# Document

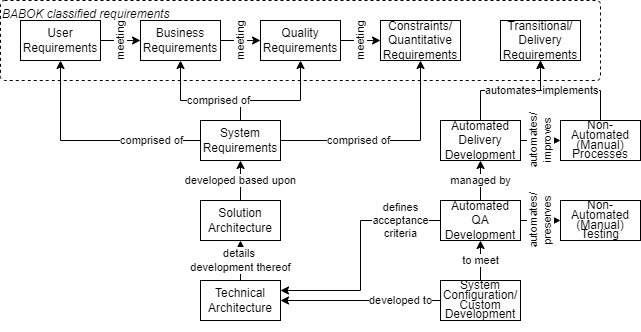
## Purpose

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.



## Structure

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

### Delivery Requirements Classification

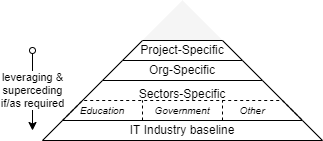
Requirements are organised according to the following delivery quality categories, covering both Delivery processes and the System being delivered.  
  
System specific requirements are organised according to ISO-25010 classification:



To avoid duplication, scope sections do not require requirements for each ISO-25010 classification, instead relying on a more general scope.

### Scopes

Within each of the above sections, Requirements are organised according to layered Scopes – starting with Project-Specific, followed by Organisation-Specific, Sectors-Specific, and Baseline/Generic industry requirements -- each section expanding or superseding one or more requirements in a more general scope.



**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.

## Content

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.

### 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.

### 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 an endorsable work around that can meet the same obligations and/or objectives.

### Acceptance Criteria

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

### Acronyms and Terms

Acronyms and terms used in this, and potentially reliant documents, are defined in the Appendices.

Key terms of specific meaning include:

* digital deliverables

# Quality Requirements

The ISO-25010 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.

## Integration Services

The Services are expected to integrate with the following organisation provided or approved 3rd party services:

* Identity:
  + Organisation (internal) User Identity Provider (AAD)
  + Organisation (sector) Identity Provider (ESL)
  + Organisation (external) public consumer Identity Provider
* Validation:
  + Organisation provided or approved Malware Detection Service
* Still to define clearly: handling of TENANCY, ORGANISATIONS, Resource Usage  
  Footers specifying Regulations (Rule 61/3, etc.)

## Baseline Custom Development Scope

Although not a certainty of every solution proposal, Custom Development *is* required for most solutions, in of one or more of the following forms: deployment pipeline development, pipeline run environment customisation scripting, automated pipeline run QA test development, integration development, data storage schema development, or system logic development.

Custom development of any kind is expected to be delivered in a transparent manner requiring the least effort to qualify, maintain and/or improve over the solution’s full lifecycle.

### SECURITY (ISO-25010/Security)

Security is a key quality defined under ISO-25010.

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

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

* Confidentiality is the degree to which the solution ensures data is accessible only by those authorised to do so.
* Integrity defines the degree to which the solution prevents unauthorised access, modification of systems and the information they manage.
* Non-Repudiation and Accountability are associated in that non-repudiation defines the degree to which the solution can prove that actions have been taken, and accountability is being able to associate the non-repudiable (audited) activity to a specific user.
* Authenticity defines the degree to which the identity of a user can be claimed.
* Availability – which is a prerequisite for Security 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.

| # | | State | | Title | | Statement | | Rationale |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| QRC02 | **Technical Baseline** | | **Security/APIs/DTOs** | | Service APIs **MUST** not expose the internal schema of entities or data storage schemas, by using mapping between internal system entities and DTOs at the Service Facade. | | Security requires that internal structures are not exposed.  Maintainability requires that changes to internal logic and entities does not cause changes to integration messages – DTOs – which would break contracts with established integrated systems. | |

### PORTABILITY (ISO-25010/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.

Note: Installability, is the most appropriate category to cover automation of delivery (ie, DevOps & SecOps).

| # | State | Title | Statement | Rationale |
| --- | --- | --- | --- | --- |
| TODO | **Technical Baseline** | **Delivery/ALM** | An ALM, accessible by all stakeholders, MUST be used to manage the automated delivery of custom digital deliverables to target environments. | The development of infrastructure, configuration, schemas, logic or data must be able to be influenced and followed by stakeholders. |
|  | **Technical Baseline** | **Delivery/Source Control** | A publicly accessible source control service MUST be used to persist custom digital deliverables. | All Infrastructure as Code, all Db[Schema] as Code, all Data seeding as Code, all custom logic as code, all QA Tests as Code is to be developed and persisted using a good practice protocol on an accepted source control service (eg: Git on GitHub, Git on ADO, etc.) |
| QRM08 | **Technical Baseline** | **Modifiability/ Loosely coupled** | Any custom development for the solution **SHOULD** prefer being developed using loosely coupled systems and components. | The solution SHOULD allow modification to one component or group of functionalities with the least chance of affecting other parts of the solution. |

### MAINTAINABILITY

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # | State | | Title | Statement | | Rationale | |
|  |  | |  |  | |  | |
|  | | | | | | | |
|  |  | |  |  | |  | |
|  | | | | | | | |
|  |  | |  |  | |  | |
|  | | | | | | | |
|  |  | |  |  | |  | |
|  | | | | | | | |
|  |  | |  |  | |  | |
| Industry Baseline Quality Requirements | | | | | | | |
|  |  |  | | |  | |  |
|  |  |  | | |  | |  |
|  |  |  | | |  | |  |
|  |  |  | | |  | |  |

### USABILITY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | State | Title | Statement | Rationale |
|  |  |  |  |  |
|  | | | | |
|  |  |  |  |  |
|  | | | | |
|  |  |  |  |  |
|  | | | | |
|  |  |  |  |  |
|  | | | | |
|  |  |  |  |  |
| Industry Baseline Quality Requirements | | | | |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Baseline Scope

