 00 | Default/ Reliability/ Recoverability/ Backups | The solution 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. |  |  | |  | The solution’s data is backed up in full every day.  The solution’s data is backed up incrementally at an interval that satisfies the constraints defined in the ‘Target Objectives’.  The solution’s 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 | The solution’s 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. |  |  | |  | The solution 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. |  |  | |  | The solution attempts to ensure that write operations are committed within a transaction so that all operations either occur together, or don't.  The solution is developed using an ORM to handle requests (as they generally are wrapped in transactions).  The solution 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 | The solution 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. |  |  | |  | The solution 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 | The solution MUST be capable of supporting the projected number of concurrent and absolute users as defined in the ‘Target Objectives’. | The solution 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. |  |  | |  | The solution dynamically scales horizontally based on the CPU being consumed at higher than a specified %, for longer than a specified duration.  The solution 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 | The solution MUST trap unexpected errors and capture relevant information in permanent records. | The solution must record error reports for later analysis by operations specialists. |  |  | |  | The solution 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 | The solution MUST be able to recover from unexpected behaviour. | The solution 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. |  |  | |  | The solution 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 | The solution 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. |  |  | |  | The solution’s 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 | The solution 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. |  |  | |  | The solution uses automation to recreate environments as needed, including restoring data from backups, within short delays. |  |

## Performance

Table 7: Default System Performance Quality Requirements

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | þ **Time Behaviour** þ **Capacity** | | | |  |  |  |  |  |
|  | **Time Behaviour** | | | |  |  |  |  |  |
|  | QR-DEF-PRF-02 | Default/ Performance/ Time Behaviour | The solution 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** | | | |  |  |  |  |  |
|  |  | Default/ Performance/ Resource Utilisation/ SPA | Interfaces developed within ‘Custom Code’ MUST be developed following ‘Single Page Application’(SPA) patterns. | The reduction of interface payloads improves responsiveness, while decreasing the memory and therefore devices required to service peak load.  . |  |  |  | Client side developed pages retributes compute load to edge computers, making the service more economical to manage over its service lifespan |  |
|  | **Capacity** | | | |  |  |  |  |  |
|  | QR-DEF-PRF- 00 | Default/ Performance/ Capacity/ Time Behaviour/ Response Time | The solution’s APIs and User Interface MUST be able to capable of completing Peak surge requests and returning control to users within response times defined in the ’Target Objectives’. | The solution 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 | The solution MUST be capable of completing the requests of the peak user quantity defined in the ‘Target Objectives’ while meeting Responsivity targets. |  |  |  |  | the solution is capable to dynamically scale up and down horizontally to meet peak normal activity. |  |
|  | 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. |  |  |  | The solution does not open transactions at the beginning of requests and close them at the end. |  |
|  | QR-DEF-PRF- 00 | Default/ Performance/ Capacity/ Storage | The solution 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. |  |  |  | The solution 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 | The solution 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. |  |  |  | The solution 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 | The solution MUST be able to manage the expected number of users and resources, described elsewhere. | The solution SHOULD be capable of meeting expectations of users to access the system and manage information. |  |  |  | The solution 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 | The solution MUST be capable of handling – within max acceptable delays defined in the ‘Target Objectives’– the requests of the peak projected number of concurrent users. | The solution SHOULD be capable of handling projected activity surges without frustration of end users, or becoming unavailable. |  |  |  | The solution 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/ CPU | The solution MUST be capable of completing peak surge user requests within delays defined in the ‘Target Objectives’, while consuming no more than 50% of each virtual device they are on. | The solution must be able to handle requests without putting undue demands on physical or virtual hardware, which in turn shortens the lifespan of physical infrastructure. |  |  |  | The solution is capable of dynamically horizontally scaling to handle surge activity requests, using CPU activity as a trigger.  The proposed solution will meet performance delays at peak loads as defined in the ‘Target Objectives’, with CPU loads being no more than 50%, preferably 33%. |  |
|  | QR-DEF-PRF- 00 | Default/ Performance/ Resource Usage/ Background Operations | The solution’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. |  |  |  | The solution 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 | The solution **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 | The solution 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 |  |  |  | The solution processes background activity in a paged, multiple threading manner. |  |
|  | QR-DEF-PRF- 00 | Default/ Performance/ Timing/ Background Tasks | The solution 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. |  |  |  | The solution processes background activity as a separate service account running a separate process, accessing the same database. |  |

