DRAFT - ICT Project Guidance

Discovery:   
Technical -   
Default System Functional Requirements

Version:

0.1

Author:

Sky Sigal, Solution Architect

## Purpose

This document catalogues functional requirements common to systems, irrespective of the system’s business purpose.

## Synopsis

All systems are constrained by legislation to provide all users specific functionality. In addition, all systems are expected to provide well-known functionality to support the tasks of customer support specialists, operations specialists and maintenance specialists.

## Contents

[Description 1](#_Toc155264662)

[Synopsis 1](#_Toc155264663)

[Contents 2](#_Toc155264664)

[Introduction 6](#_Toc155264665)

[Purpose 6](#_Toc155264666)

[Context 6](#_Toc155264667)

[Organisation 6](#_Toc155264668)

[Tiers 6](#_Toc155264669)

[Qualities 7](#_Toc155264670)

[Requirement Attributes 8](#_Toc155264671)

[ID 8](#_Toc155264672)

[[Diagram] Title 8](#_Toc155264673)

[Statement 8](#_Toc155264674)

[Prioritisation 8](#_Toc155264675)

[Acceptance Criteria 8](#_Toc155264676)

[Details 9](#_Toc155264677)

[Questions and Response 9](#_Toc155264678)

[Exemptions 9](#_Toc155264679)

[Comment 9](#_Toc155264680)

[Custom Development Quality Requirements 9](#_Toc155264681)

[Quantitative Settings 11](#_Toc155264682)

[Quality Requirements 12](#_Toc155264683)

[ISO Defined Qualities 12](#_Toc155264684)

[Terminology Used 12](#_Toc155264685)

[Prioritisation 12](#_Toc155264686)

[Headings 12](#_Toc155264687)

[Project Specific System Qualities 13](#_Toc155264688)

[Scope 13](#_Toc155264689)

[Organisation (NZ MOE) Specific System Qualities 15](#_Toc155264690)

[Security 15](#_Toc155264691)

[Maintainability 16](#_Toc155264692)

[Organisation (NZ MOE) Specific (Hosted) System Qualities 18](#_Toc155264693)

[Scope 18](#_Toc155264694)

[Security 19](#_Toc155264695)

[Reliability 23](#_Toc155264696)

[Maintainability 23](#_Toc155264697)

[Organisation (NZ MOE) Specific (Subscribed) System Qualities 25](#_Toc155264698)

[Scope 25](#_Toc155264699)

[Processes 26](#_Toc155264700)

[Security 27](#_Toc155264701)

[Confidentiality 30](#_Toc155264702)

[Integrity 30](#_Toc155264703)

[Compatibility 31](#_Toc155264704)

[Usability 33](#_Toc155264705)

[Performance 34](#_Toc155264706)

[Sector (NZ Education) Specific System Qualities 36](#_Toc155264707)

[Scope 36](#_Toc155264708)

[Processes 37](#_Toc155264709)

[Security 38](#_Toc155264710)

[Compatibility 38](#_Toc155264711)

[Maintainability 39](#_Toc155264712)

[Sector (NZ Government) System Qualities 41](#_Toc155264713)

[Scope 41](#_Toc155264714)

[Processes 42](#_Toc155264715)

[Security 42](#_Toc155264716)

[Functionality 51](#_Toc155264717)

[Compatibility 52](#_Toc155264718)

[Usability 52](#_Toc155264719)

[Maintainability 53](#_Toc155264720)

[Portability 54](#_Toc155264721)

[Sector (NZ) specific System Qualities 55](#_Toc155264722)

[Scope 55](#_Toc155264723)

[Privacy 56](#_Toc155264724)

[Default Baseline IT System Qualities 58](#_Toc155264725)

[Scope 58](#_Toc155264726)

[Functionality 59](#_Toc155264727)

[Completeness 59](#_Toc155264728)

[Security 63](#_Toc155264729)

[General 63](#_Toc155264730)

[Integrity 64](#_Toc155264731)

[Confidentiality 68](#_Toc155264732)

[Privacy 80](#_Toc155264733)

[General 80](#_Toc155264734)

[Compatibility 83](#_Toc155264735)

[Co-Existence 83](#_Toc155264736)

[Compatibility 83](#_Toc155264737)

[Usability 87](#_Toc155264738)

[Operability 87](#_Toc155264739)

[User Protection Error 90](#_Toc155264740)

[User Interface Aesthetics 91](#_Toc155264741)

[Accessibility 91](#_Toc155264742)

[Recognisability 93](#_Toc155264743)

