Service Qualities

IT Project Procurement

## Synopsis

Procurements are more likely to fail being approved or delivering on expectations if they the requirements are incorrect or incomplete.

This document lists high-level Quality Requirements business service systems must address.

## Author

Sky Sigal, Solution Architect, ITC SPA

# Document

## Table of Contents

[1.1 Synopsis i](#_Toc74748266)

[1.2 Author i](#_Toc74748267)

[2 Document 2](#_Toc74748268)

[2.1 Table of Contents 2](#_Toc74748269)

[2.2 Creation 2](#_Toc74748270)

[2.3 Distribution 2](#_Toc74748271)

[2.4 Conventions 2](#_Toc74748272)

[Document 4](#_Toc74748273)

[3 Background 5](#_Toc74748274)

[3.1 Synopsis 5](#_Toc74748275)

[4 Background 6](#_Toc74748276)

[5 Purpose 7](#_Toc74748277)

[6 Questions 8](#_Toc74748278)

[6.1 Obligations 8](#_Toc74748279)

[6.2 ISO-25010/ISO-25012 Qualities 10](#_Toc74748280)

## Creation

Date: 18/05/2021

## Distribution

Distribution/Review List:

* Amy Orr, Data Architect
* Brad Atte Le Crouche, Solution Architect
* Diane Simpson, Infrastructure Architect
* Michelle Nicolson,
* Dries Venter, Cloud Infrastructure Specialist
* Grayson Mitchell, Manager, BE&S ICT SPA
* Jeff Grove, Security Specialist, Contractor
* Sally Murrey, ICT Change Advisor
* Sean Torley, ICT Change & Transition
* Stuart McGrigor, Solution Architect
* Werner Van der Merwe, Automation Lead
* Yujia Huang, Security Specialist, Contractor

## Conventions

### Terms

The Appendices include a Glossary of Terms to assist understand this document.

### Diagrams

Where applicable, diagrams are developed using ISO-\*, Archimate, UML or appropriate industry standards and conventions.

**Document**

# Background

## Synopsis

TODO

# Background

NZ government agencies are obligated by law and regulation[[1]](#footnote-1) to deliver secure and reliable public services in an equitable manner, with evidence and decisions permanently recorded for transparent yet privacy-protecting auditability.

These obligations are applicable whether the service is developed internally or by 3rd party services (and so forth).

Before a government procured service can be made publicly available, the service requires Certification & Accreditation certification of the service’s adherence to the above constraints.

The security, accountability and accessibility obligations often lead to design choices above and beyond those of commercial products and services.

For this reason, C&A specialists understand that not all 3rd party procured services can meet all obligations. But the process requires that current gaps and risks are identified, acknowledged, registered, monitored, and both parties continue to work together developing acceptable mitigations to as-yet non-compliancy risks.

# Purpose

The questions below fulfil two purposes. They apprise you of the requirements that will require addressing before the service can go live. They are to elicit from you a truthful declaration of the current state of the proposed service, so that collaborative effort can be planned to find acceptable mitigations, either before contractual obligations, or later.

# Questions

## Obligations

Could you please describe whether your proposed service, with or without additional expense, can or cannot meet our obligations to the following regulations, and if not, how would you propose to mitigate the service’s non-compliance risk?

### Privacy Act

Key concerns of how our obligations are or will be met involve better understanding of your proposed services ability in the following areas:

* Systems must provide access to clear & current instructions as to the data collection purpose, its use, retention duration, and sharing.
* Users must be provided a means to correct personally identifiable information (PII), preferably by self-service.
* Users must be provided a means to logically (not physically) remove their personally identifiable information from availability via the service.

