ICT Project Guidance

Definition:   
Default Baseline System  
Non-Functional Requirements (NFRs)  
[DRAFT]

Version:

0.4

Author:

Sky Sigal, Solution Architect

## Purpose

The purpose of the document is to diminish project delivery risks by listing expected qualities of proposed solution system(s).

## Synopsis

This document lists the expected qualities of systems and services irrespective of whether they are purchasable products, custom development,rentable services, or hosted and operated by suppliers or this organisation’s resources.

## Contents

[Purpose 1](#_Toc158372650)

[Synopsis 1](#_Toc158372651)

[Contents 2](#_Toc158372652)

[Background 5](#_Toc158372653)

[Methodology 5](#_Toc158372654)

[Organisation 6](#_Toc158372655)

[Transitional Requirements 6](#_Toc158372656)

[Abstraction 6](#_Toc158372657)

[Tiering 7](#_Toc158372658)

[Terms 8](#_Toc158372659)

[Quantitative Values 21](#_Toc158372660)

[System Quality Requirements 25](#_Toc158372661)

[Functional Suitability 25](#_Toc158372662)

[Functional Completeness 25](#_Toc158372663)

[Functional Correctness 26](#_Toc158372664)

[Functional Appropriateness 29](#_Toc158372665)

[Performance Efficiency 31](#_Toc158372666)

[Time Behaviour 31](#_Toc158372667)

[Resource Utilisation 32](#_Toc158372668)

[Capacity 34](#_Toc158372669)

[Compatibility 35](#_Toc158372670)

[Co-Existence 35](#_Toc158372671)

[Interoperability 36](#_Toc158372672)

[Integrations 38](#_Toc158372673)

[Usability 40](#_Toc158372674)

[Appropriateness Recognisability 40](#_Toc158372675)

[Learnability 40](#_Toc158372676)

[Operability 41](#_Toc158372677)

[Accessibility 45](#_Toc158372678)

[Reliability 46](#_Toc158372679)

[Maturity 46](#_Toc158372680)

[Availability 46](#_Toc158372681)

[Fault Tolerance 47](#_Toc158372682)

[Recoverability 49](#_Toc158372683)

[Security 50](#_Toc158372684)

[General 50](#_Toc158372685)

[Confidentiality 51](#_Toc158372686)

[Integrity 56](#_Toc158372687)

[Non-Repudiation 58](#_Toc158372688)

[Authenticity 59](#_Toc158372689)

[Accountability 59](#_Toc158372690)

[Maintainability 59](#_Toc158372691)

[General 59](#_Toc158372692)

[Modularity 60](#_Toc158372693)

[Reusability 61](#_Toc158372694)

[Analysability 62](#_Toc158372695)

[Modifiability 63](#_Toc158372696)

[Testability 63](#_Toc158372697)

[Portability 65](#_Toc158372698)

[Adaptability 65](#_Toc158372699)

[Installability 66](#_Toc158372700)

[Replaceability 67](#_Toc158372701)

[Regulations and Agreements 67](#_Toc158372702)

[Data Location 67](#_Toc158372703)

[System Data Quality Requirements 68](#_Toc158372704)

[Inherent Data Qualities 68](#_Toc158372705)

[Accuracy 68](#_Toc158372706)

[Completeness 68](#_Toc158372707)

[Consistency 69](#_Toc158372708)

[Credibility 69](#_Toc158372709)

[Correctness 69](#_Toc158372710)

[Combined Data Qualities 70](#_Toc158372711)

[Accessibility 70](#_Toc158372712)

[Compliance 70](#_Toc158372713)

[Confidentiality 71](#_Toc158372714)

[Efficiency 71](#_Toc158372715)

[Precision 72](#_Toc158372716)

[Traceability 72](#_Toc158372717)

[Understandability 73](#_Toc158372718)

[System Dependent Data Qualities 73](#_Toc158372719)

[Availability 73](#_Toc158372720)

[Portability 74](#_Toc158372721)

[Recoverability 74](#_Toc158372722)

[System User Experience Quality Requirements 75](#_Toc158372723)

[Effectiveness 75](#_Toc158372724)

[Efficiency 75](#_Toc158372725)

[Satisfaction 76](#_Toc158372726)

[Usefulness 76](#_Toc158372727)

[Trust 76](#_Toc158372728)

[Pleasure 77](#_Toc158372729)

[Comfort 77](#_Toc158372730)

[Freedom from Risk 78](#_Toc158372731)

[Economic Risk Mitigation 78](#_Toc158372732)

[Health and Safety Risk Mitigation 78](#_Toc158372733)

[Environmental Risk Mitigation 79](#_Toc158372734)

[Context Coverage 79](#_Toc158372735)

[Context Completeness 79](#_Toc158372736)

[Flexibility 80](#_Toc158372737)

[Transitional Requirements 81](#_Toc158372738)

[Appendices 82](#_Toc158372739)

[Appendix A - Document Information 82](#_Toc158372740)

[Versions 82](#_Toc158372741)

[Images 82](#_Toc158372742)

[Tables 82](#_Toc158372743)

[References 82](#_Toc158372744)

[Review Distribution 82](#_Toc158372745)

[Audience 83](#_Toc158372746)

[Structure 83](#_Toc158372747)

[Diagrams 83](#_Toc158372748)

[Terms 83](#_Toc158372749)

[Appendix B – FAQ 84](#_Toc158372750)

[Appendix C – Requirement Record Template 85](#_Toc158372751)

[Appendix D – Continuous Improvements 86](#_Toc158372752)

[Appendix E - TODO 87](#_Toc158372753)

## Background

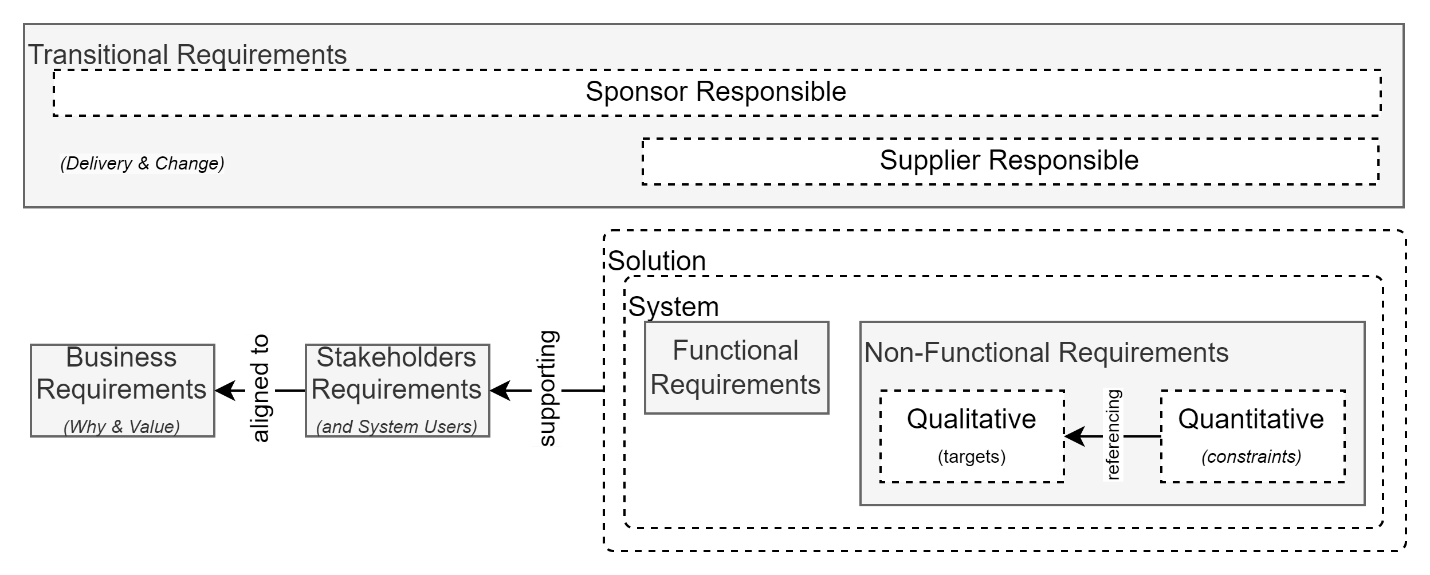


Figure : IIBA's BABOK defined Requirement types

Non-Functional Requirements (NFRs) are one of the 5[[1]](#footnote-2) types of requirements defined within the [International Institute of Business Analysis (IIBA)](#Term_IIBA)’s latest version of the [Business Analysis Body of Knowledge (BABOK)](#Term_BABOK).

NFRs have a notable history of being unclear about their scope, leading to being defined poorly and adding risk to project delivery. The reasons for this are more fully covered in another document [TODO:LINK].

A solution for developing valuable NFRs is following the guidance and organisation defined by ISO-25010, ISO-25012, ISO-25022.

## Methodology

This document was developed according to guidance given within:

* ITC Project Guidance – Definition – Requirements Development
* ITC Project Guidance – Definition – Requirements Development – System Non-Functional Requirements

## Organisation

As per the above, this document’s is structured to first define target *quantitative* values, then the NFRs that reference them, organised as per the International Standards Organisation (ISO)s specific to defining Quality based NFRs:

* *ISO-25010 – Qualities of Systems[[2]](#footnote-3)*, supporting:
* *ISO-25012 – Qualities of [System] Data[[3]](#footnote-4)]*, both supporting:
* *ISO-25022 – Qualities of [System Experience of] Systems in Use[[4]](#footnote-5)*.

## Transitional Requirements

The document concludes by listing a default set of Transitional Requirements.

Transitional requirements are often incorrectly included in NFR documents but require distinction. Specifically, Transitional Requirements do not describe the solution’s system(s) but describe expectations of how the solution is to be delivered, covering setup, collaboration, development, assessment, certification & accreditation, delivery and maintenance expectations.

## Abstraction

The requirements are intentionally abstract for purpose for reuse from project to project, to be of value whether the proposed solution’s system(s) are rented Software as a Service ([SaaS](#Term_SaaS)), purchased Software as a Product ([SaaP](#Term_SaaP)), custom developed, Off the Shelf ([OTS](#Term_OTS)), extendable [platform](#Term_Platform) or not.

The requirements intentionally avoid specific reference to a specific sponsor or supplier organization, specific projects, local conditions and/or internal systems. The objective is to focus on achieving durable and valuable outcomes, adhering to [international](#Value_Standards) and [industry standards](#Value_Standards_Industry), and established maintainable patterns, while minimizing the influence of local and transient limitations.

## Tiering

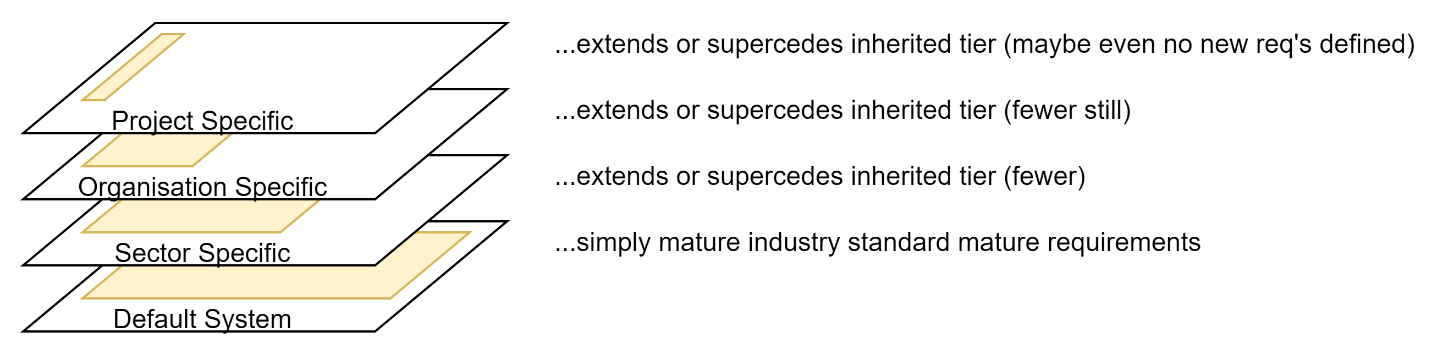


Figure : Hierarchical Stacked Requirements

As described within *ITC Project Guidance – Definition – Requirements Development* there exists a natural tiering of scope.

Requirements benefit from being organised according to tiered Scopes -- each tier extending or superseding one or more requirements inherited from a more general tier.

At the bottom is this document, suitable for use in most scenarios. Projects and/or organisations develops the more specialised overriding requirements documents.

A detailed diagram of these areas co-existing is shown below.

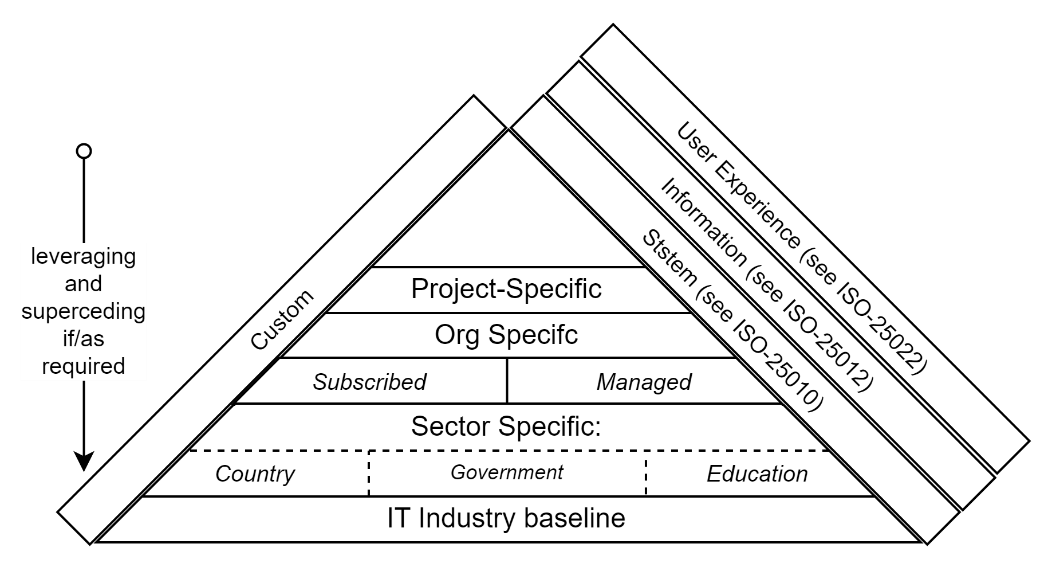


Figure : Pyramid of Requirements

## Terms

[Requirements](#Term_Requirement) are developed using terms that have specific meanings, listed below.

|  |  |  |
| --- | --- | --- |
| **Term** | | **Definition** |
| Acceptance Criteria | The set of individual *Acceptance Criterion*s used to determine if a [Requirement](#Term_Requirement) has been sufficiently met. Sometimes referred to as *[Fit](#Term_Fit)* statements. | |
| Access Level | A system defined collection of permissions. Access levels are often mapped one to one to business roles, so other than in [Role Matrixes](#Term_UserRoleMatrix), people skip the precision and simply call them ‘[System roles](#Term_Role)’. | |

**Acceptance Criteria**

: the set of individual *Acceptance Criterion*s used to determine if a [Requirement](#Term_Requirement) has been sufficiently met. Sometimes referred to as [*Fit*](#Term_Fit) statements.

**Access Level**

: a system defined collection of permissions. Access levels are often mapped one to one to business roles, so other than in [Role Matrixes](#Term_UserRoleMatrix), people skip the precision and simply call them ‘[System roles](#Term_Role)’.

**Agile**

: an oft misunderstood and misapplied delivery methodology, abused to deliver Missing Valuable Planning ([MVP](#Term_MVP)) outcomes.