### ACCREDITATION

As a government agency of New Zealand, services offered are constrained by the country’s laws, as well as some regulation that is specific to government agencies.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # | State | | Title | Statement | | Rationale | |
|  |  | |  |  | |  | |
| Project Specific Quality Requirements Scope | | | | | | | |
| TODO |  | |  |  | |  | |
| Organisation Specific Quality Requirements Scope | | | | | | | |
| N/A |  |  | | |  | |  |
| Education Sector Specific Quality Requirements Scope | | | | | | | |
| QRA01 | **Education** | **Legal obligations – Education Sector** | | | 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. |
| Government Scope Quality Requirements Scope | | | | | | | |
| *Note: As a government agency of New Zealand, services offered are constrained by the country’s laws, as well as some regulation that is specific to government agencies.* | | | | | | | |
| QRA01 | **Government** | **Legal obligations – Government Sector** | | | Services **MUST** comply with current legislation obligations:   * Public Records Act,   Official Information Act | | The solution is subject to the same laws that govern any other aspect of the country. Specifically, but limited to, the following considerations:   * Privacy: Security Breaches must be immediately reported to this organisation’s Privacy Officer and the Privacy Commissioner. Users must be informed of their Privacy rights. Users must be able to correct incorrect PII. * Public Records: For government transparency reasons, no data record must be physically deleted (only logically deleted),   OIA: the system must make it reasonably possible to respond to OIA Requests. |
| QRA02 | **Government** | **Regulation obligations** | | | Services **MUST** comply with obligations made to other agencies, including:   * National Archive’s directives for public data, * Declaration on Open & Transparent Government, * International Open Data Charter (2017), * NZ Data Content Standards, * NZ Digital Service Standards, * GDRP (2018),   NZ Government Web Standards (NZGWS). | | * Archiving: For government transparency reasons, no data record must be physically deleted (only logically deleted), * Data should be made available by API wherever it does not impact a Natural or Legal Person’s Privacy or weaken the solution’s security. * The solution’s interfaces must be usable by all forms of the visually impaired. * The solution interface media must be translatable into national written languages.   Dispensation for delays in meeting these obligations may be requested and may be temporarily granted, but it remains the vendors cost to remedy.  An Authority to Operate – which is required prior to a solution be deployed to PROD -- cannot be obtained without demonstrable proof that agreements have been upheld. |
| QRA03 | **Government** | **Regulated guidance** | | | Services **MUST** follow All of Government (AoG) guidance including:   * NZ Cloud First, * NZ Information Security Manual (NZISM) * NZ API Standards and Guidelines * NZ Data and Information Principles * NZ Data and Information Management Principles (NZDIMP),   NZ Government Access & Licensing (NZGOAL) | | * The solution must be hosted on cloud infrastructure where feasible at reasonable cost, * The solution must adhere to guidance provided for security, API design, copyright and data usage.   Dispensation for delays in meeting these obligations may be requested and may be temporarily granted, but it remains the vendors cost to remedy.  Issuance of an Authority to Operate is dependent on evidence that AoG guidance being adhered to --unless dispensation is obtained prior to Go-Live of the solution. |
|  |  |  | | |  | |  |
| Industry Baseline Scope Quality Requirements Scope | | | | | | | |
| QRA01 | **Baseline** | **Legal obligations –Baseline** | | | Services **MUST** comply with current legislation obligations:   * Privacy Act | | The solution is subject to the same laws that govern any other aspect of the country. Specifically, but limited to, the following considerations:   * Privacy: Security Breaches must be immediately reported to this organisation’s Privacy Officer and the Privacy Commissioner. Users must be informed of their Privacy rights. Users must be able to correct incorrect PII. |

### PORTABILITY (ISO-25010/Portability)

ISO-25010 defines 3 subcategories under Portability: Adaptability, Installability, Replaceability.

##### ISO-25010/Portability

| # | Scope | Title | Statement | Rationale |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| Project Specific Quality Requirements | | | | |
| TODO |  |  |  |  |
| Organisation Specific Quality Requirements | | | | |
| N/A |  |  |  |  |
| Education Sector Specific Quality Requirements | | | | |
| N/A |  |  |  |  |
| Government Sector Specific Quality Requirements | | | | |
| N/A |  |  |  |  |
| Industry Baseline Quality Requirements | | | | |
| QRD-B-01 | **Baseline** | **Portability/Start** | Customizable and deployable customisation, configuration, and/or custom code **MUST** be delivered by an automation pipeline to the production environment for end users to access within the duration defined in the *Target Quality Objectives* table. | Results, regularly reconsidered, must be the norm in order to decrease the risk of non-delivery. |
| QRD-B-02 | **Baseline** | **Portability/Delivery cadence to Prod-Data environment** | Customizable and deployable customisation, configuration, and/or custom code **MUST** be delivered and made available to end user stakeholders at a high cadence, as defined in the *Target Quality Objectives* table (approximately every 2 weeks). | High cadence permits regular testing of assumptions as to what is most important to stakeholders, putting results in front of them, allowing them redirecting subsequent effort based on new or simply refined requirements.  High cadence requires a reliance on automation to be able to manage compilation, deployment and testing in the short time frame.  Automation is a key component of an appropriate DR and testing IP retention over the project's lifespan. |
| QRD-B-03 | **Baseline** | **Portability/Iterative development**  **of Deployment Pipeline** | Customizable and deployable customisation, configuration, and/or custom code **MUST** be delivered via a pipeline that is iteratively improved to automate all compilation, environment development, deployment, configuration, data restoration, integration and testing: unit, integration and functional/behavioural testing. | The automated delivery pipeline is a system in its own right – if not the *actual* deliverable – which requires its own iterative design, development, testing, maintenance and improvement. |
| QRD-B-04 | **Baseline** | **Portability/Deliverability/Automated Environment creation & deployment** | Customizable and deployable customisation, configuration, and/or custom code **MUST** use a pipeline that first creates and deploys new environment created solely by automation: - BuildTest (BT), DevTest (DT), System Test (ST), User Test (UT), Integration (INT) for external clients to test their API integration, and PROD – and compilation, testing and deployment thereto.  If a pipeline is possible, the automated deployment pipeline must address:   * Compilation, * Running Unit tests, * using Infrastructure as Code to build environments, * Backup the target Data before deployment, * Backup (or locate) the previous deployment package, * Deployment of the current package, * Injection of Configuration settings retrieved from secure storage, * updating Db schemas using Database schemas as Code, * Automatic wakeup of deployment websites * Automated backups of data, * Automated Data Restoration (if Prod), * Running Integration and Functional Tests * Optionally configuring of Automated Migration of Data to other systems (either drop/pickup areas, or APIs of external Data warehouse, SIEMs, etc.) * Upon failure of any tests, roll back the deployment, restore the previous package, restore the previous database backup,   The solution must backup before commencing a rollout, rollback failed deployments, restoring the previously deployed instance. | In order to support Maintainability & Availability quality objectives, the solution must be able to be tested and deployed rapidly. In the event of a disaster, a solution must be able to be rebuilt quickly from scratch.  Minimise the chance that failed deployments make the solution unavailable for significant amounts of times. |
| QRD-B-05 | **Baseline** | **Portability/Tests Definitions first** | Customizable and deployable customisation, configuration, and/or custom code, work items (i.e., development/configuration tasks) **MUST** be completed with test scripts before any customisation and/or development begins – first with automating the test scripts into the deployment pipeline, then developing the system’s logic to pass the pipeline’s automated tests. | Developers must know what they are aiming for, rather than developers and testers both interpreting the intent of Business Analysts separately, putting in the effort to do their individual tasks, only to find out at the end they disagreed as to the BA’s intent. |
| QRD-B-06 | **Baseline** | **Portability/Requirement volatility** | The solution’s functional and quality requirements **MUST** be able to evolve by mutual consent. | As the cone of uncertainty inherent with the beginning of projects decreases, it is natural that requirements need adjustment. The process of coming to an agreement should be rapid and straightforward. |
| QRD-B-07 | **Baseline** | **Portability/Application Lifecycle Management Suite** | Unless agreed otherwise, the solution implementation personnel **MUST** use the organisation endorsable Application Lifecycle Management (ALM) (Azure DevOps) to integrate Work Item Management, Configuration and Customisation code repositories, Workflow Management, Integration and Deployment services, testing services. | It’s difficult enough to integrate a system that is to be delivered to prod.  The long-term maintainability of the service should not depend on having to keep integrating and testing the tools used to manage the discovery, definition, design, development, deployment, defect fixing. Use a Suite that already delivers this, and is used by this organisation’s operations, support and implementation teams. |
| QRD-B-08 | **Baseline** | **Portability/Staff** | 1/3 of provided resources **MUST** have demonstrable relevant senior experience, optionally be certified in the solution’s technologies, and be vetted and accepted by this organisation. | Successful delivery of projects is largely dependent on the attitude, capabilities, and experience of resources involved. |
| QRD-B-09 | **Baseline** | **Portability/Avoid Redevelopment** | Redevelopment **MUST** be minimized. | Correctly managed projects ensure correctness, clarity, and achievability of work items so as to enable understanding and execution without unnecessary correction.  Unless agreed otherwise, corrections and repetition of effort avoidable by automation are at the cost of the solution provider. |

### FUNCTIONALITY (ISO-25010/Functionality)

Functionality is a key quality defined under ISO-25010.