### Digital Service Principles & NZ Govt Web Standards

Key concerns of how our obligations are or will be met involve better understanding of your proposed services ability in the following areas:

* **Accessibility:** will your proposed service’s interface be capable of being externally validated as meeting Web Content Accessibility Guidelines (WCAG) 2.1 (AA+) for visually impaired users, before it goes live?
* **Availability:** will your proposed service’s interface be accessible from current web browsers (e.g.: mobile phone current browsers), regardless of network environment?  
  *Note: our internal networks add some latency due to security firewalls, proxying, auditing.*
* **Understandability:** Can you deliver the service’s content and interface media in NZ’s 3 official languages?   
  *Note: the NZ Govt Web Standards addresses the requirements of the third official language.*

### Public Records Act

Key concerns of how our obligations are or will be met involve better understanding of your proposed services ability in the following areas:

* **Logical deletions:** will your proposed service be able to meet the Archivist General’s directive that digital records only be *logically[[2]](#footnote-2)* deleted?   
  *Note: physically deleting and restoring records from either audit tables or backups does not meet this obligation.*
* **State Metadata:** will your proposed service develop & permanently keep metadata in the system as to when the logical states of records were changed, and by whom?   
  *Note: operation & version history is often distinct from auditing requirements.*

### Official Information Act

Key concerns of how our obligations are or will be met involve better understanding of your proposed services ability in the following areas:

* **Permanency of auditable records:** will your proposed service be capable of persisting all system records, changes, in-system and external notifications (e.g. email), in order to fulfil OIA Request obligations?  
  *Note: OIA obligations are another reason that records should not be physically deleted.*

### NZISM’s system security guidelines

Key concerns of how our obligations are or will be met involve better understanding of your proposed services ability in the following areas:

* **Security of environment:** will you proposed service be used within an ISO-27001 Stage 2+ accredited environment?   
  *Note: with so many accreditable options available at reasonable cost, the use of a non- or self-accredited, local or on-prem facility is not defendable if reviewed.*
* **Security of network:** will every channel your proposed service uses between components & services -- internal and 3rd party -- be monitored?  
  *Note: expectations include monitoring, auditing, and reporting unexpected patterns.*
* **Security of Infrastructure:** will your proposed service be deployed to a secured network?  
  *Note: expectations include one or more of the following: authenticated and authorised changes to network configuration, no physical access to the infrastructure.*
* **Security of Infrastructure configuration:** will your proposed service be deployed by automation? Will service integration authentication keys and certificates be secured within an appropriate secure storage service, which only the pipeline’s service account has access to? Will you avoid allowing the confidential storage accessible to delivery and other stakeholders? *Note: automation & auditing is recommended to protect the “keys to the kingdom”.*
* **Security of data access:** will you restrict access to production premises, data or backups only the service’s service account such that nobody can access unless it via the system’s audited, permission based, interfaces?  
  *Note: expectations include direct access to both current or stale/obfuscated prod data by BAs, Testers or maintenance stakeholders be denied.*
* **Security of availability:** will your proposed service be automatically monitoring to horizontal scaling up or down as needed to meet demand surges?  
  *Note: expectations include the use of standard features of modern cloud environments.*
* **Security of system:** will your proposed service’s security be in depth, by design, both during development and subsequent during ongoing maintenance and regular updating?  
  *Note: expectations include using validation of all incoming messages, meeting OWASP recommendations and using current versions of actively maintained libraries throughout the service’s full lifetime.*
* **Security of data at rest:** will your proposed service use encryption for operational, reporting and backup data?  
  *Note: expectations include ensuring that if someone is able to download a backup they are unable to decrypt it without keys that are secured elsewhere, to which access is denied (see security of infrastructure above).*
* **Security of data in transit**: will your proposed service ensure encryption and privacy is maintained on all communication between system components using current, valid and recommended encryption?   
  *Note: expectations include the use of SSL3 based HTTPS, HTTP Redirection to HTTPS equivalent endpoints, Safe cookies and OWASP recommendations.*
* **Security of user credentials:** will your proposed service be capable of using an external web-based single-sign-on Identity [token] Provider (IdP) service – such as this organisation’s Azure B2C and/or Azure AD services?
* *Note: the use of an in-system credential storage approach is not defendable under review.*
* **Security of accountability**: will your proposed service audit all changes to any records, such that operations can be attributed to a current Session, and therefore an authenticated user?  
  *Note: functionality is expected to be provided within system, in order to not need another system to discover and investigate abnormal behaviour.*
* **Security of notifications:** will your proposed service be capable of ensuring that messages do not contain sensitive or personal data, but instead provide links back to authenticated and audited access to data? *Note: disclosure of Personally Identifiable Information (PII) – especially national identifiers – is a serious breach of trust and privacy. Disclosure of private data in an unaudited manner is a breach of security.*
* **Security of system messages:** will your proposed service be capable of sanitising error messages in order to not display confidential information?  
  *Note: in order to not leak confidential information new systems will be expected to log the error report, providing the unique id of the report in the message to the end user, such that it can be reference in conversations with support.*