**Application Programming Interface (API)**

: an interface for use by authenticated remote systems to use as permitted. Contrast with *[user Interface](#Term_UserInterface)*.

**Architecturally Significant**

**[Changes]**

: change to a solution’s [SaaP](#Term_SaaP) system(s) topology, devices, internal component types, [dependent service](#Term_DependentService) integrations, security controls, or privacy or security impacting information.

**Archiving**

: the process of reducing the number of records to find results, by either physical or logical deletion of records[[5]](#footnote-6).

**Atypical**

: a condition outside of a typical condition.

**Authenticated user**

: a [System user](#Term_SystemUser) who has signed into the system. Contrast to [Unauthenticated user](#Term_UnAuthenticatedUser).

**Control**

: limit operations to authenticated and permitted persons or users.

**Custom Code**

: includes any of the following:

* [Custom System Code](#Term_CustomSystemCode),
* [Custom Extension Code](#Term_CustomExtensionCode),
* [Custom Supporting Code](#Term_CustomSupportingCode).

**Average**

: see [Mean](#Term_Mean).

**BREAD**

: an acronym for the most common operations a system user does with data managed by the system: search and/or **B**rowse a [[querable](#Term_Queryable)] set of the record types, **R**ead or view a single record, **E**dit it, add a new one, or [logically] **D**elete an existing one. The acronym is closely related to [CRUD](#Term_Crud) but broader in scope.

**Business Analyst Body of Knowledge (BABOK)**

: developed by the [IIBA](#Term_IIBA), the industry’s authoritative source of guidance on resource elucidation and definition.

**Business Requirements**

: a catalogue of the sponsor’s reasons for a new solution. The *why,* devoid of defining *what* is required, which is defined in [Stakeholder Requirements](#Term_StakeholderRequirements)*.*

**Business Support Specialist**

: a support role dedicated to support business service consumers. Handed off to by a [Customer Support Specialist](#Term_SupportSpecialist).

**Channel**

: a communication pathway between devices and or Persons, using a common protocol or pattern to transmit messages back and forth.

**Claim**

: a [Credential](#Term_Credential) about a person, made by trusted 3rd party (e.g., an [Identity Provider (IdP)](#Term_IdP)).

**CLEAR**

: acronym for characteristics of valuable requirements gathering: Collaborative/Consensus developed, Limited scope, Evaluated, Appropriate, Resource conscience. See [SMART](#Term_SMART) and [Stakeholder Requirements](#Term_StakeholderRequirements).

**ClearText**

: non encrypted text, generally used in the context of discussions about avoiding transmitting confidential credentials over insecure channels.

**Confidential Information**

: any information whose dissemination should be limited and not be openly accessed. Contrast with [Open Information](#Term_OpenInformation).

**Coordinated Universal Time (UTC)**

: the primary time standard. See also [UCS](#Term_UCS) and [UTF](#Term_UTF).

**Credential**

: information about a Person that may be [Open](#Term_OpenInformation) or [Confidential](#Term_ConfidentialInformation). The most common credentials are username (an example of [open information](#Term_OpenInformation)) and Password (an example of [confidential information](#Term_ConfidentialInformation)).

**CRUD**

: an acronym for common operations done to data in a [datastore](#Term_DataStore): Create a new record, Read an existing set of one or more result items, Update an existing record, or Delete an existing set of record. While commonly used, our reference is to use the [BREAD](#Term_Bread) when describing user accessible functionality.

**Custom Extension Code**

: Custom Code commissioned to extend a [SaaS](#Term_SaaS) or [SaaP](#Term_SaaP) [platform](#Term_Platform) with a separately deployed custom functional extension or plugin.

**Custom System**

: a custom [SaaP](#Term_SaaP), developed via [Custom System Code](#Term_CustomSystemCode)*.*

**Custom System Code**

: [Custom Code](#Term_CustomCode) commissioned to develop a [Custom System](#Term_CustomSystem).

**Custom Supporting Code**

: code to develop transitional tasks, including [automation pipelines](#Term_Pipeline) and one or more of the following tasks (depending on whether the system is a SaaS or custom SaaP): [custom system code](#Term_CustomSystemCode) compilation instructions, static testing thereof, packaging, target infrastructure development using [Infrastructure as Code](#Term_InfrastructureAsCode), developing database schemas within developed database infrastructure using [Database Schemas as Code](#Term_DbSchemaAsCode), deploying and unpacking packages on the target infrastructure, configuring integrations between components and/or 3rd party dependency services, initialising the system, configuring all of system settings via [API](#Term_API)s, provisioning reference data, [user](#Term_SystemUser)s and [System Data](#Term_SystemData), and/or performing dynamic tests.

**Data Projection Impact Assessment (DPIA)**

: Includes an [Privacy Impact Assessment (PIA)](#Term_PIA).

**Datastore**

: any store of data within an [environment](#Term_Environment). Includes secure data store, relational databases, non-relational datastores (e.g., blob, table, file, document) and variants, including graph databases.

**Database [Schema] as Code (DsaC/DaC)**

: code to instruct the development of a relational database’s schema within a relational database. See [Infrastructure as Code](#Term_InfrastructureAsCode).

**Distributed Denial of Service (DDoS) Attack**

: a cybercrime in which attackers floods a server with internet traffic from an array of compromised computers they control, to prevent legitimate service consumers from accessing the server’s service.

**Domain Driven Development (DDD)**

: an approach to system definition, design and development that keeps areas of code separated by [domain](#Term_Domain) to promote maintainability and extensibility of systems. Recommended for medium to complex systems[[6]](#footnote-7).

**Dependent Service**

: a system that depends on the service. Term often used to describe a service that relies on an external dedicated 3rd party [IdP](#Term_IdP) service to authenticate [users](#Term_SystemUser).

**Digital Identity**

: A [Person](#Term_Person)’s proof of membership within an external trusted system (often an [IdP](#Term_IdP)). A [system user](#Term_SystemUser) may have one or more external digital identities associated to them. Disambiguate from [Identity](#Term_Identity).

**Disaster Event (DE)**

: a [critical error](#Term_ErrorSeverity) that leads to requiring a [Disaster Recovery](#Term_DisasterRecovery) process being initiated.

**Disaster Recovery (DR)**

: the process of restoring a system to a state usable by system users after a [disaster event](#Term_DisasterEvent). See [RPO](#Term_RPO) and [WRT](#Term_WRT).

**Documentation**

: [systems](#Term_System) require being delivered with accessible documentation sufficient to develop, deploy, integrate, provision, support, operate, and maintain them.

**Domain**

: shorthand for “domain of knowledge”.

**Duty**

: an obligation on a Person within a system, irrespective of accepting a [Role](#Term_Role) or [Responsibilities](#Term_Responsibility). Contrast with [Responsibilities](#Term_Responsibility). Terms and Conditions commonly define Duties.

**Environments**

: a distinct set of infrastructure components developed and assembled to support a single discoverable and addressable service. Environments are deployed to be managed via different network Directory Domain Services (e.g., Active Directory). Only PROD is a Production Data Environment. Environment types are:

- **Test** Directory Domain Service (AD):

- **Build Test (BT)**: for dynamic tests by automation [pipelines](#Term_Pipeline),

- **Developers Test (DT)**: for exploratory testing by developers,

- **System Test (ST)**: for exploratory testing by quality assessors (testers),

- **Production** Directory Domain Service (AD):

- **User [SME] Test (UT)**: for exploratory testing by service user SMEs,

- **Interoperability Test (IT)**: for **integration** testing by remote 3rd parties,

- **Training Environment (TR)**: for training users on system functionality,

- **PreProd Environment (PP)**: final **smoke** test environment prior to PROD deployment,

**Production (PROD)**: a [production data environment](#Term_ProductionDataEnvironment) for use by service consumers.

**Error Severity**

: the severity of system errors is rated as follows:

- **Critical**: system [user](#Term_SystemUser) harm by disclosure, corruption, theft. Or shutdown.  
- **High**: business reputation impact. Or service operation incompletable.  
- **Medium**: business cost impact. Or service operation completion is delayed, or only partially achievable.  
- **Low**: no business risk or service impacts.

**Extract Transform Load (ETL)**

: the process of extracting information from a remote source system – preferably its APIs as opposed to its underlying, non-auditing, [data store](#Term_DataStore)), transforming it to be acceptable to a remote target system, and loading it into it via its audited and validated [API](#Term_API)s.

**Fit**

: see [Acceptance Criteria](#Term_AcceptanceCriteria).

**General Data Protection Regulation (GDPR)**

: Regulation (EU) 2016/679.

**Globally Unique Identifier (GUID)**

: incorrect term for a [UUID](#Term_UUID). Do not use.

**GraphQL**

: an *industry* standard (as opposed to an [*international* standard](#Term_ISO)) based protocol for requesting data from a [queryable](#Term_GraphQL) API endpoint. Note: while similar, GraphQL is not [REST](#Term_REST) compliant. To be internationally standards compliant, a system is expected to provide [ODATA](#Term_ODATA) based APIs first, then (optionally) GraphQL based [API](#Term_API) endpoints.

**GUID**

: an vendor specific term for a UUID. Avoid using, preferring the correct term.

**Identity**

: one of many ways a [Person](#Term_Person) can present themselves within different systems and/or groups. A physical [person](#Term_Person)’s identity may have multiple names used within different groups, as well as a *gender*, not necessarily the same as the Person’s biological *sex* at birth. Identities may have different communication channels (mail, email, phone, SMS, Instagram, etc.) associated to them, as well as a current location (their GPS location, distinct than their address). Disambiguate from Digital Identity. See [Person](#Term_Person).

**Identity Provider (IdP)**

: a service that manages a person’s credentials, and can use them to validate username and passwords, to return access and/or identity tokens that cannot be tampered with and are trusted by a [dependent service](#Term_DependentService), that can be used by [system users](#Term_SystemUser) without disclosing [confidential](#Term_ConfidentialInformation) [credentials](#Term_Credential) to [dependent service](#Term_DependentService)s. A more descriptive term for an IdP might be *“Identity* Token *Provider”*.

**Information Technology & Communication (ITC)**

: the domain of using technology to manage information and communicate it between devices for access by system users.  
Specifically, it is about integrating and orchestrating technology ([infrastructure](#Term_Infrastructure), [data storage](#Term_DataStore), local and remote services) to be put to the use of managing system state data, to in turn manage the communication from and responses back from service clients devices to source information systems of user requests to submit or access data.

**Infrastructure**

: the technology components required to host one or more solution service system(s) in one or more [environments](#Term_Environment). Traditionally developed by hand, current best practice is to build it solely with [Custom Supporting Code](#Term_CustomSupportingCode) ([Infrastructure as Code](#Term_InfrastructureAsCode) and [Database Schema as Code](#Term_DbSchemaAsCode) running within [pipelines](#Term_Pipeline)).

**Infrastructure as Code (IaC)**

: code instructions to build target infrastructure, usually in cloud environments. See [*DsaC*](#Term_DbSchemaAsCode).

**Installed**

: a SaaP. Could be a either a [custom system](#Term_CustomSystem) or finished [Off the Shelf (OTS)](#Term_OTS) product.

**Interface** : may be a [user Interface](#Term_UserInterface) (Graphical (GUI) or Textual (TUI)) for use by [system users](#Term_SystemUser), or Application Programming Interfaces ([API](#Term_API)) for use by third party service consumers to submit Operation *Requests* within a *Session*. See [*View*](#Term_View).

**International Institute of Business Analysis (IIBA)**

: stewards of the [BABOK](#Term_BABOK), the industry source of best practices for requirement elucidation & defining.

**International Standards Organisation (ISO)**

: the international body in charge of developing and maintaining internationally agreed standards, including ones for assessment, development, delivery, storage, transmission, and interoperability.

**Invitations**

: in the case of systems, a part of the process by which a Person – whether already an existing system user or not -- [optionally Applies to] be Invited to Accept a Role within a system, at which point an internal authenticated user record is created [JIT](#Term_JIT) if required. See [JIT](#Term_JIT) and [SCIM](#Term_SCIM).

**ISO-25010**

: international standard defining desirable Qualities of *Systems,* in turn supporting qualities of data (see [ISO-25012](#Term_ISO_25012)), and ultimately user experience (see [ISO-25022](#Term_ISO_25022)).

**ISO-25012**

: international standard defining desirable Qualities of System *Data*.

**ISO-25022**

: international standard defining desirable Qualities of the Experience users have when using *Systems* (see [ISO-25010](#Term_ISO_25010)) to access and manage *Data* (see [ISO-25012](#Term_ISO_25012)).

**ISO-27001 Information Security, Cybersecurity and privacy protection**

: guidance for companies of any size and from all sectors of activity on establishing, implementing, maintaining and continually improving an information security management system.

**Important:** While *Level 1* means a company has self-assessed their capability of adhering to ISO-27001 outcomes, *Level 2* indicates the assessment has been done *by an independent 3rd party.*

**Just In Time (JIT)**

: in the case of system user creation, this means than the creation of an internal authenticated [system user](#Term_SystemUser) record is deferred until an user authenticates themselves and actually begins using the system. Most often associated to [Invitations](#Term_Invitation). See [SCIM](#Term_SCIM).

**Logical Deletion**

: the act of changing a state flag on a record to remove it from future returns. Often the basis of providing end users Undo capabilities. See [Archiving](#Term_Archiving).

**Logical State Change**

: a flag-based method of controlling the inclusion of records in search operations. See [Archiving](#Term_Archiving) , [Logical Deletion](#Term_LogicalDelete) and [workflow](#Term_Workflow) management.

**[Logical] User Role Catalogue**

: a list or catalogue of logical roles, used to develop a [Logical User Role Matrix](#Term_LogicalUserRoleMatrix).

**[Logical] User Role Matrix**

: developed from a [Logical User Role Catalogue](#Term_LogicalUserRoleCatalogue), a matrix of logical roles to logical permissions. Used to develop RFPs. Based on Respondents, progressed to a [[System] User Role Matrix](#Term_UserRoleMatrix).

**Mail Server**

: combination of an [MTA](#Term_Mail_MTA) and [MDA](#Term_Mail_MDA).

**Mail Delivery Agent (MDA)**

: most [email servers](#Term_MailServer) are both an [MTA](#Term_Mail_MTA) and an [MDA](#Term_Mail_MDA), but most services don’t receive messages, only send them, so only need integration to [MTA](#Term_Mail_MTA) functionality (using SMTP, not POP/IMAP).

**Mail Transfer Agent (MTA)**

: most [email servers](#Term_MailServer) are both an [MTA](#Term_Mail_MTA) and an [MDA](#Term_Mail_MDA), but most services only require integration with the [MTA](#Term_Mail_MTA) part (using SMTP, not POP/IMAP).

**Majority**

: the mid value of a data set, plus a small value (e.g., +1). See [Qualified Majority](#Term_QualifiedMajority), [Mean](#Term_Mean) and [Median](#Term_Median).

**Maximum Allowable System Outage (MASO)**

: TODO

**Maximum Tolerable Downtime (MTD)**

: the duration of time between an event and when users can return to using the system. It is composed of RTO plus WRT.

**Maximum Allowable Data Low (MADL)**

: See [RTO](#Term_RPO).

**Mean**

: the result of summing all numbers in a data set and dividing them by the number of values in the set. See [Average](#Term_Average) and [Quartile](#Term_Quartile). Contrast with [Median](#Term_Median).

**Media**

: text, images, sound, video, 3d models, virtual experiences uploaded to systems, usually described using [metadata](#Term_Metadata) records for later re-discovery.

**Median**

: the middle value when a data set is ordered from least to greatest. See [Midway Point](#Term_MidwayPoint). Contrast with [Mean](#Term_Mean).