| # | Scope | Title | Statement | Rationale |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| Project Specific Scope Quality Requirements | | | | |
|  |  |  |  |  |
| Organisation Specific Scope Quality Requirements | | | | |
| N/A |  |  |  |  |
| Education Sector Quality Requirements | | | | |
| N/A |  |  |  |  |
| Government Sector Quality Requirements | | | | |
| N/A |  |  |  |  |
| Industry Scope Baseline Requirements | | | | |
| QRF-B-01 | **Baseline** | **Functionality/Completeness** | Service analysis and functionality MUST address equally and regularly the needs of all key stakeholder groups, including the following stakeholder groups:   * Business Owner Stakeholder, * Test Analyst Stakeholders, * Customer User Stakeholders * Business Specialist Stakeholders * Customer Support Stakeholders * Operations Specialist Stakeholders * Monitoring Specialist Stakeholders * Security Specialist Stakeholders * Maintenance Specialist Stakeholders * Infrastructure Specialist Stakeholders | 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. |
| QRF-B-02 |  | **Functionality/Completeness** | Services **MUST** provide functionality to support the following key capabilities:   * System Management, via:   + Diagnostics   + Errors Reports   + Configuration     - Host Device     - Integration     - System * User & Group management, via:   + Users     - User Profile/Preferences   + User Groups   + Role Permission Assignment   + User Group Role Invitation   + Group Role Provisioning/ Acceptance Workflow Management, * User Session Management, via:   + Session Management   + Session Operations * Record, Resource & Collection Management, via:   + Discovery Metadata Management,   + Access Rights Management,   + Collaboration Roles Invitations & Management,   + Role Provisioning/Acceptance Workflows |  |
| QEF-B-03 | **Baseline** | **Correctness** | Work Items to deliver configuration and/or customisation MUST be broken down into achievable Testable Tasks before development commences. | User Story Work Items are stakeholder Defined Desires, and therefore loaded with Ambiguity, leading to redevelopment and unnecessary cost. User Stories must be broken down into singular SMART Tasks, each with one or more QA test definitions, before development starts.  The Tests prove the Correctness of the Statements before Development begins. |

### SECURITY (ISO-25010/Security)

Security is a key quality defined under ISO-25010.

