# Document

## 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)

| # | 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. |

## 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 |
| --- | --- | --- | --- | --- |
| 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. |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### FUNCTIONALITY (ISO-25010/Functionality)

Functionality is a key quality defined under ISO-25010.

| # | Scope | Title | Statement | Rationale |
| --- | --- | --- | --- | --- |
| Industry Scope Baseline Requirements | | | | |
| 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 |  |
|  |  |  |  |  |

### SECURITY (ISO-25010/Security)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # | State | | Title | Statement | | Rationale | |
| Government Sector Quality Requirements Scope | | | | | | | |
| Industry Baseline | | | | | | | |
| 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-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-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.). |

### USABILITY (ISO-25010/Usability)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 |  |  |