**Metadata**

: information about another entity (in the context of [systems](#Term_System), this is often [media](#Term_Media)). Metadata for [resource](#Term_Resource)s may include but is not limited to:

* Classification (Security, Curriculum, etc.)
* State (Draft, Rejected Accepted, Released, etc.),
* Technical (Size, Dimensions, Type)
* Source Information (Original Name, Source Identifier(s), GPS coordinates, etc.)
* Current Context (Folder, Tags)
* Description (Title, Description)
* Content (Summary)

**Midway Point**

: See [Median](#Term_Median) and [Quartile](#Term_Quartile). Contrast with [Average](#Term_Average).

**Multi-Page App (MPA)**

: a traditional approach to developing service graphical user interfaces (GUIs), developing a new view on the server for each request. Consumes more resources. Contrast with [SPA](#Term_SPA).

**Multipurpose Internet Mail Extensions (MIME) type**

: as defined by RFC 2045, the nature and format of a document.

**MVP**

: acronym for *Minimum Viable Product*, but too often -- due to a fundamental misunderstanding and misapplication of [Agile](#Term_Agile) methodologies -- becomes instead the acronym for *Missing Valuable Planning*.

**Non-Functional Requirements**

: requirements defining the system, data and user experience quality obligations.

**Non-Production Data Environment**

: [environments](#Term_Environment) whose datastores contain test data specifically developed to test and/or demonstrate system functionality. Best practice is to NEVER use production data, even if it is truncated, obfuscated, or old. Contrast with [Production Data Environment](#Term_ProductionDataEnvironment).

**OAuth**

: an HTTP/S based authentication standards. See [OIDC](#Term_OIDC).

**ODATA**

: an [international standards](#Term_ISO) based [querable](#Term_Queryable) extension to [REST](#Term_REST) based [APIs](#Term_API). See [GraphQL](#Term_GraphQL).

**Off the Shelf (OTS)**

: a [SaaP](#Term_SaaP) that is not a [Custom System](#Term_CustomSystem).

**On-Premises System**

: see [Self-Hosted](#Term_SelfHosted) System.

**Open Identity Connect (OIDC)**

: an [OAuth](#Term_OAuth) based *authentication* (as opposed to *authorisation*) system.

**Open Information**

: information that is openly accessible. Contrast with [Confidential Information](#Term_ConfidentialInformation).

**Operation**

: an act within a [system](#Term_System) requested by a [user](#Term_SystemUser) within a session. Most often the act is one to Browse, Read/View, Edit, Add, Delete (BREAD) a Resource.

**Organisation Managed**

: the service’s systems are purchased, installed and managed on [Sponsor Organisation](#Term_SponsorOrganisation)’s infrastructure. Contrast with the [SaaS](#Term_SaaS) based services.

**OWASP**

: The *Open Worldwide Application Security Project[[7]](#footnote-8)* is a non-profit Foundation that both publishes the “Top Ten” security risk report and the WAF “Core Rule Set”.

**Platforms as a Service (PaaS)**

: cloud infrastructure that is managed as a service platform. Not to be confused with [SaaP](#Term_SaaP).

**Permission**

: a credential that a [system user](#Term_SystemUser) may have that is verified by a [system](#Term_System) before it grants an operation requested by the user.

**Person**

: a physical or juridical entity, that may have multiple Identities, may be a [system user](#Term_SystemUser) and become authenticated within the system using one or more digital identities developed by trusted 3rd party systems.

**Personal Data**

: as per the GDPR “Any information relating to an identified / identifiable individual, whether it relates to his or her private, professional, or public life. Can be anything from a name, photo, email address, bank details, posts on social networking sites, medical information, IP address, or a combination of the data that directly or indirectly identifies the person.”. See Sensitive Personal Data.

**Privacy Impact Assessment (PIA)**

: a process to identify and manage risks to privacy of persons. An sub aspect of a [Data Projection Impact Assessment (DPIA)](#Term_DPIA).

**Pipeline [Automation]**

: custom developed automation logic to do any one or more of the following: [Custom System Code](#Term_CustomSystemCode) Compilation, Static Testing, Packaging, Infrastructure creation, Deployment, [Integration] Configuration, [System Settings] Setup, [Users & Data] Provisioning, and/or Dynamic Testing.

**Platform**

: in the context of software, a [SaaS](#Term_SaaS) or [SaaP](#Term_SaaP) [system](#Term_System) to which can be deployed extensions developed by 3rd parties without assistance from the service’s developers. In the case of infrastructure, a platform that can be remotely managed to create, configure, monitor, and remove infrastructure without assistance from the infrastructure provider – mostly cloud infrastructure and services providers.

**Production Data**

: data developed by business service consumers and business service providers within a [Production Data Environment](#Term_ProductionDataEnvironment). It **must** not be used as a source for [Test Data](#Term_TestData).

**Production Data Environment**

: an [environment](#Term_Environment) that contains [datastores](#Term_DataStore) of production data. Best practice is to only have one [environment](#Term_Environment) (PROD) be a production data environment. Contrast with [Non-Production Data Environment](#Term_NonProductionDataEnvironment).

**Project**

: an attempt to accomplish set objectives within resource constraints.

**Qualified Majority**

: a specified (e.g., 90%) [majority](#Term_Majority). See [Mean](#Term_Mean) and [Median](#Term_Median).

**Quartile**

: a single interval within a set of data divided into four intervals. Depending on analysis purpose, the quartiles can be either contain the same number of items, or same sum of numbers. See [Mean](#Term_Mean) and [Median](#Term_Median).

**Queryable**

: a data set that can be filtered, projected, sorted, paged. See ODATA.

**RASCI**

: acronym for level of responsibility towards a task: Responsible (for doing the work), Accountable (managing the allocation of the task), Supporting (can include task dependencies), Consulted, Informed, [Ignored].

**Record**

: a single structured unit of data within a dataset within in a solution’s system datastore, (often a relational database). Can be used to record information about the system (diagnostics, errors, configuration, settings, state, process step, etc.), system purpose records (people, suppliers, invoices, payments, student assessment scores, etc.), or categorisation of a Resource.

**Recovery Point Objective (RPO)**

: the maximum duration of time since the last system data [incremental] backup and disaster event occurred. It effectively reflects the maximum data loss considered acceptable in the case of a disaster event. See [MADL](#Term_MADL).

**Recovery Time Objective (RTO)**

: the maximum duration of time between the occurrence of a disaster event and system recovery. Does not include [WRT](#Term_WRT).

**Requirement**

: comprised of a [Statement](#Term_Statement), *Rationale* and associated [Acceptance Criteria](#Term_AcceptanceCriteria) and optional details.

**[System] Resource**

: in the context of technology, could refer to hardware, devices, applications, files, or even virtual assts such as network bandwidth or processing power.   
In the context of system data refers to [media](#Term_Media) uploaded to the system, stored as a [record](#Term_Record) or otherwise, tracked with a [metadata](#Term_Metadata) [record](#Term_Record).

**Responsibility**

: an obligation accepted by a Person when accepting a [Role](#Term_Role) in a System. Contrast with [Duty](#Term_Duty).

**Representative State Transfer (REST)**

: a software architecture that imposes conditions on how APIs are expected to work. See [ODATA](#Term_ODATA) and GraphQL.

**Resource**

: TODO

**Role**

: a collection of system [Permission](#Term_Permission)s issued to a [system user](#Term_SystemUser) when they accept the Role’s [Responsibilities](#Term_Responsibility). Depending on the [system](#Term_System), purpose and design maturity, roles are generally developed as:

* System based (SystemSuperuser, SystemMember, etc.),
* Tenancy based (TenancySuperuser, TenancyMember, etc.),
* Group based (Accountable, Responsible, Member, Consulted, Informed, Guest, etc.), or
* Resource based (Creator, Contributor, Approver, Maintainer, Commentor, Reader, etc.).

**Salt**

: a salt, in the context of confidential storage, is a piece of random data added to a password before it is hashed and stored.

**Self-hosted**

: see [Software as a Product](#Term_SaaP) ([SaaP](#Term_SaaP)).

**Sensitive Personal Data**

: Special categories of personal data. The special categories of data include racial or ethnic origin, political opinions, religious or philosophical views, trade union membership, sexual orientation, and health, genetic and biometric data where processed to uniquely identify an individual. Personal data relating to criminal convictions and offenses are not included, but similar extra safeguards apply to its processing. See [Personal Data](#Term_PersonalData).

**Session**

: a sustained stateless logical connection between a service consumer and a service provider [system](#Term_System) -- during which the service consumer (e.g., [system user](#Term_SystemUser)) performs multiple permitted [operations](#Term_Operation).

**Single Page Application (SPA)**

: a current form of developing service clients, as a single html page containing all view templates, hidden till required when they are populated with data retrieved from APIs. Consumes far less resources on the server side. Contrast with a [Multi-Page Applications (MPA)](#Term_MPA) approach.

**SMART**

: acronym for the properties of valuable requirement gathering/eliciting: **S**ingular, **M**easurable, **A**chievable, **R**elevant, **T**ime/Resource constrained. See [CLEAR](#Term_CLEAR) and [System Requirements](#Term_SystemRequirements).

**Software as a Product (SaaP)**

: software that is purchased, either as a pre-existing product sold to many, or commissioned as a [Custom System](#Term_CustomSystem) sold to just one (the [Sponsor’s Organisation](#Term_SponsorOrganisation)). A [SaaP](#Term_SaaP) is [self-hosted](#Term_SelfHosted), deployed by [Sponsor Organisation](#Term_SponsorOrganisation) resources infrastructure they manage (“On Premise”), whether that is in the building, on traditional data centre infrastructure or modern cloud provider infrastructure. Not to be confused with [PaaS](#Term_PaaS).

**Software as a Service (SaaS)**

: “Software as a Service” is an example of [Vendor Managed](#Term_VendorManaged). Contrast with [Software as a Product](#Term_SaaP).

**Software as a Product (SaaP)**

: software developed as custom code for one consumer, by a [Supplier](#Term_Supplier), or many, as a Product, sold by a [Vendor](#Term_Vendor).

**Solution or System Requirements**

: a logical grouping of a Solution or System’s [Functional Requirements](#Term_FunctionalRequirements) and [Non-Functional Requirements](#Term_NonFunctionalRequirements).

**Sponsor Organisation**

: the Organisation that is purchasing the solution.

**Stakeholder Map**

: map of stakeholders’ [RASCI](#Term_RASCI) relationship to a [project](#Term_Project). Along with a user persona catalogue, is used to develop [Stakeholder Requirements](#Term_StakeholderRequirements).

**Stakeholder Requirements**

: a catalogue of Stakeholders desires of *how* they can contribute to meeting the *why* of [Business Requirements](#Term_BusinessRequirements), while not yet analysing *what* needs to be made available to support what they do (see [System Functional Requirements](#Term_FunctionalRequirements)).

**Statement**

: in the context of [Requirements](#Term_Requirement), a Statement is a short [SMART](#Term_SMART) instruction that is either an Obligation (**must**), Recommendation (**should**), Permission (**could**) or Prohibition (**must** **not**). For Valuable requirements, a 90+% [supermajority](#Term_Supermajority) of statements are Obligations or Prohibitions, avoiding the uncertainty of Recommendations and Permissions.

**Supermajority**

: a qualified [majority](#Term_Majority) (e.g., “90% majority”).

**Support Specialist**

: a customer support specialist role managing calls from authenticated and non-authenticated users, passing the call on to [Business Support Specialist](#Term_BusinessSupportSpecialist), [Operational Specialists](#Term_OperationsSpecialist) or [Maintenance Specialist](#Term_MaintenanceSpecialist) roles as required.

**Supplier**

[Organisation] : a distributor of [vendor](#Term_Vendor) products or SaaS services, optionally providing one or more of licensing, configuring, customising, developing [custom code](#Term_CustomCode), deploying, and/or provisioning *services.*

**Supplier Managed**

: the service is rented by the [sponsor’s organisation](#Term_SponsorOrganisation), installed on the [supplier’s](#Term_Supplier) preferred infrastructure – cloud or otherwise -- and managed by [supplier](#Term_Supplier) staff. [SaaS](#Term_SaaS) is an example.

**System**

: a [SaaS](#Term_SaaS) or [SaaP](#Term_SaaP) for providing a service to system [users](#Term_SystemUser) as part of a solution.

**System Data**

: data persisted in the system. Comprised of both [System Operations Data](#Term_SystemOperationsData) and [[System] User Data](#Term_UserData).

**System for Cross-Domain Identity Management (SCIM)**

: an open standard for provisioning [system users](#Term_SystemUser). See [JIT](#Term_JIT).

**System Media**

: media (text and images) that is deployed with the system, by system maintenance specialists. Updates require a new release to be deployed. Contrast with [user media](#Term_UserMedia).

**[System] Functional Requirements**

: a catalogue of the Functionality required of a system to address [Stakeholder Requirements](#Term_StakeholderRequirements). Combined with [Non-Functional Requirements](#Term_NonFunctionalRequirements) comprise the [Solution or System Requirements](#Term_SystemRequirements).

**[Systems] Maintenance Specialist**

: a role to manage the deployment, logging, configuration, provisioning, data backups, data restorations of a system. May be invoked by [System Operation Specialists](#Term_OperationsSpecialist) to investigate issues.

**[****System] Operations Data**

: data required to maintain and record system state. Includes data used for Diagnostics, Error Recording, System Settings, [Session](#Term_Session) recording, Session Operations recording, System [Permission](#Term_Permission)s, [System, Group, Resource] [Role](#Term_Role)s, Tenancies, System Users, System User [external] Digital Identities, User Settings Profile, User Grouping, Group Nesting, [Role](#Term_Role) [Applications, Invitations, Acceptances, Approvals], and/or Associations, etc.

**[System] Operations Specialist**

: a role that manages the system’s settings common to all tenancies and/or users, which a [Customer Support Specialist](#Term_SupportSpecialist) or [Business Service Support](#Term_BusinessSupportSpecialist) specialist might handle.

**[System] User**

: an unauthenticated or authenticated Person or remote System accessing the System.

**[System] User Role Matrix**

: a matrix of user roles to system Permissions.

**Test Data**

: data specifically prepared for testing system functionality. It **must** not be developed from [production data](#Term_ProductionData), *even* if obfuscated or truncated. The only form of [system data](#Term_SystemData) permitted in environments other than [production data environments](#Term_ProductionDataEnvironment).

**Transitional Requirements**

: requirements for how to transition from a current state to a desired future state where the solution is available for use by users. They do not describe solution’s system(s) qualities and therefore are separate from [System Requirements](#Term_SystemRequirements). They do not cover just a ‘transition to BAU’ phase – they cover Transitional Tasks prior and through the project’s discovery, design, development, delivery, provisioning, operating and decommissioning concerns.

**Transitional Tasks**

: tasks to move from the current state to the target state where users can use the solution’s system(s).

**Typical**

: the average of the context.

**Unauthenticated User**

: a public system user who can only access publicly accessible resources, who has not yet signed into the system. Contrast to [Authenticated User](#Term_AuthenticatedUser).

**Universal Product Code (UPC)**

: a barcode symbology used worldwide.

**User Digital Identity**

: some systems permit a [system user](#Term_SystemUser) identify themselves to the system by associating themselves to one or more user Identities within trusted external [Identity Providers (IdP)s](#Term_IdP).

**User Data**

: data and [user media](#Term_UserMedia) entered by [system users](#Term_SystemUser).

**User Media**

: media (text, images, documents) uploaded to the system after deployment, during normal use, by authorised [system users](#Term_SystemUser). Contrast with [System Media](#Term_SystemMedia).

**User Interface (UI)**

: a *Textual User Interface* (TUI or “console”) or *Graphical User Interface (GUI)* composed of a series of navigable sets of nested [View](#Term_View)s.