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

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

* Confidentiality is the degree to which the solution ensures data is accessible only by those authorised to do so.
* Integrity defines the degree to which the solution prevents unauthorised access, modification of systems and the information they manage.
* Non-Repudiation and Accountability are associated in that non-repudiation defines the degree to which the solution can prove that actions have been taken, and accountability is being able to associate the non-repudiable (audited) activity to a specific user.
* Authenticity defines the degree to which the identity of a user can be claimed.
* Availability – which is a prerequisite for Security 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.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # | State | | Title | Statement | | Rationale | |
|  |  | |  |  | |  | |
| Project Specific Requirements Scope | | | | | | | |
| TODO |  | |  |  | |  | |
| Organisation Specific Quality Requirements Scope | | | | | | | |
| QR-SC-O-01 | **Organisation** | | **Security/Accreditation** | Services **MUST** complete and achieve security Certification and Acceptance (C&A) get approved by the CAB board and receive an Authority to Operate prior to first time deployment to PROD.  Important: Evidence of the above for products – as opposed to custom development – is required prior to contract.  *Note: Custom development design and technologies are verified for current design patterns, as well as the use of the latest version of current and supported components and technologies.* | | 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 (such as the latest version of the NZISM). | |
| Education Sector Quality Requirements Scope | | | | | | | |
| N/A |  | |  |  | |  | |
| Government Sector Quality Requirements Scope | | | | | | | |
| *Note all government agencies digital services must implement NZISM controls to mitigate ascertained risks.* | | | | | | | |
| QR-SC-G-01 | **Government** | | **Security/Integrity/Data Classification** | Services **MUST** use NZISM recommended security and risk mitigations controls appropriate to the system's NZ government data classification, as defined in the *Target Quality Objectives* table. | | A system must apply applicable NZISM recommended and /or organisation C&A accepted safety and risk mitigation controls to safely persist user provided data. | |
| QR-SC-G-02 | **Government** | | **Security/Integrity/Firewalls & WAFs** | As per NZISM recommendations, Services **MUST** be protected by a Web Access Firewalls (WAF), maintained to address current threats, while not negatively impacting end user experience. | | Firewalls limit the surface of attach to a single (web) port, and WAFs analyse web traffic for abnormal behaviour and intrusion.  *Note: The solution’s WAF should be configured to flag & allow through media containing malware so that the service’s malware detection service can analyse the upload and return a system error (as opposed to a WAF generated error).* | |
| Industry Baseline Quality Requirements | | | | | | | |
| QR-SC-B-01 | **Organisation** | **Security/C&A** | | | Services MUST undergo a security assessment as part of the organisation’s C&A process. | | A security assessment by an independent service is required as part of the organisation’s C&A process, which is a prerequisite for CAB to recommend the CDO issue an ATO, required to operate in a PROD-DATA environment. |
| Industry Baseline | | | | | | | |
| QR-SC-B-02 | **Baseline** | **Security/Integrity/Encryption in Transit** | | | Services **MUST** protect user-submitted information in transit between all components, devices and tiers, using the latest TLS encryption over HTTPS or protocol-equivalent where available. Where channel encryption is not available, message encryption is appropriate. | | To receive accreditation for a production environment, this organisation’s systems are assessed against NZISM’s recommendations according to the data’s security classification as per the *Target Quality Objectives* table. |
| QR-SC-B-03 | **Baseline** | **Security/Integrity/Encryption at Rest** | | | Services **MUST** protect both user-generated information and configuration credentials at rest (e.g., databases, blob, diagnostics trace files, configuration entries within system config files etc.), by using encryption (up to but excluding requiring certificate deployment). | | To receive accreditation for a production environment, this organisation’s systems are assessed against NZISM’s recommendations according to the data’s security classification as per the *Target Quality Objectives* table. |
| QR-SC-B-04 | **Baseline** | **Security/Integrity/Access Limitations** | | | Any location where Production data is persisted **MUST** adhere to ISO-27001 level 2+ limiting physical, virtual and remote access, copying or removal of stored data – and auditing any access that did occur.  Access to data is granted to deployment service accounts, and must exclude access by Developers, Testers, BAs. Optimally also including Operations specialists. | | 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. |
| QR-SC-B-05 | **Baseline** | **Security/Integrity/External PII Management Services** | | | Services **MUST** collect the least amount of Personally Identifiable Information (PII) required to function correctly and persist it in encrypted database columns or an external specialised and hardened storage service. | | The less PII information maintained in a solution, the smaller the attack surface a solution has.  A key reason PII information is encrypted or persisted separately is to minimise risk of data leakage when data is copied to a reporting database and/or data warehouse.  Note that encrypted columns often incur a higher DBMS licensing cost, whereas merging incurs more development cost. |
| QR-SC-B-06 | **Baseline** | **Security/Integrity/External Identity Provider Services** | | | Services **MUST** use external Identity Provider Services to persist UI and API User Credentials, maintained to use the latest versions of current protocols (OIDC, OAuth). | | The less secrets maintained in a solution, the less attack surface has. |
| QR-SC-B-08 | **Baseline** | **Security/Integrity/Clear Text Credentials** | | | Services **MUST NOT** transmit clear text credentials, even over encrypted channels. | | Channels pass through devices that may strip off encryption, log traffic, before re-attaching new encryption. |
| QR-SC-B-09 | **Baseline** | **Security/Integrity/Encrypted at Rest/Sensitive Configuration Parameters** | | | Services **MUST** retrieve encrypt any persisted sensitive configuration information in external secure key storage services accessed only by automated pipeline service accounts, or provide an agreed similarly secure mechanism for persisting and accessing sensitive configuration information.  Where the use of an external configuration information service is not possible, encryption is used when persisting it.  Where encryption is not possible, the credential is referenced in the project’s risk registry. | | 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. |
| QR-SC-B-10 | **Baseline** | **Security/Integrity/Encrypted at Rest/Sensitive Configuration Parameters/Setting** | | | Services **MUST** source confidential configuration credentials from confidential storage services and re-encrypt them and inject them into config files without human handling of confidential information. | | 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. |
| QR-SC-B-11 | **Baseline** | **Security/Integrity/Secure Development Practices** | | | The solution’s source code repository **MUST** be protected from stakeholders committing any security credentials or environment specific information.  If credentials and/or environment specific properties are checked in, steps must be taken to:   1. remove the credentials from the code repository and 2. rotate the credentials so the information is no longer a potential risk. | | 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.  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-SC-B-12 | **Baseline** | **Security/Integrity/Certificate Lifespans** | | | Services **MUST** limit the duration of certificates to short lifespans, as per the *Target Quality Objectives* table, by automated creation and deployment of certificates. | | The shorter the duration certificates are used, the less time bad actors have to crack the certificates. |
| QR-SC-B-13 | **Baseline** | **Security/Integrity/Service Accounts** | | | Services **MUST** run under individual service accounts, either developed on the fly by automation or beforehand by the organisation's operation specialists.  *Note: Consider using Microsoft Secure Identities (MSI) or a cloud provider equivalents.* | | Use of a single service account, creates a single point of failure that if compromised provides access to multiple components. |
| QR-SC-B-14 | **Baseline** | **Security/Integrity/Client Credentials** | | | Services **MUST NOT** rely on or deploy credentials to external clients. | | Credentials that are deployed and persisted outside a system’s infrastructure are compromised. |
| QR-SC-B-16 | **Baseline** | **Security/Integrity/Authorisation/Permission based** | | | Services **MUST** be Permission based, and assigned directly to Users, or more commonly to Roles, which are in turn assigned to Users.  *Note: Removal/De-assignments of Permissions take precedence over Assignments of Permission.* | | Roles are descriptions of a person's activities, but do not allow fine grain control. |
| QR-SC-B-17 | **Baseline** | **Security/Integrity/Authorisation/Obligations based** | | | Services **SHOULD** require Responsibilities & Obligations be digitally accepted by Users before they are assigned a Role’s Permissions.  *Note: These can be assigned to Users and Roles the same way as Permissions.* | | Roles are a combination of accepted Responsibilities (SHOULDs) & Obligations (MUSTs) in return for Permissions (MAYs).  Adding them to Role definitions makes Invitation to Group or Resource Roles by Notification possible to be automated. |
| QR-SC-B-18 | **Baseline** | **Security/Integrity/Authorisation/Group-specific Groups Roles** | | | Services **MUST** be capable of assigning group-specific roles definitions (e.g.: a single Accountable, Administrators, Approvers, Group Contact Person, Members, Collaborators, Guests). | | A user may belong to different groups, in different capacities/roles (Owner in one, Member in another, etc.). |
| QR-SC-B-19 | **Baseline** | **Security/Integrity/Authorisation/Group Specific Resource Roles** | | | Services **MUST** be capable of associating Users to Resources, in different group-specific Roles definitions (e.g.: Accountable/Owner, Collaborators, Reviewers, Approvers, Administrators/Publishers, Guests).  *Note: The solution’s Inheritable Group configuration settings will determine if resources that belong to a group inherit default roles from the group.* | | A resource can be commenced, collaborated on, approved, published and managed by different users. |
| QR-SC-B-20 | **Baseline** | **Security/Integrity/Least Privilege** | | | Services **MUST** allow solution and business group administrators to attribute to end users the least amount of privilege needed to perform their tasks without frustration. | | Limit unauthorised activity (accidental or otherwise). |
| QR-SC-B-21 | **Baseline** | **Security/Integrity/Firewalls & WAFs** | | | Services **MUST** be protected by an Web Access Firewalls (WAF), maintained to address current threats.  *Note: The solution’s WAF should be configured to flag & allow through media containing malware so that the service’s malware detection service can analyse the upload and return a system error (as opposed to a WAF generated error).* | | Firewalls limit the surface of attach to a single (web) port, and WAFs analyse web traffic for abnormal behaviour and intrusion. |
| QR-SC-B-22 | **Baseline** | **Security/Integrity/Sanitised Queryable Logs** | | | Operation audit, error, debug and access logs **MUST** be protected from tampering, loss.  Entries must be protected from disclosure by being sanitised and cleansed of confidential information. Entries must be queryable pageable, sortable , filterable via API & Interface.  *Note: Temporal diagnostic logs are not to be used as permanent audit logs.* | | Audit logs of session operations are used by security specialists towards accountability objectives. Diagnostics & Error logs are queried by Support specialists to return prompt service to Support Specialists. |
| QR-SC-B-23 | **Baseline** | **Security/Integrity/Key Management** | | | The solution design and operational processes **MUST** demonstrate appropriate encryption key management. | |  |
| QR-SC-B-24 | **Baseline** | **Security/Integrity/Compartmentalised Defence in Depth** | | | Services **MUST** remain secure if a component, layer or tier's security is breached, using encrypted communication, port protection via Firewalls, WAFs based intrusion detection, authentication, least-privilege authorisation, protecting against DoS via dynamic horizontal scaling, session activity monitoring & alerting, session activity auditing, encryption at rest, system hardening, ISO-27001 Level2+ physical access controls. | | Multiple layers of security slow the progress of attackers. |
| QR-SC-B-25 | **Baseline** | **Security/Integrity/OWASP** | | | Services **MUST** address and demonstrate application of the Open Web Application Security Project (OWASP)'s recommended mitigation of the latest Top Ten Application Security Risks:   * injection * broken authentication * sensitive data exposure * broken access controls * security misconfiguration * cross site scripting (XSS) * cross site request forgery (CSRF) * insecure de-serialisation * using components with known vulnerabilities | | Rely on a reputed source of current knowledge regarding web application vulnerabilities in order to pass a third-party validation of the system's security. |
| QR-SC-B-26 | **Organisation** | **Security/Integrity/security Incidents** | | | The solution **MUST** support Ministry endorsed security incident processes to inform stakeholders and users within *Target Quality Objectives* table defined delays as to risks, activities being undertaken, time to recovery & resolution. | | 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. Note: The process will align with the Privacy Commissioner’s expectations and the Privacy Act. |
| QR-SC-B-27 | **Baseline** | **Security/Confidentiality/ Production Data** | | | Production Data **MUST NOT** be made accessible outside of the Production Environment and Production data backup environment.  Access to Production Data, whether in a PROD data system or a backup, must be restricted to only service accounts. | | The less people who have access to information the less chance of data being divulged by accident or intent. |
| QR-SC-B-28 | **Baseline** | **Security/Confidentiality/ Production Data Backup** | | | If deployed, Production Data Backups **MUST** be separated from Non-Production Data backup environments. | | Backups *are* production data – just from a point in time in the past – and should be protected as completely as production data. |
| QR-SC-B-29 | **Baseline** | **Security/Non-Repudiation & Accountability** | | | Services **MUST** permanently store remotely queryable, filterable, pageable, audit records of all operations within a session, in order to correctly ascertain the process by which information was changed.  *Note: A User may have multiple Sessions, begun from different Devices and/or browsers. A Session begins on first interaction with the system, and may be associated to an Anonymous User, re-associated to an identified User later.*  *Background system operations are associated to a System Daemon user’s session.* | | 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.). |
| QR-SC-B-30 | **Baseline** | **Security/Accountability/Multiple Digital Identities** | | | Services **SHOULD** allow a user to associate multiple digital Identities to their system user's record, sourced from different social IdPs (MS Accounts, Google Accounts, etc.) and organisation IdPs (Azure AD). | | Users belong to multiple organisations (schools, organisations, groups) each of which may have their own Identity Provider Service.  A user should be able to use either identity to sign in.  But also be able to keep them separate as different Users, if they so require. |
| QR-SC-B-31 | **Baseline** | **Security/Accountability** | | | Services **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. |
| QR-SC-B-32 | **Baseline** | **Security/Authenticity** | | | Services **MUST** correctly ascertain the identity of system users using external Identity Providers. | | The basis of allowing access to users is knowing who they are. |
|  |  |  | | |  | |  |