[Reliability 105](#_Toc155264744)

[Performance 115](#_Toc155264745)

[Maintainability 122](#_Toc155264746)

[Portability 139](#_Toc155264747)

[Default Internal Requirements 147](#_Toc155264748)

[Conclusion 149](#_Toc155264749)

[Appendices 150](#_Toc155264750)

[Appendix A - Document Information 150](#_Toc155264751)

[Images 150](#_Toc155264752)

[Tables 150](#_Toc155264753)

[References 150](#_Toc155264754)

[Review Distribution 150](#_Toc155264755)

[Audience 151](#_Toc155264756)

[Structure 151](#_Toc155264757)

[Diagrams 151](#_Toc155264758)

[Terms 151](#_Toc155264759)

[Appendices B – ISO-25010 Qualities 152](#_Toc155264760)

[Delivery 152](#_Toc155264761)

[Security 152](#_Toc155264762)

[Confidentiality 152](#_Toc155264763)

[Integrity 152](#_Toc155264764)

[Non-Repudiation (of Action) and Accountability (by Whom) 152](#_Toc155264765)

[Authenticity 152](#_Toc155264766)

[Availability 152](#_Toc155264767)

[Privacy 153](#_Toc155264768)

[Functionality 153](#_Toc155264769)

[Functional Completeness 153](#_Toc155264770)

[Functional Correctness 153](#_Toc155264771)

[Functional Appropriateness 153](#_Toc155264772)

[Performance 153](#_Toc155264773)

[Time behaviour 153](#_Toc155264774)

[Resource Utilisation 153](#_Toc155264775)

[Capacity 153](#_Toc155264776)

[Compatibility 153](#_Toc155264777)

[Co-existence 153](#_Toc155264778)

[Interoperability 153](#_Toc155264779)

[Usability 153](#_Toc155264780)

[Appropriateness recognisability 154](#_Toc155264781)

[Learnability 154](#_Toc155264782)

[Operability 154](#_Toc155264783)

[User Error Protection 154](#_Toc155264784)

[User Interface Aesthetics 154](#_Toc155264785)

[Accessibility 154](#_Toc155264786)

[Reliability 154](#_Toc155264787)

[Maturity 155](#_Toc155264788)

[Availability 155](#_Toc155264789)

[Fault tolerance 155](#_Toc155264790)

[Recoverability 155](#_Toc155264791)

[Maintainability 155](#_Toc155264792)

[Modularity 155](#_Toc155264793)

[Reusability 155](#_Toc155264794)

[Analysability 155](#_Toc155264795)

[Modifiability 155](#_Toc155264796)

[Testability 155](#_Toc155264797)

[Portability 155](#_Toc155264798)

[Adaptability 155](#_Toc155264799)

[Installability 155](#_Toc155264800)

[Replaceability 155](#_Toc155264801)

## Introduction

As per the Business Analysis Body of Knowledge (BABOK), Functional Requirements, a subset of a system’s System Requirements.

# Project Specific System Qualities

# Default System Qualities

## Configuration

To support Maintenance specialists deploying and maintaining system operations, Configuration are settings that are set when a system is deployed.   
The primary type of configuration is to organise integration of services and devices (data storage, caching, credentials for 3rd party support services, etc.)

Note:  
In most cases, they are immutable, relying on a new deployment to be changed, although – with development effort along with some operational risk – once connection to a data storage device or service has been established, other configuration settings can be persisted to the datastore and therefore can be made mutable.

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

## Diagnostic Tracing

To support Maintenance, and issue correction Development Specialists, Diagnostic Tracing is essential to provide insight as to the flow of activity related to the issue being investigated.

Note:  
Diagnostics traces used to be persisted to the local directory, but no longer the recommended approach due to changes of architecture as required of PaaS based systems. Current best practice for cloud based services are the use of Cloud based storage, invoked in a fire and forget manner.

The storage location of diagnostics traces records are generally not database management services. For specialists to be able to search for relevant records (by request thread, by User, by Date, combination thereof, etc.) the usual practice is to load diagnostics trace files into 3rd party specialist in-mem tools.

In rare cases, the storage used is a queryable database of some kind – but it should always be the operational database.

Useful log files generally are large in size. Log files are temporal, and are deleted after a configurable duration (usually set to 31 days).

Functionality is required by Maintenance and Development Specialists to retrieve and/or Browse and View Diagnostic trace records.

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

## Error Recording

While Diagnostic records trace activity, error records trace exceptions, recording the date, time, session, user, exception reason.   
Error Records are persisted permanently, making it possible to develop charts presumably showing progress at improving service quality, demonstrated by a reduction of the number of errors that occur over time.