**View**

: a logical grouping of related input fields, action buttons and output within a *Graphical User Interface* (GUI) type of [User Interface](#Term_UserInterface), often rendered in a *Window*.   
The term *Screen* or *Page* is often incorrectly used.

**Universal Coded Character Set (UCS or Unicode)**

: Standard set of internationally defined characters. See ISO-10646. See also [UTF](#Term_UTF) and [UTC](#Term_UTC).

**Unicode Transformation Format (UTF)**

: encoding to represent any character for storage, transfer and display. See also [Unicode/UCS](#Term_UCS) and [UTC](#Term_UTC).

**Universal Unique Identifier (UUID)**

: Correct term for a unique 128-bit value used as an identifier. Use for storage and transmission identifiers. **Do** **not** use the [vendor](#Term_Vendor) proprietary term “[GUID](#Term_GUID)”.

**User Personas**

: catalogue of user types that will use the system. Several user personas can share the same [Permissions](#Term_Permission) and [Role](#Term_Role) but have different use cases. Informs the development of a [logical user roles catalogue](#Term_LogicalUserRoleCatalogue), which in turn is used to develop a [logical user role catalogue](#Term_LogicalUserRoleCatalogue).

**Vendor [Organisation]**

: create, distribute, update and support their own *products* sold directly to customers or businesses.

**Vendor Managed**

: services installed and managed on Vendor selected infrastructure. [SaaS](#Term_SaaS) is an example of such ([SaaP](#Term_SaaP) is not).

**Work Recovery Time (WRT)**

: duration of time used to verify system functionality after a Disaster Recovery has completed system recovery, presumably within its [RTO](#Term_RTO) constraints.

**Workflow**

: a managed sequence of operations on records by different [roles](#Term_Role). For example, onboarding a user to a specific role may be an efficient sequence of an external public Person *Apply* for a system [role](#Term_Role), a permitted user receiving the Application request deciding to proceed to issuing an [Invitation](#Term_Invitation), which when accepted by the public person signals the Service to JIT create a system user record for the new person, and immediately associate it to the role in question.

# Quantitative Values

The following is a table of *quantities* referenced form the *qualities*-based statements within the Requirements defined next, and subsequent/downstream requirement documents.

| **Term** | **Description** | **Value** | **Comments** |
| --- | --- | --- | --- |
| [Sponsor Organisation](#Term_SponsorOrganisation) | The organisation that is contracting the solution. | New Zealand  Ministry of Education |  |
| Expected Service Lifespan | The duration the solution’s system(s) will be expected to be available. | 7 years | This duration starts from the date of first release. |
| Operating Jurisdictions |  | New Zealand | While systems are accessible from any country, the laws of the country where the sponsor organisation is registered apply. |
| Regulations |  | NZ Public Records Act 2005  NZ Privacy Act 2020 |  |
| Agreements |  |  |  |
| Delivery Cultures | language codes [users](#Term_SystemUser) can chose from to render [System Media](#Term_SystemMedia). | - en/[NZ,GB,US] - mi/NZ | Expressed in ISO-639x codes. |
| Service Criticality |  | **Tier 2 of 5** |  |
| Service Availability Period | Availability can be measured per Month or Year. | **Month** | The service is required all the time, so it is relatively non-sensical to measure per year. |
| Availability | Percentage a system must be available per [Service Availability Period](#Value_ServiceCriticalityPeriod). | **99.5%** | Downtime per year/month/day:  - 99.9%:  - 8.77h/43.83m/8.64secs  - 99.5%  - 1.84d/3.65h/7.2mins  - 99%:  - 3.65d/7.31h/14.40mins  **Note:** For example, Azure services are generally 99.9% or better. Assuming service is dependent on 5 different components or services, the compounded value is: 99.9% x 99.9% x 99.9% x 99.9% x 99.9% = 99.501% |
| Upgrade Window | The maximum delay permitted to defer the updating system, components, and cryptographic algorithms to required targets. | 6 months |  |
| Max users | The expected maximum number of users registered in the system, whether active in the last 12 months or not. | 20% of the country’s population, or 1 million, whichever is the higher. |  |
| Concurrent Sessions | The number of concurrent users who are individually making requests within a minute. | 10% of Max users | 100,000 |
| Concurrent Requests | The number of requests per second. | 10% of Concurrent Sessions |  |
| Operation Response Times |  | 0.25 second | Excludes Network Latency. An operation that will take longer than this duration would be queued. |
| Operation Completion Duration | The maximum time permitted to complete an operation. | 20 seconds | No queued or immediately processed operation will take longer than this duration. |
|  |  |  |  |
| View Response Times | Time to render a new view. | 1 second | Excludes Network Latencies. |
|  |  |  |  |
| Acceptable Percentage of Resources Consumed | The percentage of available resources required to meet availability and responsiveness targets. | 33% | Applies to memory, CPU, storage.  TODO: Network may need a different metric. |
| [RPO](#Term_RPO) | Recovery Point Objective | 15 Minutes | A Disaster Recovery will recover all data saved prior to this interval before an incident occurred. |
| [RTO](#Term_RTO) | Recovery Time Objective | 12 hours | A Disaster Recovery will re-enable the infrastructure system and data within this time duration after an incident. |
| [WRT](#Term_WRT) | Work Recovery Time | 12 hours | This is the duration of time after a system is recovered (its RTO) to test that the system is fit for purpose by end [users](#Term_SystemUser). |
| [MTD](#Term_MTD) | Maximum Tolerable Downtime | 24 hours | The combined sum of the RTO + WRT intervals. |
| International Standards to Adhere To |  | - character set:  ISO-10646 - date/time encoding:  ISO-8601  - country codes:  ISO-639x - UUIDs:  ISO-98348:2014  - OAuth:  RFC 6749 - OData:  ISO-20802 - WCAG:  ISO-40500:2012 - Qualities:  ISO-25010/12/22 - Information Security:  ISO-27001 stage 2+ - HTML (5):  ISO-15445 - ECMAScript:  ISO-16262 |  |
| Industry Domain Standards & Patterns |  | OIDC API-First Continuous Delivery |  |
| Industry Domain *Custom* Development Standards & Patterns |  | DevOps Domain Driven Design SOLID, TDD | Only applicable to Solution System(s) that are [Custom System](#Term_CustomSystem) [SaaP](#Term_SaaP)s. |
| Data Interchange Standards |  | Custom Sponsor Organisation defined modelling and messaging standard. |  |
| Integrated Systems |  | Sponsor’s IdP. Sponsor’s MTA. |  |
| Sector Guidance |  | NZ Secure Web Services Standard Compliance. |  |
| Error Severity Acceptance | 0 Critical 0 High |  |  |
| Sponsor Guidance |  | - Domain Naming Guidelines - Accessibility Guidelines - Usability Guidelines - Interface Design Guidelines - Monitoring Guidelines |  |
| Supplier and/or Vendor Qualifications |  | [ISO-27001](#Term_ISO_27001) Level 2 |  |

# System Quality Requirements

The following Qualitative requirements are organised per the guidance provided within ISO-25010 System Requirements, with Statements referring to target values defined within the Quantitative Values listed below.

### Functional Suitability[[8]](#footnote-9)

The degree to which a product or system provides functions that meet stated and implied needs when used under specified conditions. This characteristic is composed of the qualities listed below.

#### Functional Completeness

The degree to which the set of functions covers all the specified tasks and user objectives.

##### QR-DEF-FUNC-COMP-00: **Comprehensive Functionality**

**Category**: ISO-25010/Functionality Suitability/Functional Completeness

**Statement**: The solution’s system(s) MUST provide a comprehensive set of features to address the diverse needs of default conceptual [user](#Term_SystemUser) [role](#Term_Role)s.

**Rationale**: A comprehensive set of features enhances [user](#Term_SystemUser) satisfaction and efficiency.

**Details**:

**Prompts:** Which of the above listed standard conceptual user [role](#Term_Role)s does the system provide functionality for?

##### QR-DEF-FUNC-COMP-00: **System Functionality**

**Category**: ISO-25010/Functional Suitability/Functional Completeness

**Statement**: The solution’s system(s) **must** provide mature underlying system functionality.

**Rationale**: A solution that concentrates too much on business requirements is at risk of not being supportable, operable, monitorable, maintainable by other stakeholders over its service lifespan.

**Details**: …

**Prompts:** Recognising that not all services provide functionality to manage the following, it remains important for consideration and evaluation purposes to know which of the following functionality is provided by the solution’s services:  
- Integration Configuration  
- Diagnostics Tracing  
- Error Recording  
- System Configuration  
- [Session](#Term_Session) & Session Operation Auditing  
- User Management  
- System [Permission](#Term_Permission) & [Role](#Term_Role) Management  
- User System [Role](#Term_Role) application/invitation/acceptance/allocation Management  
- Tenancy Management  
- Group Management  
- Group [Role](#Term_Role) Management  
- User Group [Role](#Term_Role) application/invitation/acceptance/allocation Management  
- Resource Management  
- Resource [Role](#Term_Role) Management  
- User Resource [Role](#Term_Role) application/invitation/acceptance/allocation Management  
- Resource Collection Management  
- Resource Collection [Role](#Term_Role) Management  
- Resource Collection [Role](#Term_Role) application/invitation/acceptance/allocation Management  
  
**Note:** All of the above functionality is not related to any specific business domain - just the underlying system domain.

##### QR-DEF-FUNC-COMP-00: **Functionality Dependencies**

**Category**: ISO-25010/Compatibility/Usability

**Statement**: Solution service(s) **must not** require integration with a 3rd party service to provide end-user accessible functionality missing from the service itself.

**Rationale**: Using an external service to provide core services is poor practice.

**Details**: An example of this is requiring an external service (e.g., an [IdP](#Term_IdP)) to provide missing [role](#Term_Role) management and assignment capabilities.

**Prompts:** Does the service rely on 3rd party services for user interaction to manage [role](#Term_Role)s, rules, [workflow](#Term_Workflow)s, or other?

#### Functional Correctness

The degree to which a product or system provides the correct results with the needed degree of precision.

Large organisations and national services require mature systems that correctly model scenarios common to their scale that may not be required for very small entities.

##### QR-DEF-FUNC-COR-00: **Universality**

**Category**: ISO-25010/Functionality Suitability/Functional Correctness

**Statement**: The solution **must** use Universal Types, Codes and Encoding.

**Rationale**: Solution system(s) will be located within different time zones than the locations where the solution’s service(s) will be used in multiple languages.

**Details**: Use [UTC](#Term_UTC) based date and time types. Do not use Epoch (1970) or similar legacy solutions to use less data when saving information but have proven to be unreliable even when wrapped with further instruction.  
Use [UNICODE](#Term_UCS) based character displays for storage and display and UTF for transmission (UTF-8). Umlauts, macrons, and all language specific characters must be preserved, transmitted and validated correctly.  
Use universal code sets where they exist. For example, [MIME](#Term_MIME), [UPC](#Term_UPC), etc..  
Use [UTF](#Term_UTF) for transmission. If not available on a service, suggest an equivalent for approval.  
[UUID](#Term_UUID)s are the recommended design approach for the development of datastore index keys on different servers. Database incremented Numbers are not.   
If [custom system](#Term_CustomSystem), the recommended approach for the creation of database clustered key indexes is the use of [UUID](#Term_UUID)s that are time + random based [UUID](#Term_UUID)s (see [UUID](#Term_UUID)v6[[9]](#footnote-10)), generated on the application server tier – not the database tier.

**Prompts:** To support flexibility of installation and scalability supporting availability, do the solution’s system(s) use universal types for record identity and time?

##### QR-DEF-FUNC-COR-00: **Role as Permission Sets**

**Category**: ISO-25010/Functional Suitability/Functional Correctness

**Statement**: The solution system(s) [Role](#Term_Role)s **must** be [Permission](#Term_Permission) based.

**Rationale**: It is our experience that a key indicator of the appropriateness and evolvability of a system over time is the correct modelling of [users](#Term_SystemUser) and [Role](#Term_Role)s both within and outside of an enterprise context, where service consumers and partners exist.

**Details**: [Role](#Term_Role)s are simply not granular enough to model real world conditions.  
Instead, it is important to recognise that [Role](#Term_Role)s as logical sets of one or more [Permission](#Term_Permission)s, granted in exchange for [users](#Term_SystemUser) accepting the [Responsibilities](#Term_Responsibility) associated to them.

**Prompts:** Are the solution’s system(s) capable of developing [Role](#Term_Role)s from [Permission](#Term_Permission)s?   
Can custom variations be developed by adding or removing specific [Permission](#Term_Permission)s while assigning [Role](#Term_Role)s to Persons (e.g., both the Accountant and Assistant Accountant have the same [Role](#Term_Role), but the Assistant Account has an overrider that the [Permission](#Term_Permission) to sign cheques above $5000 is removed).

##### QR-DEF-FUNC-COR-00: **Information Deletion**

**Category**: ISO-25010/Functional Suitability/Functional Correctness

**Statement**: The Solution’s Service(s) **must** not physically delete information.

**Rationale**: Correct handling of data is based on logical state-based versioning of records, not deletion.

**Details**: Physical deletion of data was recommended when storage was more expensive, and security and auditability were considered a secondary concern. Logical state changes (Draft, Rejected, Approved, Released, Replaced, Restored, etc.) is the current recommended best practice.  
**Important:**   
Deletion of Personal Data (e.g., see Right to be Forgotten) is done by anonymising data, by deleting Identifying attributes of the System [user](#Term_SystemUser), and any data within records associated to the user.

**Prompts:** Does the solution’s services physically delete or logically delete records?  
Can changes be undone?

##### QR-DEF-FUNC-COR-00: **Time Bound Relationships**

**Category**: ISO-25010/Functional Suitability/Functional Correctness

**Statement**: The solution’s system(s) Reference Data, Resources and Relationships **must** be time bound with start and end dates.

**Rationale**: In many business domains (e.g., education), operational change management is simplified and less execution errors occur when change can be done beforehand but scheduled to take effect or terminate at a specific date in the future (e.g., next term start).   
The same for [Role](#Term_Role) allocations as they may be issued early, but only take effect at a future date (e.g., beginning of the next month or start of the next term).  
Both system and [users](#Term_SystemUser) provided resources are similar. New material (e.g., new teaching curriculums and associated resources) may be developed earlier, but only published and made available at a future date.  
For security reasons, while [Role](#Term_Role) associations could have undefined end dates for permanent staff, it is not a recommended approach. Instead, always setting an end date and raising reminders to appropriate [Role](#Term_Role)s that the association is soon coming to an end, permits extending them easily while not leaving risks associated to forgotten ex-employees still having [Role](#Term_Role)s.

**Details**: Reference data will require Start and End dates to control their availability for rendering and selection by UIs.

**Prompts:** What Reference Data is offered by systems that has time constraints?  
What Reference Data is offered without the option to preset them?

##### QR-DEF-FUNC-COR-00: **Metadata**

**Category**: ISO-25010/Functional Correctness

**Statement**: Records and Resources are categorisable and discoverable by [Metadata](#Term_Metadata).

**Rationale**: Discovery is improved, improving operability and efficiency.

**Details**: The [term](#Term_Metadata) lists common metadata fields to consider.

**Prompts:** What records & resources are organisable by [metadata](#Term_Metadata)?  
What records & resources are not?

#### Functional Appropriateness

The degree to which the functions facilitate the accomplishment of specified tasks and objectives.

##### QR-DEF-FUNC-COR-00: **Role Association**

**Category**: ISO-25010/Functionality Suitability/Functional Correctness

**Statement**: The solution system(s) **must** permit [users](#Term_SystemUser) to apply for being invited to [Role](#Term_Role)s rather than be unilaterally allocated [Role](#Term_Role)s.