### PRIVACY

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | State | Title | | Statement | | Rationale |
|  |  |  | |  | |  |
| Project Specific Quality Requirements Scope | | | | | | |
| TODO |  |  | |  | |  |
| Organisation Specific Quality Requirements Scope | | | | | | |
| N/A |  |  | |  | |  |
| Education Sector Quality Requirements Scope | | | | | | |
| N/A |  |  | |  | |  |
| Government Sector Quality Requirements Scope | | | | | | |
| QR-PV-G-01 | **Baseline** | **Privacy/ Acts** | | Services **MUST** adhere to the applicable Acts outlined under the *Target Quality Objectives* Table.  Note: Refer to the linked AoG Principles, which outline data and information handling constraints. | | The solution must meet legal obligations before being accreditable to be delivered as a service by this organisation. |
| Industry Baseline Quality Requirements | | | | | | |
| QR-PV-B-01 | **Baseline** | | **Privacy/ Minimum PII** | | Services **MUST** collect the minimum amount of PII to meet its functionality expectations and persist it in a separate secure data store. | 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. |
| QR-PV-B-02 | **Baseline** | | **Privacy/ PII Scope** | | 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-PV-B-03 | **Baseline** | | **Privacy/ Correction** | | Services **MUST** allow users to self-correct their own PII. | Users know themselves best. |

### USABILITY (ISO-25010/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 Ministry 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | State | Title | Statement | Rationale |
|  |  |  |  |  |
| Project Specific Quality Requirements Scope | | | | |
| TODO |  |  |  |  |
| Organisation Specific Quality Requirements Scope | | | | |
| Note cost to organisation is decreased by users being simple enough for users to not require assistance. | | | | |
| None |  |  |  |  |
| Education Sector Quality Requirements Scope | | | | |
| Note the average age of sector staff is high compared to other industries. | | | | |
| None |  |  |  |  |
| Government Sector Quality Requirements Scope | | | | |
| None |  |  |  |  |
| Industry Baseline Quality Requirements | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TODO | Organisation | Usability/Recognisability | Interfaces MUST be kept styled as per organisation style guidelines. | All custom Interfaces to be developed following organisation defined guidelines and constraints to provide visual recognisability, and cohesion with other services provided. |
| TODO | **Organisation** | **Usability/ Recognisability** | Interfaces **MUST** be kept styled as per organisation style guidelines. | All custom Interfaces to be developed following organisation defined guidelines and constraints to provide visual recognisability, and cohesion with other services provided. |
|  |  | **Usability/Operability/Mobile** | End user facing custom developed user interfaces **MUST** be web and mobile capable web pages (preferably following PWA SPA development practices), using device sensors and services where available. | Services must be accessible and easily usable via Mobile devices.  The solution must take advantage of the devices and sensors available in a device to provide a better user experience (based on location, etc.) |
| QR-UB-B-03 | **Technical Baseline** | **Usability/Operability/BREAD Interfaces** | Custom developed user interface flows **MUST** be developed according to the Browse/Read/Edit/Add/Delete (BREAD) design patterns to improve recognisability, learnability and operability. | Using a commonly recognised pattern consistently throughout a system improves usability and decreases navigation and data entry error. |
| QR-UB-B-12 | **Baseline** | **Usability/Operability/Localisation** | All UX text and images other than user submitted media **MUST** be translatable and able to be persisted in Culture packs.  The solution should handle different layouts & orientation per culture, if required. | The NZ Realm is composed of multiple cultures and should be inclusive to all.  The first cultures to address with this requirement are those implicit in The Treaty – both the English and Māori cultures. |
| TODO | **Baseline** | **Usability/Positive** | Gathered feedback by end users MUST be mostly positive. | An agreed percentage of feedback received must be positive as opposed to negative. |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| No. | Function | Description | Desirability | Rationale | Pilot Fit Criterion | Production Fit Criterion |
|  |  |  |  |  |  |  |
| EX-01 | Appearance | The user interface appearance shall reflect the strength based new entrant teaching environment | Must | The user interface subtly reinforces teachers’ knowledge and understanding of mokopuna learning environment | * Pilot survey shows that [x%] of users have positive feedback | * Affirmative feedback in pilot survey |
| EX-07 | In-platform notification | The platform shall be able to send users in-platform notifications  User story ref [insert] | Must | To support the notification functionality |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Scope | Title | Statement | Rationale |
|  |  |  |  |  |
| Government Specific Scope | | | | |
| QR-UB-G-02 | **Government** | **Usability/Recognisability/NZ WAG** | Any service UX element **MUST**  meet NZ Government Web Standards – both the Web Usability Standards and Web Accessibility Standards. | The solution MUST be operable by the widest range of users.  All NZ Government web services MUST use similar branding layout and structure. |
| QR-UB-G-01 | **Government** | **Usability/Languages/NZ** | The service MUST be accessible to National language speakers. | The solution must be accessible to both English and Māori users. |
| Baseline Industry Scope | | | | |
| QR-UB-B-01 | **Baseline** | **Usability/Operability/Mouse** | The System MUST be usable without a Mouse | The requirement is a prerequisite for permitting visually impaired users to use the system. |
| QR-UB-B-02 | **Baseline** | **Usability/Operability/Language** | The System MUST be user configurable to be operable in one of multiple languages. | The system must be accessible to more than just English language speakers. |
| QR-UB-B-03 | **Baseline** | **Usability/Operability/Instructions/Non-technical** | The System’s Instructions (interface text, alerts, warnings, notifications, etc.) MUST be easy to understand by non-technical users. |  |
| QR-UB-B-04 | **Baseline** | **Usability/Configurability** | Any services’ mutable system configuration values **MUST** be configurable via API and 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. |
| QR-UB-B-05 | **Baseline** | **Usability/Learnability/Undo** | Services **MUST** allow users to undo Operations, by using Logical versus Physical state changes (e.g.: Deletion of records), and queuing & delaying external operations (sending notifications). | Users make mistakes. Beyond being and embarrassing and frustrating experience, having support specialists on call to undo mistakes, and designing a system to provide the necessary permissions on behalf of users, is expensive. |
| QR-UB-B-06 | **Baseline** | **Usability/Sessions/Multiple** | A user MUST be able to initiate multiple concurrent sessions. | The system must permit a user to use it from a desktop at the same time as cell phone. |
| QR-UB-B-07 |  | **Usability/Session/Duration** | A User’s Session maximum duration MUST be configurable (eg: 20 minutes to eg: 30 days). | A user should not be required to unnecessarily sign back in while working. |
| QR-UB-B-08 | **Baseline** | **Usability/Learnability/Training** | Services **MUST** be intuitive enough to not require users to undergo training to use the solution. | 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 on to resolve an in adequacy in usability that was already paid to vendors to resolve in the first place. |
| QR-UB-B-09 | **Baseline** | **Usability/Operability/Malware Detection** | Services **MUST** protect users from downloading malware by inspecting uploaded media for malware.  The solution **SHOULD** use a 3rd party service to inspect uploads, returning informative messages if required. | The reputation of the organisation is dependent on users trusting its services to do them and their group or organisation no harm. |
| QR-UB-B-10 | **Baseline** | **Operability/User Management** | Services **MUST** not rely on 3rd party services to manage users, groups, permissions or roles. | Users closest to work are in the best place to make decisions of whom they wish to work with. |
| QR-UB-B-11 | **Baseline** | **Operability/Web Browsers** | Services **MUST** be operable from the widest range of current devices, and 2 latest automatically deployed versions of the 3 most common browser technologies (Edge, Chrome, Safari). | The solution SHOULD be accessible from corporate and popular cell phone devices, using current browsers. |
| QR-UB-B-12 | **Baseline** | **Universality** | Services **MUST** by default handle Unicode persistence, UTF-8 transmission, UTC date times, UUID identifiers, and case insensitive, macron/diacritic insensitive phonetic matching.  *Culturally aware* phonetic search is a real added benefit. | The solution must persist and transmit universal data. |
| QR-UB-B-13 | **Baseline** | **Search** | 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 precaution against DOS resource consummation attacks. |
| QR-UB-B-14 | **Baseline** | **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). |
| QR-UB-B-15 | **Baseline** | **Reportability/ Channels** | Services **MUST** be capable of developing both on-screen and independently developed 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. |
| QR-UB-B-16 | **Baseline** | **Alerts/Abnormal Behaviour** | Services **MUST** be capable of monitoring for and alerting to abnormal behaviour by time, volume, source, illogical activity flows.  3rd party devices (e.g., WAF) may be used. | Alerting operations and/or security specialists early can allow them to defend a system against manual or automated access to data. |
| QR-UB-B-17 | **Baseline** | **Alerts/Errors** | Services **MUST** be capable of alerting subscribed users of errors. | Errors should be flagged to stakeholders who can analyse error reports and action any required resolution of the logged problem. |
| QR-UB-B-18 | **Baseline** | **Error Protection/ Meaningful Messages** | Services **MUST** inform the end user in generic plain language of any failure (e.g., network, 3rd party service, data storage, application logic, user authentication, resource location) that caused the request to not complete successfully.  Messages are sanitised of PII or confidential credentials before persistence or presentation.  Where possible Error Messages should providing correct steps to take to exit an error state.  A unique ID (e.g., UUID) should be assigned to the error log and displayed to the end user to ease interactions with Support Specialists. | Informing users of the category of the error may help inform conversations they may have with support services. |
| QR-UB-B-19 | **Baseline** | **Validation** | Services tier **MUST** validate all input at the Service Facade.  *Note that the solution service client repeats the validation to provide a better user experience.* | The solution must use a common validation approach irrespective of the Service Client used. |
| QR-UB-B-20 | **Baseline** | **Documentation** | Services **MUST** be accompanied with enough documentation for all components to be deployed, maintained and operated by revolving resources over the solution’s service lifespan. | Developers and testers are not expected to stick with the project for the service's lifespan.  In order to ensure their knowledge is not lost, documentation within a wiki is desirable.  Better yet, automated tests that demonstrate how the system works should be developed prior to beginning work items. |
| QR-UB-B-21 | **Baseline** | **Printed Resources** | 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.  Note: It is common that Resources are developed using print-focused style sheets, but it would preferred that the resources are developed into rich text (e.g., PDF) for better quality print artefacts. | Although a need that is diminishing in a digital era, there is still value in having physically distributable artefacts of information. |
| QR-UB-B-22 | **Baseline** | **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. |