Trace records persist a record of the stack for later analysis by Development specialists.

System Functionality to Browse and View Error Records is required by Maintenance Specialists.

Note:  
While they take up space, the number of exceptions are far fewer than Diagnostic tracing records, so there is generally no strong reason to clear them out after a duration of time.

Note:  
There was an IT engineering school of thought recommending throwing Exceptions for normal flow control. This is flawed logic and is to be avoided (it’s resource intensive as well as clogging Error Recording, and Monitoring, discussed next).

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

## Monitoring

Counter are used to monitor various aspects of the system. Common examples of use cases may include capturing:

* Requests/Time
* Views/Request (informing stickness/usefulness of site, but may also be showing confusion)
* Current Active Sessions (informing Functional Appropriateness)
* Bytes received and sent (impacting Resource Utilisation)
* Exceptions/Request

For Performance reasons, Counter values require specialised storage solutions are persisted separately from the Oeprational Database. Specialists use 3rd party tools to view the results.

In admittedly rare cases the system may periodically import values into a system database to make them visible to permitted users as rolling charts within the system. In which case the system is required to provide functionality to Maintenance specialists to select and view one or more of these charts.

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

## Caching

Functionality is required by Maintenance Specialists to configure the values of system wide Short (e.g.: 1 second) , Medium (e.g. 5 seconds) and Long (eg 30 seconds) caching durations.

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

## System Settings

System settings are different than Configuration Settings in that Configuration Settings are for integrating components, and are generally immutable, whereas System Settings are mutable values persisted in the operational database to set up the whole system, across all tenancies if any.

System Settings include but are not limited to the following:

* Sponsor Information & Branding
* System Naming & Branding
* Discoverability by public Search Engines
* System Appearance: base layout & styling
* Default Tenancy (if Tenancies are used)
* Short, Medium & Long Caching Durations
* Enabling Logical Modules

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

## Reference Data

Systems use Reference Data to list acceptable values for resource fields.

Common examples include but are not limited to:

* Countries
* Person Sexes (M/F)
* Identity Genders (different and broader than Sexes)
* Location Types (Personal, Business, Shipping, Custom, etc.)
* Etc.

Note:  
Reference Data must by default be customizable on a per-Tenant basis while also including non-changeable System-wide values.

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

## Permission

Permissions are the basic unit of Authorisation, bundled together as logical Roles.

Note:  
It is a common logical error to manage Operation Authorisation by Role instead of by the Permissions a User has by being in a Role.

Common Permissions include but are not limited to:

* Resource Permissions:
  + xxx-Create
  + xxx-Contribute
  + xxx-Read
  + xxx-Comment (used by resource Reviewers)
  + xxx-Approve (used to progress reviewed Resources)
* Resource Metadata Permissions:
  + xxx-Metadata-Create/Update (can maintain a subset of the Resources’ metadata, etc.)
  + xxx-Metatada-Delete

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

## Roles

Roles are the logical bundling of Permissions to a User.

System Operators Must be able to develop Roles.

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

## Users

Users must be able to sign in and out, review their personal preference settings,

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

## User Groups

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

## User Group Roles

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

## User System Preference Profile

As mentioned above under Users, a User expects to be able to manage their personal system preference settings to improve accessibility or effectiveness qualities.

A User’s System Preference Profile is a logical grouping of these Preference settings.

A Profile’s settings include but are not limited to:

* Culture/Language: their preferred language
* Appearance settings (overriding or supplementing the default System Appearance settings)
* Accessibility settings: font size, colour schemes, that override their etc.

All system Users require functionality to view and edit the settings in their system preference profile.

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

## User Security Profile

In addition to each user having a logical System Preference Profile, they also have a logical grouping of their roles.

This is their viewable list of Roles they have accepted or been assigned.

All system Users benefit from having functionality to view the Roles they belong to. They benefit from being able to see the

Permissions they have been received by being assigned these Roles.  
  
All Users benefit from having the means to Apply for a Role (which if accepted is leads to the issuance of an Invitation to a Role that they can accept or decline).

Permitted Users benefit from having functionality to invite users to roles.

Mature systems provide the means to tweak the assignments by selecting a role, and then removing some of the permissions or adding new ones, without creating a new Role definition first.

Roles must be independently developable per Tenancy (if tenancies are available), while acknowedlging that some Roles are system Roles that cannot be deleted, and/or their association to Permissions cannot be changed.