**Rationale**: It is our experience that a key indicator of the appropriateness and evolvability of a system over time is a correct modelling of [users](#Term_SystemUser) and [Role](#Term_Role)s both within and outside of enterprise contexts, where service consumers, suppliers and partners exist.  
  
Such that [users](#Term_SystemUser) are not allocated [Role](#Term_Role)s, but that [users](#Term_SystemUser) may apply for them, and other [users](#Term_SystemUser) Accept to Invite them or not, and Invitations are accepted or not.  
Correct modelling provides better solutions to classic user and [role](#Term_Role) allocation provisioning issues.

**Details**: The full [workflow](#Term_Workflow) allows for a person to make an Application to a [Role](#Term_Role), which when received may lead to the issuance of an expiring Invitation to a [Role](#Term_Role), explaining [Responsibilities](#Term_Responsibility) associated to the [Permission](#Term_Permission)s of the [Role](#Term_Role), which if Accepted is sent back for Allocation.   
Note that for correct modelling reasons – that also has security benefits -- it is also correct to not issue open ended relations of any kind. [Role](#Term_Role)s associations should have an end date which can trigger a reminder to extend.

**Prompts:** Are [Role](#Term_Role)s unilaterally Allocated to [users](#Term_SystemUser) by permitted [users](#Term_SystemUser), or is a more correct modelling used?  
Are [Role](#Term_Role)s issued open ended? Is there any control used to close [Role](#Term_Role)s after an amount of time?

##### QR-DEF-FUNC-COR-00: **Workflows**

**Category**: ISO-25010/Functional Suitability/Functional Correctness

**Statement**: The solution’s service(s) **must** be capable of managing records via workflows and roles.

**Rationale**: Systems appropriate to servicing large organisations and national and/or international require a correct modelling of processes, dependent on being able to manage records through several stages by different roles working together towards high quality outcomes.

**Details**: Logical states for records and/or resources often include but are not limited to classical states of Draft, For Review, Reject, Approve, Published, Replaced, Retracted, with permissions to move from one state to another reserved for specific roles (Creator, Collaborators, Reviewers, Approvers, Managers, Consumers, etc.)

**Prompts:** What records or resource are processed through multiple states?  
Limited to what roles?

##### QR-DEF-FUNC-COR-00: **Undoable**

**Redirect**: See “Undoable” (under ISO-25010/Reliability/Fault Tolerance)

### Performance Efficiency

The degree of performance relative to the amount of resources used under stated conditions. This characteristic is composed of the sub-qualities listed below.

#### Time Behaviour

The degree to which the response and processing times and throughput rates of a solution, when performing its functions, meets requirements.

##### QR-DEF-PERF-TIM-00: **Responsiveness**

**Category**: ISO-25010/Performance Efficiency/Time Behaviour

**Statement**: The solution’s system(s) **must** return control to [users](#Term_SystemUser) within defined response times.

**Rationale**: Responsiveness contributes to user efficiency, a key ISO-25022 quality.

**Details**: Control means the ability to accept subsequent commands. Additional rendering may occur after the maximum control acceptance time.

**Prompts:** Respecting other constraints (e.g., resource consumption) can the solution’s system(s) meet the stated requirement?

##### QR-DEF-PERF-TIM-00: **Archiving**

**Category**: ISO-25010/Performance Efficiency/Time Behaviour

**Statement**: Solution system(s) **must** incorporate archiving capabilities, preferably Logical.

**Rationale**: System Performance is inverse to the count of records that need to be scanned.

**Details**: Physically removing records from systems to secondary datastores often increase security risks (e.g., by providing archived data in an a less rigorously audited and controlled store).  
  
In [Custom System](#Term_CustomSystem)’s Archiving **must** be logical versus physical, accompanied with appropriate indexing as required to decrease table scans and improve data query performance.  
  
**Important:**It is important to understand that Archiving is never either a business or regulatory requirement. It is purely a performance and resource utilisation concern, with resource utilisation being less of an impact than performance which impacts efficiency.  
  
**Note:**  
while removal of records does decrease the number of records than need scanning, the *actual* development change required to reduce the number of records that need scanning is the introduction of an appropriate index, removing the need to physically remove records.

**Prompts:** Which catalogues of data are archivable? Which are not?  
Is the archiving process logical, or physical?

#### Resource Utilisation

The degree to which the amounts and types of resources used by a product or system, when performing its functions, meets requirements.

##### QR-DEF-PERF-RES-00: **Common Dependencies**

**Category**: ISO-25010/Performance Efficiency/Resource Utilisation

**Statement**: The solution’s system(s) **must** not require exotic infrastructure, devices, integrations, configuration, or software licensing.

**Rationale**: Supporting portability as well as accessibility, the solution must not require dependencies that are difficult for service consumers or service providers to source, provision, integrate with, pay for or provision.

**Details**: The solution, must not require a specific browser, specific device manufacturer, or atypical network capabilities (throughput) or device requirements (memory, CPU capabilities, graphics processor(s)).

**Prompts:** Will the service be accessible via current browser types (Chrome, Edge), running within current OS’s (Windows, Linux, Apple) on current devices (mobiles, laptops, desktop), using Standard licenses (not Enterprise grade), using standard memory (e.g., 8Gb, 4 Client Cores, 8 Server Cores), meeting other requirements (e.g., Capacity, Resource Consumption, Time Behaviour)?

##### QR-DEF-PERF-RES-00: **Required Limited Device Resources**

**Category**: ISO-25010/Performance Efficiency/Resource Utilisation

**Statement**: If a [SaaP](#Term_SaaP), the solution’s system(s) **must** meet target peak Capacity and Time Behaviour Requirements while constrained to the [defined percent of available resources](#Value_AcceptablePercentageOfResource), under standard conditions.

**Rationale**: A solution’s installed solutions must not require exotic configurations of infrastructure or licenses to meet other conditions.

**Details**: This applies to both devices and licensing, e.g.: An installed service should not require an Enterprise version of SQL Server, nor 24 cores (the maximum number of cores available using a Standard edition SQL Server). But nor should it require clustering of database servers (a relatively exotic and non-standard condition) to meet other requirements (availability, responsiveness, capacity)

**Prompts:** If a SaaP, what are exotic infrastructure and/or resource and/or licensing requirements of the proposed solution?  
If a SaaP, will the installation dynamically horizontally scale up and down as required, while accepting to be limited to a [defined subset](#Value_AcceptablePercentageOfResource) of CPU and Memory resources of a shared host physical or virtual device?

##### QR-DEF-PERF-RES-00: **Use Resources closest to Service Consumer**

**Category**: ISO-25010/Functional Suitability/Resource Utilisation

**Statement**: The service client **must** use resources closest to it while following secure practices and meeting requirements.

**Rationale**: Decrease impact on central datastores and infrastructure, improving responsiveness to self and availability to others.

**Details**: Consider the following examples:  
- remembering on the device whether to keep the session when the browser is closed,  
- retrieving resources from CDNs and “cloud edge” devices where possible,  
- consider local storage for caching personal settings that are not confidential,  
- using the device’s CPU and memory where possible to remove this burden from the service’s server device,  
Note: the service client **must not** persist Confidential information on the service.

**Prompts:** Does the solution’s service(s) enable user to retain their session if they close their browser?  
Does the solution’s service(s) [graphical user interface](#Term_UserInterface) follow a [SPA](#Term_SPA) or [MPA](#Term_MPA) design approach?

##### QR-DEF-PERF-RES-00: **Compiled Custom Systems**

**Category**: ISO-25010/Performance Efficiency/Resource Utilisation

**Statement**: [Custom Systems](#Term_CustomSystem) **must** be developed using compiled Languages with standard supported Code Libraries.

**Rationale**: While development may be faster using Interpreted languages, decreasing development costs for the [Supplier Organisation](#Term_Supplier), the infrastructure requirements to offset the deficiencies in interpreted languages over the full-service lifespan are born by the [sponsor organisation](#Term_SponsorOrganisation).

**Details**: While interpreted languages remain preferred for the development of supporting code (deployment [Pipeline](#Term_Pipeline)s, etc.) compiled code is preferred for the following reasons:  
Speed: Python currently runs approximately 40 times[[10]](#footnote-11) slower than .NET Core CLR, which translates to requiring 40 more servers to do the same work that can be done with one.  
Certainty: the value of a supported and potentially constrained mature supply chain outweighs the benefits of the bazaar of open development of libraries

**Prompts:** What languages and frameworks are used in the development of the solution’s systems?  
What steps are or will be taken to secure the supply chain of libraries, etc. that the system depends on?

#### Capacity

The degree to which the maximum limits of the solution meet or exceed requirements.

##### QR-DEF-PERF-CAP: Peak Demand

**Category**: ISO-25010/Performance Efficiency/Capacity

**Statement**: While meeting other constraints, the solution’s service(s) **must** meet defined expected peak demand.

**Rationale**: Remaining Available at capacity is a key expectation.

**Details**: If a [SaaP](#Term_SaaP), the service must be horizontally scalable to expand and contract resources available to meet temporary peak demand.

**Prompts:** Are the solution’s system(s) installed?  
If so, are they horizontally scalable.

##### QR-DEF-REL-AVAI-00: **Available for Users**

**Category**: ISO-25010/Reliability/Availability

**Statement**: The service **must** support the projected number of users and concurrent users using the least resources.

**Rationale**: The service must be available to peak users economically.

**Details**: Refer to the [project](#Term_Project)’s Quantitative settings for the projected values.  
If the solution’s system(s) is custom developed, the resources must scale horizontally dynamically both up and back down to meet varying peak demands.

**Prompts:**

##### QR-DEF-PERF-CAP: **Storage Capacity**

**Category**: ISO-25010/Resource Utilisation/Capacity

**Statement**: The solution’s system(s) **must** be capable of persisting all records for double the [expected service lifespan](#Value_ExpectedServiceLifespan).

**Rationale**: Software is expensive to procure or rent and may be kept running longer than originally expected to recuperate initial costs.

**Details**: …

**Prompts:** Is there a practical limit to the storage used for the solution service(s)?  
Does the proposed solution approach this limit?  
Even if the service is run for double the originally [expected service lifespan](#Value_ExpectedServiceLifespan)?

### Compatibility

The degree to which a product, system or component can exchange information with other products, systems, or components, and/or perform its required functions while sharing the same hardware or software environment. This characteristic is composed of the sub-qualities listed below.

#### Co-Existence

The degree to which a product can perform its required functions efficiently while sharing a common environment and resources with other products, without detrimental impact on any other product.

*Noting that separation of Organisations/Tenancies is a security concern.*

*No Requirements (see Resource Utilization).*

##### ~~QR-DEF-COMP-COEX-00:~~ **~~Separated Org Data~~**

**~~Category~~**~~: ISO-25010/Compatibility/Co-Existence~~

**~~Statement~~**~~: Data specific to organisations~~ **~~must~~** ~~be logically separated from other organisations on the same system.~~

**~~Rationale~~**~~: Physical separation of data per org is a security control.~~

**~~Details~~**~~: Physical and/or Logical Separation of Data per org is a~~ *~~legacy~~* ~~security control. It interferes with sharing (hence SharePoint, etc. don’t)Persons are at the same level of Organisations. But they can have Identities per Org.~~

**~~Prompts:~~** ~~Logical Separation of Resources~~

#### Interoperability

The degree to which two or more systems, products or components can exchange information and use the information that has been exchanged.

**Note:** Interoperability is what a service provides to other services, **not** Integrations, which is what it relies on.

##### QR-DEF-COMP-INT-00: **Functionality** **APIs**

**Category**: ISO-25010/Compatibility/Interoperability

**Statement**: All of the solution’s available services functionality **must** be exposed via [API](#Term_API)s.

**Rationale**: [API](#Term_API)s are required to manage System and Business Domain functionality from 3rd party systems, e.g.,  
Deployment and/or provisioning [Pipeline](#Term_Pipeline)s use System [API](#Term_API)s to manage post-deployment system settings including identity and branding, [users](#Term_SystemUser), groups and [role](#Term_Role) provisioning, before progressing to using business domain functionality [API](#Term_API)s to provision [system data](#Term_SystemData). Monitoring services use other [API](#Term_API)s to query information on [Session](#Term_Session)s and operations, etc.

**Details**:

**Prompts:** Noting that very few systems do provide [API](#Term_API)s for all of the functionality, it is important for consideration and comparison tasks to know what service [API](#Term_API)s **are** available from this solution’s systems:  
- system settings  
- tenancies  
- [Session](#Term_Session)s  
- session operations  
- system [Permission](#Term_Permission)s  
- system [role](#Term_Role)s   
- users  
- user identities  
- user system [role](#Term_Role) allocations  
- groups  
- group [role](#Term_Role)s  
- user group [role](#Term_Role) allocations  
- resources (e.g. media, documents, that users work on)  
- resource groups  
- resource states  
- resource [workflow](#Term_Workflow)s  
- resource versions

##### QR-DEF-COMP-INT-00: **APIs using Current Patterns**

**Category**: ISO-25010/Compatibility/Interoperability

**Statement**: The solution’s services **must** offer [API](#Term_API)s using current integration patterns.

**Rationale**: REST based integrations over HTTP/S are less expensive to develop, secure, test and manage than SOAP over multiple channels.

**Details**: REST is the expected integration pattern.   
If current integration patterns are offered, other approaches are also accepted (e.g., SOAP).

**Prompts:** Are [API](#Term_API)s developed in REST?  
Is there any functionality offered in other approaches (e.g., SOAP) that are not offered via REST [API](#Term_API)s?

**Traceability:** MOE: *NFR – Migration of Data*

##### QR-DEF-COMP-INT-00: **Current** **Standards based APIs**

**Category**: ISO-25010/Usability/Interoperability

**Statement**: [API](#Term_API)s **must** be delivered meeting current international [standard](#Value_Standards)s.

**Rationale**: [Standard](#Value_Standards)s based solutions decreases [project](#Term_Project) risk and testing costs by avoiding novel solutions to solved problems.  
[Standard](#Value_Standards)s based solutions increase the number libraries available to decrease development skills requirements and thereby cost.  
ODATA is an OASIS based standard for REST [API](#Term_API)s.

**Details**: [API](#Term_API)s may **also** be delivered using non-[standard](#Value_Standards)s based interfaces (e.g., [GraphQL](#Term_GraphQL) is a widely used, but non [standard](#Value_Standards)s based, non-[REST](#Term_REST) based [API](#Term_API) pattern).

**Prompts:** Are the solution’s services’ [API](#Term_API)s REST based?  
Are the solution’s services’ REST [API](#Term_API)s available as [ODATA](#Term_ODATA) compliant solutions?  
What other patterns are used? Homebrew? GraphQL?

**Traceability:** MOE: *NFR – Migration of Data*

##### QR-DEF-COMP-INT-00: **Interoperability**

**Category**: ISO-25010/Compatibility/Interoperability

**Statement**: The solution’s system(s) **must** permit interoperability for external services using current best practice channel and encryption Protocols.

**Rationale**: A system’s value is directly related to the ability to use the system.   
Improving the approaches by which it can be used – by both [API](#Term_API) and GUI – increases its value.

**Details**: Best practice for permitting integration across networks is to use HTTP/S over other ports and channels, and preferring HTTP only approaches (e.g., REST) over multi-channel protocols (e.g., SOAP).

**Prompts:** Do all the service’s system(s) expose functionality by [API](#Term_API)?

##### QR-DEF-COMP-INT-00: **Integration Schema Standards**

**Category**: ISO-25010/Performance Efficiency/Interoperability

**Statement**: If a custom system the system **must** offer APIs endpoints that align to integration data [standard](#Value_Standards)s.