### COMPATABILITY (ISO-25010/Compatibility)

Compatibility and Interoperability is the ability for the solution to interact with other systems by providing services to, or accepting services from, the other systems. This interaction could be any combination, as appropriate, of systems that are internal or external to the Ministry, existing or proposed. Interaction should demand minimal work on the new system and rework on existing systems. It should be isolated so that it is not 100% dependent on such interaction. It is also known as system integration, interaction and compatibility while maintaining independence.

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

* *Coexistence* is the degree to which a product can perform its required functions efficiently while sharing a common environment and resources with other systems, without detrimental impact on other systems.
* *Interoperability* is the degree to which two or more solutions, systems, components can exchange information and use the information that has been exchanged.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| # | | State | Title | | | Statement | Rationale | |
|  | |  |  | | |  |  | |
| Project Specific Quality Requirements Scope | | | | | | | | |
| TODO | |  |  | | |  |  | |
| Organisation Specific Quality Requirements Scope | | | | | | | | |
| NONE | |  |  | | |  |  | |
| Education Sector Quality Requirements Scope | | | | | | | | |
| NONE | |  |  | | |  |  | |
| Government Sector Quality Requirements Scope | | | | | | | | |
| NONE | |  |  | | |  |  | |
| Industry Baseline Quality Requirements | | | | | | | | |
| QR-CP-E-01 | **Organisation** | | | **Compatibility/Integration/ Organisation Website** | Media MUST be developed for the organisation’s main website to redirect it to the PROD-DATA environment’s implementation of digital services. | | | To improve discoverability, the service must be described and linked to from the organisation’s website. Media (text and images) in languages available on the organisation’s main website is required. |
| QR-CP-E-02 | **Organisation** | | | **Compatibility/Integrity/External Identity Provider Services/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-CP-E-03 | **Organisation** | | | **Integration/Provisioning/Users/JIT** | Services MUST be capable of processing IdP issued attributes at Session start to provision first time users just in time (JIT). | | | The creation of system users should not require manual provisioning tasks. |
| Education Sector Specific Scope | | | | | | | | |
| QR-CP-E-01 | **Education** | | | **Compatibility/Interoperability/Education Sector Authoritative Systems** | Services that require sector information **MUST** integrate with and source records from the sector’s available authoritative systems:   * 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). | | | Systems must not duplicate the collection of available authoritative information, decreasing data quality and increasing user workload. |
| QR-CP-E-02 | **Education** | | | **Compatibility/Interoperability/**  **Ed Sector Protocols & Formats** | Services **MUST** exchange data with authoritative education systems using the latest version of the system appropriate education industry standard:   * SCORM * cmi5 * LTI * NZSIF   Common Cartridge | | | For improved interoperability and whole sector usability, information must be shared using education sector appropriate and endorsed formats and protocols. |
| Baseline Specific Scope | | | | | | | | |
| QR-CP-B-01 | **Baseline** | | | **Compatibility/Integration/ Organisation Website** | Media MUST be developed for the organisation’s main website to redirect it to the PROD-DATA environment’s implementation of digital services. | | | To improve discoverability, the service must be described and linked to from the organisation’s website. Media (text and images) in languages available on the organisation’s main website is required. |
| QR-CP-B-02 | **Baseline** | | | **Compatibility/Integration/IdP** | Services **MUST** integrate with an external IdP for validation of user Identities. | | | The service must avoid persisting Personal Credentials -- whether plaintext, encrypted, hashed – and prefer relying on an external dedicated service to perform this specialist task. |
| QR-CP-B-03 | **Baseline** | | | **Compatibility/Integration/Systems of Records** | Services MUST integrate with organisation or sector Systems of Records as required to perform business operations. | | | The system must not duplicate the collection of records that are already available via integration with authoritative sources.  Note: see above for Sector, Organisation and/or Project specific clarification requirements. |
| QR-CP-B-04 | **Baseline** | | | **Compatibility/APIs** | Services **MUST** expose all core elements and functionality by externally & appropriately accessible APIs, including:   * 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 * Resource User Role Assignments * Resource Permission Role Assignments, * Resources * Resource Collections * Search | | | The solution must be in accordance with this organisation's API-First design Principles and enable flexibility around future integration and channel strategy requirements.  The Ministry’s API-First design principles means that functionality of a system must be available by API with or without also having a user interface to simplify their handling. |
| QR-CP-B-05 | **Baseline** | | | **Compatibility/APIs/Queryability** | APIs **MUST** be queryable, using either ODATA, and/or optionally GraphQL. | | | To decrease development effort and complexity, and improve modularity and reuse. |
| QR-CP-B-06 | **Baseline** | | | **Compatibility/API/SCIM** | Services **MUST** be able to provision users and groups via a standards-based provisioning API (SCIM protocol or equivalent).  *Note: these APIs are in addition to the base APIs provided to manage users, groups, etc.* | | |  |
| QR-CP-B-07 | **Baseline** | | | **Compatibility/APIs/SDKs** | Exposed APIs **MUST** be supported with Software Development Kits (SDKs) developed using agreed technologies, delivered in a state invokable from a either a Command Line Interface (CLI) or pipeline automation. | | | APIs require testing from the command line, in order to develop automated integration tests that can be run by the automated deployment pipeline.  SDKs may be useful to 3rd party consumers to inform them how to connect to the service. |
| QR-CP-B-08 | **Baseline** | | | **Compatibility/Interoperability/SMTP MTA** | Services **MUST** be able to connect to a Mail Transfer Authority (MTA) to deliver notifications to subscribed stakeholders. | | | The solution must be capable of distributing notifications by at least one external channel. |
| QR-CP-B-09 | **Baseline** | | | **Compatibility/Interoperability/**  **Malware Service** | **IF** the service permits uploading media, Services **MUST** be capable of invoking a 3rd party cloud based anti-malware service. | | | The solution must be capable of validating that user uploaded media is free of malware, and alert users with informative messages. |
| QR-CP-B-10 | **Baseline** | | | **Compatibility/Separate Server & Client** | The service client **MUST** be developed in a separate tier from the service APIs. | | | When the interface is developed as a server-rendered part of the service, APIs can be bypassed and therefore there is no impetus or guarantee that all necessary APIs will be developed and sufficiently tested. |
| QR-CP-B-11 | **Baseline** | | | **Compatibility/Integration/ Data warehouse** | Services **MUST** be capable to make key information available to a data warehouse.  The common approach is to allow an ETL service invoke APIs to collect information to deposit in a location for pickup by the Data warehouse. | | |  |