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

## User Digital Identities

Each User has a digital identity. The digital identity can be a managed authenticated by a 3rd party identity, but can also be managed and authenticated in-system (not everybody will accept to use a 3rd party IdP’s identity to gain access to the system).

A User requires functionality to sign in and out.

A User benefits from seeing which digital identities have been associate to his system record. Optionally, they can disable digital identities they are no longer using (that are not the digital identity they are currently using).

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

## Notifications & Messages

Notifications are in-system messages raised by the system upon certain events happening for viewing by target users.

Notifications can be shown for a set duration (e.g.: 30 seconds) or remain available until a person has read them.

Some notifications require being sent when a User is not using the system. In which case they are sent as emails or SMS notifications.

To send them, Notifications records are created in the system, then serialised as emails for sending via organisation or 3rd party mail service providers.

Users benefit from having functionality to see, close, or review & list notifications & past messages.

## Resources

A Resource is a term used to covers any form of key record a system manages.

Resources include Users, Data Records and Metadata Records describing managed media (e.g. Images, Docs, etc.).

A permitted User may have one or more permissions to Create, Contribute, Comment, Approve, Publish, Replace, Remove, Restore records.

Note:   
It is a common logical error to physically Delete record. Records should only be removed from user access by logical state changes (i.e., record flag(s)), that can be reversed if needed. Records of Users that ask to be removed from the system are also depersonalized, ensuring that all records associated to the User record cannot be determined as to which single Person they are related to.

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

## Resource Roles

A Resource will manage access by verifying that the User has Permissions specific to the Reosurce, that are generally allocated to them by the User accepting a Role that contains them.

Permitted Users benefit from having access to functionality to create new Resources.

Permitted Users benefit from having access to functionality to invite other Users to accept a role to contribute to the Resource.

Etc.

Note:  
Roles in a parent Group can be configured to automatically allocate to some Group Members default Resource Roles (for example any Accountable, Responsible, Member of a Group may inherit the right to Create, Collaborate on Resources of type X – but only specific persons can be invited to be approvers of the Resource).

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  |  |  | The system permits the Development and Maintenance of Roles specific to Resources. | Mature organisations create high quality resources by having multiple roles work on their development, review, approval, release, maintenance and replacement or retirement. | The system has Permissions specific to the Resources it manages.  The system has roles specific to the Resources it manages, composed of Permissions. | Roles may include:  Creators, Contributors, Commentators, Reviewers, Approvers, Maintainers and Consumers.  Roles are collections of Resource specific Permissions (e.g., Read, Comment, Write, Approve, Publish, Remove) |  |  |
|  |  |  |  |  |  |  |  |  |

## Resource Role Allocation

Mature apps permit users to invite other users – even persons who are not yet system users – to accept a Role associated to a Resource.

Users benefit from being able to Apply for, or Accept Role invitations, while other users benefit from functionality to Accept the Application and in turn send out Invitations to Roles to the applicant.

Note:  
Immature systems allow users to only allocate roles to other users, requiring out of system work arounds for recording acceptance of terms and conditions, obligations, etc.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | # | ID | Statement | Rationale | Fit Criteria | Details | Response | Analysis |
|  |  |  | Permitted Users MUST be able to invite and/or allocate Users to Roles specific to a Resource. | Creators of Resources can invite Collaborators to contribute to the Resource.  Users can be invited to Comment and Review draft resources.  Users can be made Maintainers of Approved resources to publish, refresh, replace, and or remove resources. |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

## Resource Routes

A Resource is retrievable via a Route that web servers recognise.

Simple systems use default path parsing to determine the resource to return. Mature systems also provide the means of using one or more Routes to retrieve the same Resource. Different Routes can be developed to give to different Users, each with their own set of Permissions (for an example, see how O365 and Google Apps permit providing Sharing of documents to Persons who are not Users of a System, giving them specific Rights to the Resource).

Most Users of a System benefit from functionality to Share and Un-share Resources with 3rd parties who may or may not be users in the system.

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

Appendices

Appendix A - Document Information

### Images

### Tables

### References

*ICT Project Guidance – Requirement Development*

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

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

### Review Distribution

The document was distributed for review as below:

|  |  |
| --- | --- |
| Identity | Notes |
|  |  |
|  |  |
|  |  |

### Audience

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

### Structure

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

### Diagrams

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

### Terms

Refer to the project’s Glossary.

##### ‘Custom Code’

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

##### Custom Deliverables

: Code & Documentation.

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

##### IT

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

##### ICT

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

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

##### Organisation Provided

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

##### Proprietary Code

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

##### SaaS

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