## Maintainability

Table 8: Default System Maintainability Quality Requirements

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details |  |
|  | o**General** o**Modularity** o**Reusability** þ**Analysability**  o**Authenticity** þ**Modifiability** þ**Testability** | | | |  |  |  |  |  |
|  | **Analysability** | | | |  |  |  |  |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Analysability/ Reportability/ Alerting | The solution 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. |  |  |  | The solution 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** | | | |  |  |  |  |  |
|  | QR-DEF-MNT-00 | Default/ Maintainability/Modifiability/Disclosures | The Service MUST permit management of disclosure statements. | The statements will disclose:  - tracking disclosure  - data use disclosure  - privacy disclosure  The statements will be different per project.  They may be hosted in the system, in which case they need the means to update the text, or externally on the service’s dedicated brochureware site or the enterprise site - in which case there is a need to configure the links. |  |  |  |  | Does the system currently link to/display disclosure statements?  How many disclosure statements?  Is this variable?  Does the system provide the means to update disclosure statements, or links to them?  Which approach is used? |
|  | 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., “norespnse”). | Systems must have the capability of notifying users who inclusive of users who not currently using the system. |  |  |  | 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”* | Does the system send email?  Is it configurable? |
|  | **Testability** | | | |  |  |  |  |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Testability/ Environments | The Service MUST be deployed through a succession of non-Production Data environments. | The service must be testable before being released, without putting production data at risk. |  |  |  | A recommended sequence of environments  *per development branch* (Trunk or other) 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/ 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). |  |
|  | 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. |  |  |  | A Git based solution is expected.  If not expressed in the Outcome The solution uses a GitHub based repository unless otherwise defined |  |
|  | 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. |  |  |  | The solution 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- 00 | Default/ Maintainability/ Documentation/SelfHelp | Documentation for users to self help themselves MUST be maintained current before deployment. |  |  |  |  |  |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Documentation/Support | Documentation to support the service MUST be maintained current before deployment. |  |  |  |  |  |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Documentation/Operation | Documentation to operate the service MUST be maintained current before deployment. |  |  |  |  |  |  |
|  | 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 |  |  |  | The solution’s 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 | The solution’s 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. |  |  |  | The solution’s 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 | The solution 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. |  |  |  | The solution makes system records searchable in an efficient manner, using filtering criteria & response paging. |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Reportability/ Monitoring | The solution MUST include a means of monitoring key metrics. | Metrics are required to be collected in order to compare abnormal behaviour against. |  |  |  | The solution monitors:  Performance issues  Security issues  Abnormal Behaviour issues  Errors |  |
|  | QR-DEF-MNT- 00 | Default/ Maintainability/ Capacity/Diagnostics trace message storage | The solution 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. |  |  |  | The solution’s diagnostics trace messages are kept for a configurable duration (by default 31 days).  The solution’s 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).  The solution’s 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 | The solution 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 | The solution 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. |  |  |  | The solution’s capabilities, functionality and qualities are tested by automation initiated by the delivery pipeline.  The solution’s 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 | The solution’s 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.  The solution allows the dynamic disabling of features that are in the code base, but not ready for use by end users.  The solution 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. | The solution SHOULD allow modification to one component or group of functionality with the least chance of affecting other parts of the solution. |  |  |  | The solution 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. | The solution 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+  The solution’s 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. |  |  |  | The solution 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

Table 9: Default System Portability Quality Requirements

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Response | Comments | Details | Questions |
|  | o **General** þ **Adaptability** þ **Installability** þ **Replaceability** | | | |  |  |  |  |  |
|  | **Adaptability** | | | |  |  |  |  |  |
|  | QR- DEF- POR- 00 | Default/ Portability/ Adaptability/ Configurability/ API | The solution **MUST** be configurable by API. | Deployment specialists must be able to configure system components via APIs invoked within a step after the deployment step in the deployment pipeline automation. |  |  |  | Whether Bought or Built, the components must be configurable via automation, reducing documentation needs, and protecting against loss of IP when resources leave the organisation. | Is the system configurable?  By deployed configuration file or API or both? |
|  | QR- DEF- POR- 00 | Default/ Portability/ Adaptability/ Configurability/ GUI | The solution **SHOULD** 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). |  |  |  |  | Is the system configurable by GUI? |
|  | QR-DEF-POR- 00 | Default/ Portability/ Adaptability | The solution MUST be able to adaptable by configuration, and not require another deployment. | Operations Specialists must be able to reconfigure the system to meet changing use case or constraints. |  |  |  | the solution has APIs and a user view to manage system configuration. |  |
|  | QR-DEF-POR- 00 | Default/ Portability/ Adaptability/ Hardware | The solution MUST NOT require specialised hardware or licensing or subscriptions to meet defined expectations without disclosure and agreement prior to procurement. | Specialised hardware, subscriptions or licenses may not be available for the full duration of the service lifespan. |  |  |  |  |  |
|  | **Installability** | | | |  |  |  |  |  |
|  | QR-DEF-POR- 00 | Default/ Portability/ Installability/ Rollback | A deployment of the solution MUST be able to be automatically rolled back upon failure or other reason. | the system's automated deployment processes ensure that a failed deployment can be reverted. |  |  |  | Preferably the deployment process is idempotent. |  |
|  | **Replaceability** | | | |  |  |  |  |  |
|  | QR-DEF-POR- 00 | Default/ Portability/ Installability/ Environments | The solution MUST include a number of non-PROD data environments. | In addition to a PROD Data environment, stakeholders must be able to test integration and inspect the system’s functionality in environments that contain non-PROD data. |  |  |  | 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 Deployment View for proposed environments. |  |
|  | QR-DEF-POR- 00 | Default/ Portability/ Installability/ Automated Environment Creation & Deployment | The solution MUST be able to create and deploy to any new environment, 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.) |  |  |  | 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 | The solution’s 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/ Dependencies | ‘Custom Code’ MUST be operating system agnostic. | Systems SHOULD be portable to different operating systems. |  |  |  | ‘Custom Code’ should be developed using cross-OS platform & frameworks (.NET Core, Python, etc.) preferably deployable to managed platforms (eg: PaaS) that remove the need to know the underlying OS. |  |
|  | QR-DEF-POR- 00 | Default/ Portability/ Installability/ Cloud Agnostic | ‘Custom Code’ MAY be cloud agnostic. | Modern systems link to and leverage off-device services (managed storage, caching, searching, etc.).  increases the that while common across many cloud vendors, are implemented differently in each – such that they are not portable without non-trivial rework. |  |  |  | It is understood that while lock-in is a risk that should be avoided when possible.  But the design of systems that avoid the use of easily available and managed cloud specific managed services, for the object of remaining portable between cloud providers should be treated with caution.  While containers *can* be moved between cloud providers, they will *still* be referencing service endpoints belonging to the original cloud provider. |  |
|  | QR- DEF- POR- 00 | Default/ Portability/ APIs | The system’s managed resources, metadata, relationships MUST be extractable by API. | The APIs should be specific to the task, REST-ful,  preferably Queryable.   Preferably adhering to domain specific standards if they are available. |  |  |  | The purpose is to avoid vendor lock in.  The APIs should be specific to extraction and importation needs, 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). |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| >>? | Notification/Change Notificaiton | Upcoming changes to the service MUST be communicated to the users. | To decrease avoidable support costs, Users should be to prepared for changes to the system. |  |  |  | Options to consider:  Using a notification service to notify subscribed end user.  Using a webpage to list changes done in the past and upcoming changes in the future.  Using a header banner message to direct them to the above page, etc. and stop it from reshowing the same message once it has been seen. |  |