### RELIABILITY (ISO-25010/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.

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.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | State | Title | | Statement | Rationale | |
|  |  |  | |  |  | |
| Project Specific Quality Requirements Scope | | | | | | |
| TODO |  |  | |  |  | |
| Organisation Sector Quality Requirements Scope | | | | | | |
| NONE |  |  | |  |  | |
| Education Sector Quality Requirements Scope | | | | | | |
| NONE |  |  | |  |  | |
| Government Sector Quality Requirements Scope | | | | | | |
| NONE |  |  | |  |  | |
| Industry Baseline Quality Requirements | | | | | | |
| QR-RL-B-01 | **Baseline** | **Reliability/Availability** | The solution **MUST** meet the Maximum Tolerable Downtime (MTD) and availability expectations defined in the *Target Quality Objectives* table by:   * Being deployed to a Cloud provider whose SLAs are better than this solution’s MTD. * Using a DoS protecting WAF * Minimising Database connections by design first and local host caching second (for immutable data), and distributed caching last (for mutable data) * Avoiding Data Locking of records by reducing the length of open Transactions, performing updates at the end of Requests. * Complex reporting queries are relegated to a reporting database * Backups are taken regularly * DR utilizes automated deployment and data restoration pipeline * Automated deployments utilize infrastructure as code and database schema as code to ensure infrastructure and DBs are current. * Automated deployments must take down the system for as short a time as possible. | | | 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 *Target Quality Objectives*table.  In the case of a planned or unplanned outage, the solution must be able to be returned to a functionality state in the shortest amount of time. |
| QR-RL-B-02 | **Baseline** | **Reliability/Availability/**  **Background/Multi-threaded** | The solution **MUST** process continually background operations (as opposed to running them outside of work hours) spread 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 |
| QR-RL-B-03 | **Baseline** | **Reliability/Availability/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. |
| QR-RL-B-04 | **Baseline** | **Reliability/Availability/Disaster Recovery Plan** | The solution **MUST** include an organisation accepted automated Disaster Recovery plan that is capable. | | | Upon disaster to the system environment and/or production data, the service must be able to be made available to end users within the shortest agreed delay. |
| QR-RL-B-05 | **Baseline** | **Reliability/Recoverability/BCP** | The solution **MAY** rely on a capable DR plan to restore business services within delays specified in the *Target Quality Objectives* table.  *Note: this requirement is a project requirement, not answerable by a respondent – but they will be requested to participate in its planning.* | | | If cloud services are down, and services are impaired in such a way that a DR operation will not resolve the issue, the organisation will have other problems to consume our attention until the cloud becomes available. |
| QR-RL-B-06 | **Baseline** | **Reliability/Availability/Backups** | The solution **MUST** include a regular and fully automated full and incremental backup and restoration process that meets Response Point Objective Time (RPO) and Response Time objectives (RPT) targets as defined in the *Target Quality Objectives* table.  *Reminder: As stated under Security, Backups are persisted in a resource group separate from the production data resource group.* | | | Upon corruption of PROD data, data should be restored from backups within agreed duration constraints. |
| QR-RL-B-07 | **Baseline** | **Reliability/Availability/System Restart** | The process of restarting or recovering after a service or component outage or failure **MUST** **NOT** require restarting the underlying infrastructure of the services.  *Note: To improve the experience of the first users, the deployment pipeline’s final operation is usually to awake the service.* | | | 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. |
| QR-RL-B-08 | **Baseline** | **Reliability/Availability/Scheduled Downtime** | Stakeholders and 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-RL-B-09 | **Baseline** | **Reliability/Availability/Scalability/Users** | 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 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. |
| QR-RL-B-10 | **Baseline** | **Reliability/Availability/Fault Tolerance & Recoverability** | The solution **MUST** trap and recover from unexpected errors and capture relevant information in permanent records.  A unique Identifier of the error must be presented to the user to ease discussions with Support Services. | | | Error reports must be recorded for later analysis by operations specialists. |

### PERFORMANCE (ISO-25010/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.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # | State | | Title | Statement | | Rationale | |
|  |  | |  |  | |  | |
| Project Specific Quality Requirements Scope | | | | | | | |
| TODO |  | |  |  | |  | |
| Organisation Quality Requirements Scope | | | | | | | |
| NONE |  | |  |  | |  | |
| Education Sector Quality Requirements Scope | | | | | | | |
| NONE |  | |  |  | |  | |
| Government Sector Quality Requirements Scope | | | | | | | |
| NONE |  | |  |  | |  | |
| Industry Baseline Quality Requirements | | | | | | | |
| QR-PF-B-01 | **Baseline** | **Performance/Metric collection** | | | The solution **MUST** collect and make available key metrics for reports, including:   * Average & Max Duration of Operations * Average & Max Volume of Operations over Session * Average & Max Volume of Operations over Duration * 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 * Storage used per User | | Collecting metrics provides information required to direct effort towards continual improvement of the service rendered. |
| QR-PF-B-02 | **Baseline** | **Performance/Capacity, Throughput & Responsiveness** | | | The solution **MUST** be capable of completing the requests of the projected peak user quantity within the response time delays defined in the *Target Quality Objectives* table.  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. | | The solution must not cause users to be confused by receiving generic undescriptive system HTTP errors. |
| QR-PF-B-03 | **Baseline** | **Performance/Capacity/Storage** | | | The solution **MUST** be able to dynamically scale out to persist user supplied information, sized as per the *Target Quality Objectives* table. | | The information system must not physically delete information, and instead use logical flags, keeping it for the lifespan of the system. |
| QR-PF-B-04 | **Baseline** | **Performance/Capacity/Archiving** | | | The solution **MUST** **NOT** physically archive data outside the solution’s designed production data environment.  Records are not physically deleted, by logically deleted using State Flags. | | Archived data is production data at a specific point in time, and therefore has a high value compared to production data. |