**Rationale**: Integrations – whether for importing or exporting data -- are only permitted via authenticated, authorised, audited validated APIs.   
For security reasons, a system’s internal components and resources **must** remain opaque to external systems.  
…

**Details**: ETL from the system’s datastores **must** not be a permitted integration strategy.  
Therefore Data [standard](#Value_Standards)s are to be applied to the APIs only, not the internal Datastore schemas.  
If the solution’s system(s) are not custom systems and their [API](#Term_API)s cannot be changed the integration work is to be achieved as a [Transitional Task](#Term_TransitionalTasks).

**Prompts:** …

#### Integrations

Integration is not the same thing and interoperability: integration is about a system connects to 3rd party services (e.g.: an [IdP](#Term_IdP)) whereas Interoperability is about providing access to 3rd parties.

##### QR-DEF-COMP-INTG-00: **SMTP**

**Category**: ISO-25010/Compatibility/Integration

**Statement**: The solution’s system(s) **must** be integrated with agreed mail services.

**Rationale**: Timely messages are required to be sent to [users](#Term_SystemUser) who do not have an active [Session](#Term_Session).

**Details**: The solution must use SMTP to send messages.   
To trust the message, receivers must be able to recognise the organisation that manages the mail server used to send the message.  
The use of a password-less service account is preferred. If not possible, the credentials required to access the remote mail system must be secured using secure credential storage.

**Prompts:** Does the service send messages?  
Can the service be configured to use an agreed mail service?  
If installed, how are the credential persisted (system config file, else)?

##### QR-DEF-COMP-INTG-00: **OIDC**

**Category**: ISO-25010/Compatibility/Integration

**Statement**: The solution’s system(s) **must** authenticate [users](#Term_SystemUser) via an OIDC compliant endorsed [IdP](#Term_IdP) service.

**Rationale**: OIDC is a current best practice approach to integrating [IdP](#Term_IdP)s over HTTP/S that is secure while being less complex, specialised and costly to develop than SAML based identity solution integrations.

**Details**: Using an external IdP is preferred, while recognising there remain use cases where in-system authentication of [users](#Term_SystemUser) is required (e.g., very young learners who are not legally permitted to use most commercial [IdP](#Term_IdP) services).

**Prompts:** Can the solution’s services be integrated to external [IdP](#Term_IdP)s?  
Is the integration protocol used OIDC or another (e.g., SAML)?  
Does the service also provide in-system user authentication?  
Can it be turned off to force the use of external [IdP](#Term_IdP)?

##### QR-DEF-COMP-INTG-00: **OAuth**

**Category**: ISO-25010/Compatibility/Integration

**Statement**: The solution’s system(s) **must** authorise other services using OAuth.

**Rationale**: While OIDC is used for authenticating [users](#Term_SystemUser), OAuth is the best practice integration approach for authorising trusted 3rd party services to use a service’s [API](#Term_API)s over HTTP/S.

**Details**: .

**Prompts:** Can the solution’s [API](#Term_API)s be invoked by a 3rd party?  
Do they authorise using OAuth?  
Does – and if so, how – do 3rd parties identify to this solution’s service(s) the end user of 3rd party users?

##### QR-DEF-COMP-INTG-00: **Sponsor Organisation AAD**

**Category**: ISO-25010/Compatibility/Integrations

**Statement**: The Solution **may** require

**Rationale**: If the [IdP](#Term_IdP) service cannot federate to the organisation’s directory services (e.g.,: AAD) then the service **must** be integrated directly to the organisation’s AAD [APIs](#Term_API).

**Details**: AAD supports both OIDC and OAuth, but they are slightly proprietary.

**Prompts:** Can the solution’s service(s) be integrated with Azure Active Directory?

### Usability

#### Appropriateness Recognisability

The degree to which users can recognize whether a solution is appropriate for their needs.

##### QR-DEF-USA-APP-00: **Sponsor and** **Purpose Recognisability**

**Category**: ISO-25010/Usability/Appropriateness Recognisability

**Statement**: Services **must** be sufficiently configurable to identify the [Sponsor Organisation](#Term_SponsorOrganisation), and purpose of service.

**Rationale**: The trust of [users](#Term_SystemUser)’ in services is dependent on their identification and trust of the service provider.

**Details**: Systems are expected to be configurable to follow sponsor organisation guidance for appearance, branding, contact, etc.

**Prompts:** Can service systems be discoverable using organisation defined DNS records?  
Can service systems appearance be modified to present the organisation’s logo, name, etc.

#### Learnability

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.

##### QR-DEF-USA-LRN-00: **Service** **Discovery**

**Category**: ISO-25010/Usability/Learnability

**Statement**: The solution service(s) **must** be discoverable via predictable paths following DNS naming guidance.

**Rationale**: [users](#Term_SystemUser) should be able to find services using predictable URLs.

**Details**: Accepting that DNS registration is a concern outside of a system, systems are expected to accept being discoverable at an URL similar to:  
<https://[channel.][subservice.][env.]service.organisation.tld>  
providing for default values (e.g., when channel is provided, it defaults to ‘www.’, etc.)

**Prompts:** …

##### QR-DEF-USA-LRN-00: **Usability Standards**

**Category**: ISO-25010/Usability/Learnability

**Statement**: The solution **must** be kept aligned with [Sponsor Organisation](#Term_SponsorOrganisation)’s guidance.

**Rationale**: Using a standard approach for contacting the [Sponsor Organisation](#Term_SponsorOrganisation), terms and conditions and disclosures makes the solution’s system(s) more trustable and learnable.

**Details**: Guidelines commonly describe logos, links, and link text to use for references to the [Sponsor Organisation](#Term_SponsorOrganisation), tracking & data use disclosures, etc.

**Prompts:** …

##### QR-DEF-USA-LRN-00: **Use Documentation**

**Category**: ISO-25010/Usability/Learnability

**Statement**: The solution’s service(s) **must** have accessible electronic documentation sufficient for different roles of users to learn how to use the system for their needs.

**Rationale**: users that can self-help themselves to learning how to use a system reduce the cost of supporting them.

**Details**: Electronic documentation is usually hosted separate to the service itself, but using a DNS name related to the service?

**Prompts:** Do the solution’s service(s) have documentation?  
Is the service publicly accessible online?  
Where can it be currently seen?  
Can the documentation URL be customised to align to the service’s URL while meeting project defined DNS naming schemes?  
For example: *https://help.env.myservice.ourcorp.tld*

#### Operability

The degree to which a product is easy to operate, control and appropriate to use.

##### QR-DEF-USA-OP-00: **Operable on Current Devices Interfaces**

**Category**: ISO-25010/Usability/Operability

**Statement**: The solution’s systems(s) **must** be designed for effective use irrespective of the commonly available current device used.

**Rationale**: …

**Details**: This specifically implies that the design of the [graphical interface](#Term_UserInterface) modifies itself to best suit available screen dimensions (i.e., applying “Responsive Web Design (RWD)” principles to web graphical [user interfaces](#Term_UserInterface)).

**Prompts:** Are all system graphical [user interface](#Term_UserInterface)s accessible from multiple device types (mobile, tablet, desktop)?  
If not all, which ones are not operable from other than desktop devices?

##### QR-DEF-USA-OP-00: **Provisioned users**

**Category**: ISO-25010/Usability/Operability

**Statement**: The solution can be remotely provisioned with users, Groups, roles.

**Rationale**: Onboarding

**Details**: The recommended approach is to send out time limited email invitations inviting users to accept specific roles.  
Alternatively the provision of System for Cross-domain identity management (SCIM) [API](#Term_API) endpoints is recommended.  
See “**JIT users”**

**Prompts:** Does the solution’s service(s) permit remote provisioning of users to roles?  
How?  
Is SCIM provided?

##### QR-DEF-USA-OP-00: **JIT users**

**Category**: …

**Statement**: Invitations **must** be developed into System users Just In Time (JIT).

**Rationale**: Improves security and usability of the system.

**Details**: Avoid creating system users records ahead of time without certainty they will be used (a security risk).   
While *Provisioning* [users](#Term_SystemUser) and their [Role](#Term_Role)s is common practice in IT systems, *Inviting* Persons to become [users](#Term_SystemUser) to a System is more correct as well as improvable.   
See “**Provisioned users**”

**Prompts:** …

##### QR-DEF-USA-OP-00: **Multiple Sessions**

**Category**: …

**Statement**: The solution’s system(s) **must** permit system users establish multiple parallel Sessions.

**Rationale**: users either own or have access to multiple devices to use the world wide web. A person may concurrently open long duration independent Sessions from both a desktop and a mobile phone device.

**Details**: Defined elsewhere are Requirements for the permitted max length of sessions and/or features to facilitate long sessions.

**Prompts:** Does the service permit the use of concurrent sessions?  
Are there any notable limitations to this desired outcome?

##### QR-DEF-USA-OP-00: **Session Duration**

**Refer**: See: ISO-25010/Security/Session Duration

##### QR-DEF-USA-OP-00: **Localised System Media Languages**

**Category**: ISO-25010/Usability/Operability

**Statement**: The solution’s system(s) **must** enable end [users](#Term_SystemUser) to switch between the defined target country’s national written languages.

**Rationale**: The solution’s system(s) must render [System Media](#Term_SystemMedia) (text and images) according to [user](#Term_SystemUser) preferences in applicable languages.

**Details**: [System Media](#Term_SystemMedia), as opposed to user supplied media includes labels, instructions, prompts, icons, background, etc.  
**Note:** A minimum of two written language is required to be installed.  
Functionality is required to be accessible to end [users](#Term_SystemUser) for them to switch between culture/language preferences.

**Prompts:** Does the service permit rendering of [System Media](#Term_SystemMedia) according to user culture & language preferences?  
Are all of the target countries languages included?

##### QR-DEF-USA-OP-00: **Pre-notified Downtimes**

**Category**: ISO-25010/Usability/Operability

**Statement**: Downtimes of the service **must** be pre-notified.

**Rationale**: Let [users](#Term_SystemUser) plan their reliance on the service.

**Details**: The notification must be via channels they access most regularly.

**Prompts:** Is the notification in-system?  
How is notification made to users not currently using the system?

##### QR-DEF-USA-OP-00: **Organisation Appearance Standards Alignment**

**Category**: ISO-25010/Usability/Operability

**Statement**: Where technically and achievable, solution system(s) graphical [user interfaces](#Term_UserInterface) **must** use or align with the [Sponsor Organisation](#Term_SponsorOrganisation)’s standards.

**Rationale**: Common appearance of services contributes to consumer’s confidence, understandability and operation.

**Details**: Organisations may require use of and alignment to Visual Styles.

**Prompts:** Can the graphical [user interfaces](#Term_UserInterface) define the [Sponsor Organisation](#Term_SponsorOrganisation)?  
Can the appearance of interfaces be aligned to [Sponsor Organisation](#Term_SponsorOrganisation) standards?

##### QR-DEF-USA-OP-00: **Role Association**

**Category**: ISO-25010/Usability/Operability

**Statement**: Authorised Authenticated users **must** be able to invite other Persons to Accept proposed [Role](#Term_Role)s.

**Rationale**: While assigning [Role](#Term_Role)s is common practice in IT systems, applying for a [Role](#Term_Role), or being invited to accept a [Role](#Term_Role) is more correct as well as improvable.

**Details**: [TODO]

**Prompts:** How are users associated to [Role](#Term_Role)s?  
What kind of [Role](#Term_Role)s are they? System based, Tenancy based, per-Group, (e.g.,., Accountable, Manager, Member, Guest, etc.) or per Resource (e.g.,., Creator, Contributor, Approver, etc.).

##### QR-DEF-USA-OP-00: **Early Availability of Guidance**

**Category**: ISO-25010/Usability/Operability

**Statement**: The solution’s system(s) **must** provide guidance as early as practical.

**Rationale**: The sooner a user can meet operation requirements the sooner they are able to complete their task adding to their evaluation that the service is effective.

**Details**: A specific example of this type of expected behaviour is that of user input dynamic validation: provide instructions on why a field has failed validation without waiting till the user submits the whole form.

**Prompts:** Are instructions provided on how to pass validation?  
When are they shown – after a user completes input of the field and moves on to another field, or does it wait till the user presses an Action button (e.g., ‘Submit’).

##### QR-DEF-USA-OP-00: **User Input is Completed and Corrected**

**Category**: ISO-25010/Usability/Operability

**Statement**: The solution’s system(s) **must** attempt to correct and complete user input.

**Rationale**: Users hurry and makes mistakes that automation can correct in many cases without further guidance or oversight.

**Details**: The solution’s system(s) should provide autocompletion where achievable (words, phrases, addresses, etc.).  
The system should rely on browsers to propose corrections to spelling mistakes.   
These steps should be taken before validation is applied.  
User input excludes applying correction to [API](#Term_API) inputs.

**Prompts:** Approximately what % of the user input fields benefit from auto-completion?  
Approximately what % of the user input fields benefit from Input auto-correction?  
Is validation delayed till these steps are completed?

##### QR-DEF-USA-OP-00: **Undoable**

**Redirect**: See “Undoable”

#### Accessibility

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.

##### QR-DEF-USA-ACC-00: **Latest** **WCAG**

**Category**: ISO-25010/Usability/Accessibility

**Statement**: Service graphical [user interface](#Term_UserInterface)s **must** be accessible, meeting the latest WCAG Guidelines to an AA level or better.

**Rationale**: Even able persons are only temporarily within the arc of ability, being dis-abled at other times by youth, accident, illness, or old age.

**Details**: Interfaces include both interactive system [user interfaces](#Term_UserInterface) and non-interactive printed reports.  
Examples of Level A: Navigable by keyboard, Non-Text content alternatives, video captions.  
Examples of Level AA: Colour contrast, Meaningful text alternatives to images, Consistent navigation elements, correct form labels, status updates can be conveyed through a screen reader, logical headers, etc.  
Note: WCAG 2.0 is now an [international standard](#Value_Standards): ISO-40500.

**Prompts:** What is the lowest level which the solution’s service(s) interfaces meet of the latest version of the Web Content Accessibility Guidelines?

### Reliability

The degree to which a system, product or component performs specified functions under specified conditions for a specified period of time. This characteristic is composed of the sub-qualities listed below.

#### Maturity

The degree to which a system, product or component meets needs for reliability, under normal and peak demand.

##### QR-DEF-REL-MAT-00: **Maturity**

**Category**: ISO-25010/Reliability/Maturity

**Statement**: The solution’s system(s) **must** be maintained to defined [Acceptable Error Severity](#Value_ErrorSeverityAcceptance) constraints during both testing and normal operation.

**Rationale**: Reliability is **not** dependent on age or user base, it is based on reliability under normal and peak operation loads, measured by the quantity and classification of errors as per defined [error severities](#Term_ErrorSeverity).   
While procured systems can be expected to be mature, this is not always the case and vice versa, custom developed systems can be judged reliable not by age but based on the severity of errors raised.

**Prompts:** What is the set of known critical or high errors, under any circumstance, known of the system?   
Can you list **any** possible reasons that the solution’s system(s) may experience critical or high-level exceptions in the current use case?

#### Availability

The degree to which a service is available and operable to service consumers when required for use.

##### QR-DEF-REL-AVAI-00: **Availability**

**Category**: ISO-25010/Reliability/Availability

**Statement**: The solution’s systems **must** meet the stated monthly [availability](#Value_Availability) expectations.

**Rationale**: A solution that is not available is not used.   
Users who need a service look for an available equivalent service.  
Users who find an equivalent service that is more reliable do not return to use the service.

**Details**: **Important:** The availability expectations are not possible to be met without an automated delivery [pipeline](#Term_Pipeline) to perform the necessary steps required to bring a service back online.  
Azure services are almost universally 99.9%.

**Prompts:** …

#### Fault Tolerance

The degree to which a solution operates as intended despite the presence of hardware, software or user faults.

##### QR-DEF-REL-FT-00: **Validation**

**Category**: ISO-25010/Reliability/Fault Tolerance

**Statement**: All data provided via [Interface](#Term_Interface)s **must** be validated prior to adding or changing [system data](#Term_SystemData).