## ISO-25010/ISO-25012 Qualities

Whereas the previous questions were specific to discovering how your proposed service can assist with addressing obligations this organisation must meet, the following questions are intended to help us understand the quality of your product.

### Trustworthiness

The following key concerns can be addressed by better understanding your proposed services ability to integrated with other services:

* **Trustworthiness of Messages:** will your proposed service be capable of being integrated with an organisation’s Email Server (MTA)?
* **Trustworthiness of Site:** will your proposed service be able to be associated to a subdomain under this organisation’s domain?

### Discoverability

The following key concerns can be addressed by better understanding your proposed services ability to make data and content discoverable:

* **SEO:** will your proposed service be public web Search Engine Optimised (SEO)? What parts of the service would inappropriate for SEO?
* **Navigation:** Will your proposed service be provided with clear, Accessible, translated, Navigation -- such that users can quickly find relevant information?

### Error Correction

* **Validation:** describe how your proposed service will validate submitted data?
* **Idempotency:** describe how your proposed service will be idempotent, such that resubmitting the same change operations do not duplicate the change.

### Interoperability

The following key concerns can be addressed by better understanding your proposed service’s ability to interoperate with other organisation services:

* **API First:** how will your proposed service ensure that its functionality is available for other services to integrate with, import or export data by current means rather than legacy ETL operations?  
  *Note: it is policy to enforce our design principles of API First on new development, to ensure systems are architected as headless services with a separate but dedicated client.*
* **Universality**: how does your proposed service implement universal data types and encoding to facilitate interoperability between systems, potentially in different time zones, while not inadvertently introducing data errors?

*Note: it is our policy on new development to enforce the use of UUIDs, UTCs and ISO/IEEE Standards-based textual encoding.*

### Usability

The following key concerns can be addressed by better understanding your proposed service’s ability to be configured to best fit user expectations:

* **Configuration Management**: how will your proposed service diminish the necessity to redeploy the service?  
  *Note: expectations would include one or more of the following: most settings are mutable, configurable from an interface, persisted in a database, rather than being immutable and/or requiring a redeployment to change their values.*
* **Tenancy Management:** how will your proposed service permit different organisations to manage their own users independently from other organisations – while allowing users to be members of more than one tenancy?  
  *Note: expectations would include one or more of the following: without requiring a restart, the capability to setup and teardown of distinct tenancies in the same or tenancy-specific storage facilities, each with the ability to add/remove users and Groups and assign Permissions, via Group Roles as desired.   
  Important: note that schools and other education providers are* not *part of this organisation. They are distinct organisations and in many ways are similar to franchisees, as opposed to departments within this organisation.*
* **User Onboarding & Management:**will your proposed service require onboarding of users? If so, how?  
  *Note: in new custom development we can endorse allowing users to invite others to join a group as a designated role. Using SCIM v2 or later is another approach that is acceptable.*
* **Group & Permissions Management:** how will your proposed service provide management   
  *Note: in new custom development expectations would include one or more of the following: permissions are assigned ore revoked to users per their role within a group, are inheritable, can be modified via a user interface. Dependencies on deploying database changes to change permission assignment are not acceptable.*
* **Media Management:** most systems manage media in some manner or another.If applicable, how will your proposed service manage it?   
  *Note: in new custom development expectations would include one or more of the following: storage and interfaces to manage cookie, tracking, privacy & terms & condition statements. Additionally, if user profiles are provided, user images may require persistence.*