### MAINTAINABILITY (ISO-25010/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.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # | State | | Title | Statement | | Rationale | |
|  |  | |  |  | |  | |
| Project Specific Quality Requirements Scope | | | | | | | |
| TODO |  | |  |  | |  | |
| Organisation Quality Requirements Scope | | | | | | | |
| *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.* | | | | | | | |
| QR-MT-O-01 | **Technical Baseline** | | **Maintainability/ Custom/ Reference based** | The solution’s customisation **MUST** 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 | |
| Education Sector Quality Requirements Scope | | | | | | | |
| NONE |  | |  |  | |  | |
| Government Sector Quality Requirements Scope | | | | | | | |
| NONE |  | |  |  | |  | |
| Industry Baseline Quality Requirements | | | | | | | |
| TODO | **Organisation** | **Maintainability/Change Control** | | | Releases **MUST** be coordinated as per the organisation's Change Control processes. | | Impact to end users and stakeholders (e.g. Support) must be minimised by coordinating changes to the organisation web site if any, notifying users of upcoming changes to the system, and ensuring required resources are ready (e.g. Support documentation are kept current). |
| Industry Baseline Scope | | | | | | | |
| QR-MT-B-01 | **Baseline** | **Maintainability/User Voice** | | | A solution MUST be provided to collect feedback from all categories of service end users over the service’s lifespan. | | To improve the service during the whole service lifespan, Stakeholders and Users must be able to provide as yet unDefined input in the form of Desires, Issues, Ideas. |
| QR-MT-B-01 | **Baseline** | **Maintainability/Provisionability/Group Invitations** | | | The solution **MUST** allow appropriate users to invite by notification other users to one of their groups, in one group role or another.  *Note: Group configuration can configure that approval is required before issuing invitations.* | | Centrally controlled group and user provisioning requires unwieldy processes that do not scale efficiently.  Letting appropriate users organize groups as they see fit improves the speed with which users can begin to benefit from using a system. |
| QR-MT-B-03 | **Baseline** | **APIs/ Versioning** | | | Externally accessible Service APIs and associated DTOs **MUST** be versioned. | | Maintainability requires that changes to DTOs does not cause force breaking contracts with established integrated systems. |
| QR-MT-B-01 | **Baseline** | **Analysability/Search** | | | The solution’s services and service client interfaces **MUST** support a queryable, searchable, filtering and sorting capabilities using a case insensitive, accent insensitive, culture.  APIs must provide this service for consumption by external tools. | | 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. |
| QR--MT-B-02 | **Baseline** | **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. |
| QR-MT-B-03 | **Baseline** | **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. |
| QR-MT-B-05 | **Baseline** | **Maintainability/Modifiability/ Configurable Features** | | | The solution **MUST** be configurable to enable and disable different functionality depending on user group, without having to redeploy the system. | | Certain features are required to be released in stages, starting with only a subset of users. |
| 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-MT-B-07 | **Baseline** | **Maintainability/Modifiability/Lockout** | | | Any custom 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. |
| QR-MT-B-09 | **Baseline** | **Maintainability/System Status Reporting** | | | The solution **MUST** be able to develop both web interface and printable reports of the status of key aspects of the system.  Key aspects include:   * 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 | | Senior stakeholders are not always users of the system yet require reports on which to base decisions. |
| QR-MT-B-12 | **Baseline** | **Maintainability/Change Notification** | | | Upcoming Feature changes **MUST** be communicable to end users. | | Impact to end users and other stakeholders (e.g., Support) must be minimised by letting them know of upcoming changes to the system. |
| QR-MT-B-11 | **Baseline** | **Maintainability/Change Notification** | | | Feature changes to the solutions **MUST** be communicated to subscribed Stakeholders.  Note: use organisation Change Control provided processes to notify stakeholders other than users. | | Uses should be able to prepare for changes to the system. |
| QR-MT-B-12 | **Baseline** | **Maintainability/Change Control** | | | Releases **MUST** be coordinated as per this organisation's Change Control process. | | Impact to end users and other stakeholders (e.g., Support) must be minimised by letting them know of upcoming changes to the system. |
| QR-MT-B-13 | **Technical Baseline** | **Maintainability/Service Client/SPA** | | | Custom development of interfaces MUST follow Progressive Web App (PWA) Single Page Application (SPA) development patterns. | | The solution must be keep interface and service separate to improve maintainability. |
| QRM08 | **Technical Baseline** | **Modifiability/ Loosely coupled** | | | Custom development **SHOULD** develop using loosely coupled systems and components. | | The solution SHOULD allow modification to one component or group of functionalities with the least chance of affecting other parts of the solution. |
| QRPT05 | **Technical Baseline** | **Maintainability/ Custom/ Development Framework** | | | Custom development **SHOULD** use multi-platform development Frameworks. | | No OS has complete dominance of the market. |
| QRM10 | **Technical Baseline** | **Maintainability/ Custom/ Source Control** | | | Documentation and source code (but NOT configuration credentials!) developed for the solution **MUST** be persisted in a distributed source code repository accessible from the start by this organisation. | | Vendor support lock is not valued by this organisation. |

### PORTABILITY (ISO-25010/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.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # | State | Title | | Statement | | Rationale | |
|  |  |  | |  | |  | |
| Project Specific Quality Requirements Scope | | | | | | | |
| NONE |  |  | |  | |  | |
| Organisation Quality Requirements Scope | | | | | | | |
| NONE |  |  | |  | |  | |
| Education Sector Quality Requirements Scope | | | | | | | |
| NONE |  |  | |  | |  | |
| Government Sector Quality Requirements Scope | | | | | | | |
| NONE |  |  | |  | |  | |
| Industry Baseline Quality Requirements | | | | | | | |
| QR-PT-B-02 | **Baseline** | | **Portability/ Adaptability/ Configurability** | | The solution **MUST** be configurable by API and/or User Interface. | | Operations Specialists must be able to reconfigure the system to meet changing use case or constraints, using either User Interface Views or APIs without requiring redeployment, until such configuration is developed into the deployment pipeline. |
| QR-PT-B-03 | **Baseline** | | **Portability/ Adaptability/**  **Hardware** | | The solution **MUST** **NOT** require specialised hardware or service license or subscriptions without disclosure and organisation agreement prior to procurement stage completion. | | Specialised hardware may not be available for the duration of the service. |
| QR-PT-B-04 | **Baseline** | | **Portability/ Installability/**  **Dependencies** | | Digital Deliverables **SHOULD** be portable to different operating systems.  *Note: It is not a requirement that systems be portable between Cloud Providers.* | | Solutions should not be limited to commercial operating systems (e.g., Windows). |
| QR-PT-B-04 | **Baseline** | | **Portability/ Installability/**  **Cloud** | | Digital Deliverables **MAY** be portable to different cloud hosting environments. | | Note: development, deployment, configuration, provisioning, etc. scripts should be portable and reusable where applicable. |