**Rationale**: Incorrect data must not be accepted or persisted by the system as it leads to producing incorrect information on which users make decisions as to their actions.

**Details**: Validation is done after “**User Input is Completed and Corrected”**.  
Validation is done at both the field and message level.   
Validation of all fields is dependent on type and will include one or more of the following checks: required or not, format checks, type checks, range checks.   
Validation of messages as a whole is also to be expected (e.g., valid combinations of fields, minimum number of filled fields, etc.).  
Validation of uploaded media is required as well, for malware, as well as one or more of format, size, and/or description (as required to meet Accessibility standards).  
Validation is expected to be applied as early as practical (after autocorrection and autocompletion, but before waiting for the user to attempt to submit the new values).

**Prompts:** What messages are accepted by the system without validation?

##### QR-DEF-REL-FT-00: **Undoable**

**Category**: ISO-25010/Reliability/Fault Tolerance

**Statement**: The solution’s system(s) **must** enable [users](#Term_SystemUser) to undo their own changes or permitted userusers to undo the changes of others.

**Rationale**: [users](#Term_SystemUser) make mistakes, they are the first to notice this, and it should be their responsibility to undo their own (audited) mistakes.  
Permitting undo decreases training needs, user trepidation, increasing their exploration of the system, leading to increasing efficiency and decreasing support costs.

**Details**: This capability depends on other requirements being in place (see Information Deletion).  
Technically, this is generally achieved by designing and developing according to the **Command Pattern**, and/or reliance on auditing record values prior to changes, and the replacement values.

**Prompts:** Is Undo functionality provided to end users?  
To what coverage (all, most, some, none) of domains (system, domain) entities?  
Does the solution’s system(s) audit record field value changes?  
Does the solution’s system(s) permit the undoing of these changes to records?   
Does the solution permit a user to undo their own changes?  
Does the solution permit other Permitted users to undo the changes of others?

##### QR-DEF-REL-FT-00: **Error Handled**

**Category**: ISO-25010/Reliability/Fault Tolerance

**Statement**: Unexpected Behaviour **must** be handled to not affect concurrent or subsequent user operations, while recording information valuable for later analysis.

**Rationale**: No system exception is left to propagate disrupting other users and/or require an intervention activity to return to normal operation for all users.

**Details**: For any unexpected exception, the solution’s system(s) must develop handle the error. Specifically make entries in the temporary diagnostics trace logs, make permanent error log entries, and provide understandable and usable error messages to the end user.

**Prompts:** Does the system capture all unexpected errors?  
Is the occurrence traced?  
Is the occurrence permanently logged?  
Are error messages and instructions provided to the user?  
Are they understandable and/or actionable by non-technical users?

#### Recoverability

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.

##### QR-DEF-REL-REC-00: **DR within MTD**

**Category**: ISO-25010/Reliability/Recoverability

**Statement**: The solution’s system(s) and its data **must** be restorable at will, including [disaster recovery](#Term_DisasterRecovery) operations, within the [quantified](#Value_MTD) [Maximum Tolerable Downtime (MTD)](#Term_MTD).

**Rationale**: users expect to use the service as soon as possible.

**Details**: The MTD is a [quantified](#Value_MTD) value.  
Automation is expected to be used to perform data backups and restorations because   
- automated backups and restorations can be tested over and over again,   
- processes that are automated will be faster than possible manually  
- manual processes cannot be completed within the allocated MTD.

**Prompts:** Are the service’s datastores backed up manually or by automation?  
Are the service’s database restoration process automated?   
How often are database restoration processes tested?

##### QR-DEF-REL-REC-00: **DR within** **RPO**

**Category**: ISO-25010/Reliability/Recoverability

**Statement**: Upon [Disaster Recovery (DR)](#Term_DisasterRecovery) the system **must** meet its [quantified](#Value_RPO) RPO constraint.

**Rationale**: After waiting for a disaster recovery process to complete in order to continue with their work, userusers expect to lose the least amount of both unsaved and saved work.

**Details**: The RPO value is a [quantified](#Value_RPO) value.

**Prompts:** How often are they backed up fully (e.g., daily)?  
How often are they backed up incrementally? (e.g., 5 minutes)

### Security

Degree to which a product or system protects information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization. This characteristic is composed of the sub-qualities listed below.

Note: The distinctions between the following sub-qualities are subtle. For example, Confidentiality is primarily about protecting systems from the disclosure (i.e., viewing) of information – preliminarily by physical controls (e.g. HTTPS), Integrity is about the protection of the data from change using logical controls (e.g., [Permission](#Term_Permission) and [Role](#Term_Role) control). Non-Repudiation is about auditing actions, and Accountability is about tying the non-repudiable record to an Authenticated person’s digital identity.

#### General

##### QR-DEF-SEC-GEN-00: **OWASP**

**Category**: ISO-25010/Security/General

**Statement**: Solution Systems(s) **must** pass be assessed against OWASP’s latest top 10.

**Rationale**: OWASP is the default trusted source of the most pressing vulnerabilities.

**Details**: A01:2021-Broken Access Controls is partly addressed by QR-DEF-SEC-INT-00: Access Control  
A02:2021-Cryptographic Failures is addressed by QR-DEF-MAIN-GEN-00: “**Maintained Current”** and “Current Recommended Cryptography Algorithms”

**Prompts:** TODO

##### QR-DEF-SEC-GEN-00: **Security Auditing**

**Category**: ISO-25010/Security/Gen

**Statement**: Security Events will be persisted separately to Diagnostic Trace records.

**Rationale**: Security Event logs are required by a different role than diagnostic trace records which are required by [maintenance specialists](#Term_MaintenanceSpecialist).

**Details**: Mature diagnostics tracing solutions permit defining different places to send diagnostics messages, as well as configure the level of diagnostics to send.

**Prompts:** Does the solution’s system(s) register security events to a different location than general system diagnostics records?  
TODO: redefine, removing the HOW.

#### Confidentiality

The degree to which the solution ensures data is accessible only by those authorised to do so.

##### QR-DEF-SEC-CONF-00: **Physical Access**

**Category**: ISO-25010/Security/Confidentiality

**Statement**: Any physical locations where solution system(s) service devices are located all access and operations **must** be controlled and audited.

**Rationale**: Users must not be able to access system storage and server devices in an uncontrolled and/or unaudited manner, bypassing electronic and logical platform and/or system controls.

**Details**: Cloud service providers control physical access, e.g., they require all personnel who enter to be audited, as well as all operations are recorded by an accompanying observer. This drives the preference for systems hosted in market leading cloud services.

**Prompts:** Are all [environments](#Term_Environment)’ devices hosted on cloud infrastructure?

##### QR-DEF-SEC-CONF-00: **Remote Access**

**Category**: ISO-25010/Security/Confidentiality

**Statement**: Access to and changes to service and storage devices **must** be controlled and audited.

**Rationale**: users must not be able to access system storage and service devices in an uncontrolled and/or unaudited manner, bypassing electronic and logical platform and/or system controls.

**Details**: Cloud services control and audit virtual access. This drives the preference for systems to be hosted in market leading cloud services.

**Prompts:** Are all environments devices and services hosted on cloud infrastructure?

##### QR-DEF-SEC-CONF-00: **Production Data Access**

**Category**: ISO-25010/Security/Confidentiality

**Statement**: Access to Production Data **must** be limited to authenticated authorised and audited business service userusers.

**Rationale**: In depth protection cannot be effective if groups of individuals are permitted to circumvent physical and/or logical controls.

**Details**: This includes testers and developers.  
**Important:**It remains illegal to access production data for non-disclosed purposes, even development and quality assurance reasons.

**Prompts:** See *Test Data*

##### QR-DEF-SEC-CONF-00: **Encrypted Data at Rest**

**Category**: ISO-25010/Security/Integrity

**Statement**: Stored Data **must** be encrypted.

**Rationale**: Supports Defence in Depth approach.

**Details**: Note this is in addition to requirement that direct physical access is not permitted.

**Prompts:** …

##### QR-DEF-SEC-CONF-00: **Avoid Persisting Confidential Data**

**Category**: ISO-25010/Security/Confidentiality

**Statement**: Outside of the system(s) production environments, Confidential information **must** **not** be persisted in accessible systems.

**Rationale**: Persisting systems in data that can be accessed without controls or auditing enables the disclosure of sensitive data.

**Details**: Put in place controls, preferably automated, to avoid the following:  
- persisting of sensitive system integration credentials in a code repository. The correct approach is to rely on where possible permitted service accounts, authenticated by central [Permission](#Term_Permission) authorities. Any credentials still required are persisted in dedicated credential stores. Use Code Branch Policies to check for check-in of credentials  
- persisting of sensitive [system data](#Term_SystemData) in a code repository (e.g., test data derived from production data.

**Prompts:** Is training provided to communicate the risks associated to committing credentials to code repositories?  
Does the solution provide for and use a credential store for credential storage?  
How is test data derived? Where is it stored? How is it provisioned?

##### QR-DEF-SEC-CONF-00: **Avoid Transmitting Credentials**

**Category**: Avoid Transmitting Credentials

**Title**: …

**Statement**: …

**Rationale**: …

**Details**: Avoid using BASIC Authentication.   
Avoid using unencrypted HTTP channels.  
Avoid transmitting credentials in cookies.  
Decorate Cookies with secure and Http-Secure flags.

**Prompts:** …

##### QR-DEF-SEC-CONF-00: **Sensitive Settings Storage**

**Category**: ISO-25010/Security/Confidentiality

**Statement**: Sensitive Parameters **must** be encrypted.

**Rationale**: TODO

**Details**: …

**Prompts:** What Sensitive Parameters do the solution’s system(s) persist?  
Are they persisted in an encrypted manner?  
If stored locally or in the operational database, are they [Salt](#Term_Salt)-ed?

##### QR-DEF-SEC-CONF-00: **Sensitive Information Transmission**

**Category**: ISO-25010/Security/Confidentiality

**Statement**: Credentials **must** not be transmitted in [ClearText](#Term_ClearText).

**Rationale**: Even if the channel is encrypted, credentials should not be readable by intermediates.

**Details**: Proxies are potential attack vectors.

**Prompts:** …

##### QR-DEF-COMP-INT-00: External IdP

**Category**: ISO-25010/Compatibility/Interoperability

**Statement**: The solution’s system(s) **must** integrate with external agreed identity providers via current accepted protocols.

**Rationale**: Systems that are not specifically designed to secure credentials, e.g., most information services should not be used if possible as there is increased risk.

**Details**: OIDC is the approved protocol to communicating with external Identity Provider services.  
**Note:** There may be a requirement to let in users who do not want to or are too young to use a public [IdP](#Term_IdP), and therefore user Credentials will be persisted in the system.

**Prompts:** …

##### QR-DEF-SEC-CONF-00: **Credentials Persistence**

**Category**: …

**Statement**: The solution’s [SaaP](#Term_SaaP) system(s) **must** not persist Credentials in ClearText.

**Rationale**: Even if controls are in place to limit remote access to devices, the principle of Defence in Depth remains applicable.

**Details**: Prefer using mutually trusted Service Accounts to Credentials.  
If Credentials are required for configuration, they must not

**Prompts:** If a SaaP, Are Credentials required to integrate with 3rd party dependencies?  
If a SaaP, where are they retrieved from?  
If a SaaP, where are they persisted?  
If a SaaP, how are they encrypted when persisted?

**Traceability:** *MOE: NFR-Credential Handling Requirements – Service Accounts*

##### QR-DEF-SEC-CONF-00: **Data between Networks is over Confidential Channels**

**Category**: ISO-25010/Security/Confidentiality

**Statement**: Channels for data transfer between Devices in different Networks **must** be Encrypted

**Rationale**:

**Details**: Communication between Service Client/Browser and Server must be protected by HTTP/S.  
Attempts to connect to an insecure channel (e.g., HTTP) are not accepted. Preferably they are redirected to secure equivalent endpoints (e.g., HTTP/S).  
**Note:** Protocol routing is a web server configuration, outside the control of the web system itself.

**Prompts:** Does the solution’s system(s) accept insecure connections?  
What are done with them?

##### QR-DEF-SEC-CONF-00: **Current Recommended Cryptography Algorithms**

**Category**: ISO-25010/Security/Confidentiality

**Statement**: Cryptography algorithms used for encryption and signing **must** use the latest current released versions.

**Rationale**: Security relies on using best practice industry standards and remaining ahead of the capabilities of nefarious actors.

**Details**: For example, TLS 1.3 or better must be used for HTTP/S.  
Message Encryption is acceptable if Channel Encryption is not technically feasible.

**Prompts:** How will channel and device encryption be reviewed and updated to remain current?

##### QR-DEF-SEC-CONF-00: **Cleanse External Data**

**Category**: ISO-25010/Security/Confidentiality

**Statement**: Solution System(s) **must** remove sensitive data from data that is exported to services that will not control and audit access to data to the same or endorsed level.

**Rationale**: Messages sent outside the solution’s system(s) cannot be guaranteed to be access controlled or audited.

**Details**: This includes but is not limited to:  
- Diagnostics tracing messages,   
- Error Records  
- Emails  
- Printed Reports  
- Messages (SMS, other)  
  
The appropriate way is to write emails that have links back to reports in the system. This means the Viewing of the reports is authorised first as well as audited.

**Prompts:** Does the solution’s system(s) permit the editing of templates for emails and reports? In different languages?  
Do emails contain confidential information or provide a link back to reports containing the confidential information in an environment in which views are audited?

##### QR-DEF-SEC-CON-00: **Confidential Messages over Confidential Access**

**Category**: ISO-25010/Security/Confidentiality

**Statement**:

**Rationale**: …

**Details**: Mark browser cookies with Secure, and HTTP Only.  
Do not transmit confidential credentials over unsecured channels (e.g., BASIC over HTTP is unacceptable).

**Prompts:** Are cookies marked with marked with security markings?

#### Integrity

ISO-25010 Definition: the degree to which the solution prevents unauthorised access, modification of systems and the information they manage.

##### QR-DEF-SEC-INT-00: **User Suspension**

**Category**: ISO-25010/Functional Suitability/Functional Correctness

**Statement**: The solution’s system(s) **must** permit [users](#Term_SystemUser) being disabled by an authorised [role](#Term_Role).

**Rationale**: While the solution’s system(s) must be able to integrate with an external [Identity Provider (IdP)](#Term_IdP) for the authentication of [users](#Term_SystemUser), and, **if** under the control of the sponsor, this can be used to disable the user’s IdP account, there remain conditions where this is insufficient. There may be [users](#Term_SystemUser) who must use the system’s internal authentication service or they may be using a 3rd party [IdP](#Term_IdP) which the [Sponsor Organisation](#Term_SponsorOrganisation) has no control over.

**Details**: Authorised [Operations Specialist](#Term_OperationsSpecialist) Roles must be provided with functionality to search for a system wide [user](#Term_SystemUser), and disable their account.  
**Note:** This system wide disabling is above and beyond any other controls (e.g., Accounts subscriptions that are used in commercial systems).  
Mature accounts also permit suspending accounts for set durations, which implies the ability to set a series of suspension start and end dates without change to the baseline start/end dates of the [Role](#Term_Role) association.

**Prompts:** Does the solution’s system(s) provide functionality to authorised [Role](#Term_Role)s to disable userusers access to the system?  
Is the functionality exposed by [API](#Term_API) so that it can be remotely set by automation, as opposed to only providing [user interface](#Term_UserInterface)s for system administrators to operate manually?