# Default Internal Requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
| QR-DEF-MAIN-00 | Replaceability | The solution SHOULD allow the consolidation of the capabilities of one or more existing systems. | Consolidation of new solutions should be considered based on reducing complexity, improve maintainability of the organisation's system, decreasing cost. | NRN: this requirement cannot be answered by respondents. |  |  |

Maintainability

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| QR-DEF-MAIN-00 | Modifiability/Lockout | Any development or ongoing support contract prepared to deliver this solution MUST NOT exclude this organisation from actively participating in development and operations. | This organisation must not accept locking or lockout contractual conditions. | The solution’s automated pipeline, running unit tests, integration tests, behaviour tests are there to catch errors in logic before checkin branches are accepted and merged.  Any fixes required are the whole project team's responsibility, allocated to the group most knowledgeable as to the cause and resolution, dependent on availability. |  |  |
| QR-MT-B-06 | **Baseline** | **Maintainability/Accessible Code Repository** | Custom code, configuration or test scripts written for this solution **MUST** be maintained in an organisation accessible and clonable code repository. | Code written for this organisation must be analysable for code security and quality. |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| QR-DEF-MAIN-00 | Replaceability | The solution SHOULD allow the consolidation of the capabilities of one or more existing systems. | Consolidation of new solutions should be considered based on reducing complexity, improve maintainability of the organisation's system, decreasing cost. | NRN: this requirement cannot be answered by respondents. |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| QR-DEF-MAIN-00 | Reusability | The solution’s components MAY be reusable by other systems. | The cost benefits of reusing components and services must be weighed against the cost of complexity and cross-dependencies. | The solution’s components are re-using other solution's components.  This solution's components are envisioned as being reusable by other solutions. |  |  |

Training to stop checking in credentials.

# Conclusion

Appendices

Appendix A - Document Information

### Images

[Figure 1: Project Specific Tier of Quality Requirements 11](#_Toc149570784)

[Figure 2: Custom Developed Specific Tier of Quality Requirements 13](#_Toc149570785)

[Figure 3: Ministry Specific Tier of Quality Requirements 34](#_Toc149570786)

[Figure 4: Organisation Specific Tier of Quality Requirements 40](#_Toc149570787)

[Figure 5: Education Sector Specific Tier of Quality Requirements 47](#_Toc149570788)

[Figure 6: NZ Government Sector Specific Tier of Quality Requirements 51](#_Toc149570789)

[Figure 7: Default System Base Tier of Quality Requirements 62](#_Toc149570790)

### Tables

[Table 2: Table of Default System Security Quality Requirements 64](#_Toc149570774)

[Table 3: Default System Privacy Quality Requirements 77](#_Toc149570775)

[Table 4: Default System Functionality Quality Requirements 80](#_Toc149570776)

[Table 5: Default System Usability Quality Requirements 85](#_Toc149570777)

[Table 6: Default System Reliability Quality Requirements 100](#_Toc149570778)

[Table 7: Default System Performance Quality Requirements 109](#_Toc149570779)

[Table 8: Default System Maintainability Quality Requirements 115](#_Toc149570780)

[Table 9: Default System Portability Quality Requirements 129](#_Toc149570781)

### 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 |
|  |  |
|  |  |
|  |  |

### 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-repudiatable (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 correctly, accurately, and safely use the solution.

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.