### Functionality

The following key concerns can be addressed by better understanding your proposed service’s ability to deliver functionality expected by different stakeholder groups:

* **Monitoring Functionality:** how will your proposed service facilitate security and maintenance specialists monitoring and being alerted to aberrant behaviour?  
  *Note: expectations would include that the chosen service environment is capable of monitoring and alerting changes in traffic patterns that may require attention.*
* **Security Functionality:**how will your proposed service permit protecting the service’s data without disruption to other users?
* *note: expectations would include one or more of the following: having specific users be notified of abnormal behaviour, the ability to terminate suspicious sessions, temporarily locking system principal (user or remote client service) accounts, permit querying and reviewing the operations of specific sessions and/or users, in order to quickly report to stakeholders and – as required by law – the Privacy Commissioner as to the extent and actual records accessed.*
* **Maintenance Functionality:** how will your proposed service facilitate maintenance of the system?*Note: expectations would include one or more of the following: interfaces to monitor activity, change system configuration without requiring redeployment, diagnose and audit activity to discover issues that need maintenance, regular automated backups so that the system can easily be restored by automation within SLAs, integrated performance counters that can be interrogated to monitor usage, resource utilisation and exceptions.*
* **Operations Functionality:** how will your proposed service facilitate operations?*Note: expectations would include one or more of the following: user groups, change their permissions, to report to stakeholders how many users are regularly using the system, whether the number is increasing or decreasing, what resources they are most interested in, etc.*
* **Support Functionality:** how will your proposed service facilitate supporting users?*Note: expectations would include one or more of the following: ease of use to invite users to roles within groups, add or remove their group specific permissions, restore inadvertently deleted records, and when invited to do so, be able to perform operations on someone’s behalf.*

### Business Continuity, Handover & Termination

The following key concerns can be addressed by better understanding your proposed service’s ability to use interoperability to address business operations:

* **Delivery Methodology**: what standards based methodology to you use to manage client engagement, collection of their stakeholder desires, development of deployment, environment, system, process and data requirements, development, deployment, driving monitoring, maintenance, operations, and support?  
  *Note: expectations would include one or more of the following: the engagement follow an ISO recommended approach, in order to minimise risk of omission, rework, delays. Our current preference is a SecOps based approach -- a superset of DevOps – as it ensures a cross-departmental viewpoint that is missing from straight Agile (which focuses solely on Development), while ensuring that consideration of Security is woven in from the start.*
* **Collaboration & Handover:** how would your proposed service allow concurrent operations by yourselves and this organisation’s employees, ultimately leading to a complete transfer of operations to this organisation’s employees?
* **Termination:** When the service is shut down
  + what data, in what format, would be capable of being extracting for importation into another system?
  + What data do you envision not being able to export in a format usable for business continuity?

### Deployability

The following key concerns can be addressed by better understanding your ability to deploy the service in a way that can be handed over later:

* **Delivery Environment:** if your proposed service will be delivered into a cloud environment, will the subscription account that is used be your firms or our organisation? If not ours, what would be required to enable your using our subscription to ease handover later?  
  *Note: our preference would be to use the organisation’s cloud service subscriptions for deployment from the start to facilitate collaboration and ultimate handover.*
* **Pipeline Delivery:** is your system deployed using an automated pipeline that can be handed over as the primary system deliverable?

*Note: for systems we will be taking over the delivery of, we will expect work to progress towards ensuring a hand over of all of the following operations being achieved by coded automation, rather than manual operations: environment and infrastructure creation and configuration, data schema creation and updating, reference data seeding, backup restoration, system compilation & integration, static QA testing, system packaging & deployment, environment specific system configuration, and livening, ready for requests.*

### Deliverability

The following key concerns can be addressed by better understanding your ability to deliver the service in a collaborative manner:

* **Deliverables:** what deliverables will you be delivering?  
  *Note: our expectations would include a delivery pipeline, or failing that, the service itself, separate digital and print documentation on its environment and infrastructure development, deployment, usage, monitoring, maintenance, operations, support, Data backup and restoration, DR, and decommissioning.*
* **WorkItem & Issue Management:** what digital services do you use for tracking Stakeholder Desires & Feature requests, Issues, in progress and completed WorkItems? How do you envision employees from different organisations collaborating together in preparation for potentially handing operations over, over a duration of time? How do you envision minimising the amount of user PII added to WorkItems and issue tickets?  
  *Note: this organisation has an internal-only JIRA that is available if working on organisation provided devices, but can provide a dedicated project space within our web-based subscription to Azure DevOps, a collaborative* Application Lifecycle Management *(ALM).  
  It would preferable to avoid the disruption of WorkItems having to be exported/re-imported into another system at some future time.*

### Maintainability

The maintainability of your proposed service is of interest if we are to support the solution at some point in the future. The maturity of the product’s design and implementation – and therefore an estimate of the modularity, maintainability and extensibility of the proposed service – can be ascertained to some extend by answers demonstrating how much of the following will be in it:

* **Diagnostics:** will your proposed service save sanitised diagnostics log messages (cleared of PII/confidential information) to an external storage solution (blob, file, etc.) for maintenance specialists to query? Will your service provide a means (user interface and/or API) to analyse these messages remotely?  
  *note: expectations for new custom development include one or more of the following: the use of rolling log files, using cloud storage, providing an API to query it.   
  important: system and database logs are appropriate solutions to auditing, backup & restoration, undo functionality -- which is best served by state changes to records.*
* **Monitoring:** will your proposed service contain performance counters that can be monitored for abnormal behaviour? *note: expectations for new custom development include one or more of the following: performance counters of usage, throughput, resource utilisation.*
* **Client/Server Separation**: (see above, under Integration)  
  *note: expectations for new custom development include one or more of the following: permitting more chances to reuse the service’s logic from other systems, as well as keeping the client side interface code – the tier most likely to require updating over the service’s lifetime – to be separate from the service’s logic that will probably be usable without change for a far longer time.*
* **Queryable, Validated, Mapped API Models:** will your proposed service’s APIs permit queryability (OData, GraphQL), use Mapping between service entities and versioned API messages?  
  *note: expectations for new custom development include one or more of the following: the use of international Standards based OData, potentially adding GraphQL, that mapping is used to ensure internal Entities – and their internal storage Ids and metadata -- are not exposed to the outside for security reasons. To allow maintainability, without disruption to service clients, we expect API messages to be versioned, permitting a protracted sunsetting to allow clients the time to update to newer versions of messages.*
* **DDD, OO, Compiled, General Development Patterns**: will your service be developed using Compiled languages, Domain Driven Design approaches to component architecture, and Object-Oriented best practices?   
  *note: expectations for new custom development include one or more of the following: developers understand and implement Domain Driven Design component design, Objected Oriented best practices (GRASP and SOLID coding principles), Behaviour+Test Driven Development of compiled code (letting the compiler do half the work of finding potential defects) to make the code investment more cost effective to develop initially and subsequently maintain and/or extend.*
* **Object Relational Model**: will your proposed service access storage directly, or use an Object Relational Model (ORM) broker?  
  *note: expectations for new custom development include one or more of the following: a preference for the use of ORMs to abstract away access to storage, decreasing common security coding errors, therefore attack surfaces as well as development complexity – relying on subsequent performance optimisation (indexing, caching, model design) if any is required.*

1. Privacy Act, Public Records Act, Official Information Act, NZ Cabinet [CAB Min (03) 41/2B], NZ Procurement Rule 61, NZ Govt Web Standards (NZGWS). DIA Digital.govt.nz Security directives. [↑](#footnote-ref-1)
2. as opposed to physically deleted [↑](#footnote-ref-2)