##### QR-DEF-SEC-INT-00: **Session Duration**

**Category**: ISO-25010/Security/Confidentiality

**Statement**: Session Timeouts **must** respect the duration of authentication tokens.

**Rationale**: For efficiency reasons, sessions must be as long as possible while not compromising security.

**Details**: Authentication is done primarily via remote IdPs, where timeout durations are embedded in the validity duration of the remote token.   
Any development of local session tokens must duplicate and respect this value.

**Prompts:** Does the solution system(s) source session duration from IdP return tokens?  
Are locally in-system authenticated user session lengths configurable?  
What is the default value?

##### QR-DEF-SEC-INT-00: **Access Control**

**Category**: ISO-25010/Security/Integrity

**Statement**: Access to System Functions and Resources **must** be limited to only authorised users.

**Rationale**: Logical access controls contribute to adherence to a Defence in Depth principle.

**Details**: This includes both GUI Views and [API](#Term_API) endpoints.  
Consider [Permission](#Term_Permission) based [Role](#Term_Role) control and Resource Route based control.   
Goes Towards addressing OWASP A01:2021-Broken Access Controls.

**Prompts:** Does the service perform [Role](#Term_Role)s control?   
Are [Role](#Term_Role)s collections of [Permission](#Term_Permission)s?  
Is the allocation of [Permission](#Term_Permission) to [Role](#Term_Role)s configurable?  
Is the allocation of [Role](#Term_Role)s to users configurable?   
Are [Role](#Term_Role)s system based, group based, and/or resource based?

##### EQ-SEC-INT-00: **Least Privileges**

**Category**: ISO-25010/Security/Integrity

**Statement**: Unless permitted otherwise by authorised users, users **must** be given the least privileges while retaining the ability to view publicly accessible [view](#Term_View)s.

**Rationale**: A service has at least publicly accessible pages providing the means to sign into the system.

**Details**: Unless another site is dedicated to this, a system must provide pages for login, as well access to information on data use, privacy, who to contact for assistance, etc.

**Prompts:** …

##### QR-DEF-SEC-INT-00: **Multiple Access Levels**

**Category**: ISO-25010/Security/Integrity

**Statement**: A [system user](#Term_SystemUser) **must** be assignable multiple [Access Levels](#Term_AccessLevel).

**Rationale**: A [system user](#Term_SystemUser) can have concurrent Organisation/Tenancy Access Levels, Group Access Levels and/or Resource Access Levels.

**Details**: Examples might include the following:  
A [system user](#Term_SystemUser) can have an Organisation Analyst role’s [Access Level](#Term_AccessLevel), a Member Access Level in a Project group, a Creator [Access Level](#Term_AccessLevel) on a document they are developing, etc.   
A Teacher can have a Teacher [Access Level](#Term_AccessLevel) in a school tenancy, be an Administrator of a Gym Group, and have an Informed [Access Level](#Term_AccessLevel) in a school administration group.

**Prompts:** Does the solution’s system(s) permit multiple roles being associated to a system user?  
What are the types of allocated roles (Tenancy, Group, Resource)?

#### Non-Repudiation

The degree to which actions or events can be proven to have taken place so that the events or actions cannot be repudiated later.

##### QR-DEF-SEC-NONR-00: **Permanent** **User Operations Records**

**Category**: ISO-25010/Security/Non-Repudiation

**Statement**: The Operations of users of a Solution’s System(s) **must** be Recorded Permanently in a [Queryable](#Term_Queryable) manner.

**Rationale**: For later auditing and forensic analysis.

**Details**: The auditing of actions of both Authenticated and Non-Authenticated users is required.  
Whereas [Role](#Term_Role)s should only permit authenticated users to modify data in a system, recording the actions of non-authenticated users permit analysis of the breadth of people who have Viewed a record. This overall understanding may be important information to inform risk assessments.  
Goes towards addressing OWASP A09:2021-Security Logging and Monitoring Failures

**Prompts:** Do the solution’s service(s) permanently audit user actions?  
Do the solution’s service(s) audit all changes of data (field values before and after, and/or state of records and resources)?  
Do the solution’s system(s) audit the operations of unauthenticated users (e.g., ‘public’ users)?  
Do the solution’s services(s) provide in-system views to query audit records?

#### Authenticity

The degree to which the identity of a subject or resource can be proved to be the one claimed.

TODO

#### Accountability

The degree to which the actions of an entity can be traced uniquely to the entity.

TODO

### Maintainability

TODO

#### General

The degree of overall maintainability of a system.

##### QR-DEF-MAIN-GEN-00: **Accepted Technologies**

**Category**: ISO-25010/Maintainability

**Statement**: [Custom Code](#Term_CustomCode) **must** not be developed using technologies considered retiring or retired.

**Rationale**: Components and code that are no longer mainstream are more expensive to maintain, specifically a safe, and/or keep in a state that can be accredited to be of value and not a risk to users.

**Details**: If there are any concerns the solution’s procured systems or [Custom Code](#Term_CustomCode) are developed using technologies that may be deemed retiring or retired, ask for confirmation first.

**Prompts:** Are there any technologies used in the system you are concerned may be considered retiring or retired?  
Are there any technologies used in the system that you are concerned will no longer be available and supported over the defined expected lifespan of the system?

##### QR-DEF-MAIN-GEN-00: **Maintained Current**

**Category**: ISO-25010/Maintainability/General

**Statement**: The solution [SaaP](#Term_SaaP) service(s) components, dependencies and encryption algorithms **must** be kept current to the latest version minor released within the [defined window](#Value_UpdateWindow).

**Rationale**: Incremental small manageable updates improve security while decreasing the risk, [documentation](#Term_Documentation), and specialisation required for larger updates done at larger intervals.  
Systems that are not upgraded risk the risk of not be certifiable for use.  
Goes towards addressing OWASP A06:2021-Vulnerable and Outdated Components

**Details**: To maintain this continuous improvement post-delivery, this should be repeated as a [Transitional requirement](#Term_TransitionalRequirements).  
See Common Vulnerability and Exposure(CVEs).

**Prompts:** What strategy is used to remain abreast of service’s components versions, and prioritising work to upgrade libraries and components?  
What strategies are used to remain abreast of the available versions of [dependent service](#Term_DependentService) [API](#Term_API)s, and prioritising work to upgrade to the latest version?  
What strategies are used to remain abreast of the available versions of cryptographic algorithms, and prioritising work to upgrade to the latest version?

##### QR-DEF-MAIN-GEN-00: **Documentation**

**Category**: ISO-25010/Maintainability/Documentation

**Statement**: The solution’s [SaaP](#Term_SaaP) service(s) **must** have be provided with sufficient [documentation](#Term_Documentation) for sponsor organisation maintenance specialists to support the deployment, configuring, backing up and restoring the service(s) data.

**Rationale**: …

**Details**: …

**Prompts:** …

#### Modularity

The degree to which a solution is composed of discrete components such that a change to one has minimal impact on others.

##### QR-DEF-MAIN-MOD-00: **Modular Design**

**Category**: ISO-25010/Maintainability/Modularity

**Statement**: IF the solution’s system(s) provide capabilities within more than business domain, **then** the solution’s system(s) **must** be modular so that changes to one does not affect others or gain access to information of another without [Permission](#Term_Permission) to do so.

**Rationale**: Facilitates efficient and targeted modification, reducing risk of unintended consequences, such as using data without another

**Details**: …

**Prompts:** Does the service provide functionality within two business domains, or is it a [Platform](#Term_Platform)? If so, describe how the solution’s system(s) isolates them from each other.

##### QR-DEF-MAIN-MOD-00: **Scalable Architecture**

**Category**: ISO-25010/Maintainability/Modifiability

**Title**: Scalable Architecture

**Statement**: The solution’s system(s) **must** have a scalable architecture, permitting efficient growth over time and the incorporation of new functionality and features.

**Rationale**: Supports the solution’s system(s)’s ability to adapt to changing use cases and requirements.

**Details**: Review the design for extensibility at the solution and system(s) level.

**Prompts:** …

#### Reusability

The degree to which an asset can be used in more than one system or reused to build other assets.

##### QR-DEF-MAIN-REUS-00: **Reusable Providers & Patterns**

**Category**: ISO-25010/Maintainability/Reusability

**Statement**: IF the solution’s system(s) are [Custom Developed](#Term_CustomSystem)   
THEN the solution’s system(s) should reuse providers and patterns previously used.

**Rationale**: Leverages tested and proven components, reducing the risk of novel solutions that may be less valuable than originally expected, while still requiring additional training for support.

**Details**: [architecturally significant](#Term_ArchitecturallySignificant) changes (i.e., component or service used) must gain prior approval from [project](#Term_Project) governance.

**Prompts:** TODO

#### Analysability

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.

##### QR-DEF-MAIN-ANA-00: **Diagnostics**

**Category**: ISO-25010/Maintainability/Analysability

**Statement**: The solution’s [SaaP](#Term_SaaP) system(s) **must** develop accessible diagnostic logs.

**Rationale**: Maintenance Specialists require diagnostic logging to investigate issues.

**Details**: The level of logging must be configurable (e.g., DEBUG, INFO, ERROR, etc.).  
The duration which log entries are kept must be configurable (e.g., 31 days).  
The output location must be configurable (FileStream, remote service [API](#Term_API) calls).   
Note that logging to the local filesystem is non-permanent on [PaaS](#Term_PaaS) cloud infrastructure.

**Prompts:** Is diagnostic logging implemented?  
Is the duration entries are kept configurable at deployment or by [API](#Term_API)?  
Is the output destination type and location changeable?

##### QR-DEF-MAIN-ANA-00: **Errors**

**Category**: ISO-25010/Maintainability/Analysability

**Statement**: The solution’s system(s) **must** persist accessible records of error.

**Rationale**: Maintenance Specialists require access to records of errors to investigate issues.

**Details**: For [SaaP](#Term_SaaP) solution system(s) the records must be [queryable](#Term_Queryable) by [API](#Term_API).  
For [custom systems](#Term_CustomSystem), the records must be persisted permanently.

**Prompts:** Are errors recorded?  
Are they accessible by API by [sponsor organisation](#Term_SponsorOrganisation) people?  
In a [queryable](#Term_Queryable) manner?  
Are they recorded permanently?

##### QR-DEF-MAIN-ANA-00: **Analysable Test Reports**

**Category**: ISO-25010/Maintainability/Analysability

**Statement**: Test Results **must** develop by automation reports which are facilitate analysis and evaluation of compliance to specifications and obligations.

**Rationale**: Facilitates efficient and informed decision making to prioritise work.

**Details**: Consider developing reports that evidence Coverage, Technical Security, Functionality (System, Support & Operations, Business Service Providers, Business Service Consumers) & System Qualities.

**Prompts:** …

#### Modifiability

The degree to which a solution can be effectively and efficiently modified without introducing defects or degrading operational quality.

##### QR-DEF-MAIN-MOD-00: **Maintainable Custom Code**

**Category**: ISO-25010/Maintainability/Modifiability

**Statement**: Any [Custom Code](#Term_CustomCode) **must** be written to be maintainable, adhering to coding agreed standards, technologies, and documented for ongoing development, maintenance and use.

**Rationale**: Ensures that modifications and updates can be performed efficiently.

**Details**: …

**Prompts:** How will code maintainability be ensured (standards and tools) & periodically reported upon?

#### Testability

The degree to which test criteria can be established, and determination of whether the solution meets them.

##### QR-DEF-MAIN-TEST-00: **Multiple Non-Production Data Environments**

**Category**: ISO-25010/Maintainability/Testability

**Statement**: Multiple Test environments **must** be provided for the solution’s system(s).

**Rationale**: New [Custom System Code](#Term_CustomSystemCode) must not be deployed before being tested from different perspectives (e.g., Developers, Analysts, users).

**Details**: Build Test (BT), Developers Test (DT), System Test (ST), user Test (UT), Interoperability Test (IT) are expected.

**Prompts:** Please list any licensing or other limits and considerations.

##### QR-DEF-MAIN-TEST-00: **Test Data**

**Category**: ISO-25010/Maintainability/Testability

**Statement**: Production data **must** **not** be used for Testing.

**Rationale**: New [Custom System Code](#Term_CustomSystemCode) must not be deployed before being tested from different perspectives (e.g., developers, analysts, users, etc.).

**Details**: All [project](#Term_Project) members must not accept or permit the use of any part of production data in any other environment than the production data environment.  
The use of production data for any purpose not disclosed to end users is illegal within at least one of the [project](#Term_Project)’s jurisdictions, putting the [Sponsor Organisation](#Term_SponsorOrganisation) at risk of reputational damage and financial liabilities.   
The use of production data, irrespective of its age or size in any non-production data environment is insecure.

**Prompts:** Please confirm that you understand the prohibition and will develop new case specific test data to perform testing as required.

##### QR-DEF-MAIN-TEST-00: **Testing Characteristics**

**Category**: ISO-25010/Maintainability/Testability

**Statement**: Tests of the solution’s system(s) **must** be secure, automated, repeatable, useful and consistent

**Rationale**: Tests **must not** use production data: the use of production data, of any age or size, in a manner not disclosed to system users is illegal. Additionally, it is insecure due being more readily accessible in an unmonitored environment. Tests are to be automated to minimise impact on release scheduling, nor require manual preparations (e.g., resetting, reprovisioning databases, etc.). The automated tests must produce repeatable trustable results and reports.

**Details**: Using older data, of any size, does not make it less illegal, nor safer.

**Prompts:** Please describe what you would do if asked to work with a subset of old production data, how you will develop and provision data for test purpose,   
develop tests and reports of coverage and quality.

##### QR-DEF-MAIN-TEST-00: **Automation Tested Custom System Code**

**Category**: ISO-25010/Maintainability/Testability

**Statement**: [Custom Code](#Term_CustomCode) **must** be tested by automation.

**Rationale**: Extensions, plugins or modifications to purchased or subscribed products, or custom system development must be

**Details**: [Custom Code](#Term_CustomCode) includes [Custom System Code](#Term_CustomSystemCode), system infrastructure development code, provisioning code.

**Prompts:** …TODO…

### Portability

The degree of effectiveness and efficiency with which a system, product or component can be transferred from one hardware, software or other operational or usage environment to another. This characteristic is composed of the sub-qualities listed below.

#### Adaptability

The degree to which a solution can effectively and efficiently be adapted for different and evolving hardware, software, or environments.

##### QR-DEF-POR-ADAP-00: **Portable Custom Code**

**Category**: ISO-25010/Portability/Adaptability

**Statement**: [Custom Code](#Term_CustomCode) **must** be portable to different Operating Systems

**Rationale**: Ensures flexibility of deployment to meet strategies, available resources & skills, licensing constraints.

**Details**: As per defined definitions, while the term [Custom Code](#Term_CustomCode) includes [Custom System Code](#Term_CustomSystemCode), If the solution’s system(s) is a [Platform](#Term_Platform), it does include custom developed plugins for non-custom [Platform](#Term_Platform)s, delivery [Pipeline](#Term_Pipeline)s, including any configuration, setting and provisioning instructions, etc.

**Prompts:** Describe how applicable [Custom Code](#Term_CustomCode) is developed to meet the requirement (e.g., PowerShell, Python, JS, bash, PHP, .NET Core, etc.).

##### QR-DEF-POR-ADAP-00: **Custom System Logic Tier**

**Category**: ISO-25010/Portability/Adaptability

**Statement**: If it is a custom system, the Solution’s Service’s logic **must** remain in the orchestrating Application Tier, not spread out to lower tiers.

**Rationale**: Follow recommended best practice: avoid Stored Procedures for logic that should be in the application tier. Stored Procedures may be used to **shape** data results if database Views are not satisfactory.

**Details**: While stored procedures are valid to decrease the number of calls required to form and/or shape a query response, they are not the appropriate place to develop custom logic for multiple reasons (e.g., increase errors, testing and development costs while decreasing maintainability and modularity, etc.).

**Prompts:** Are solution system(s) custom developed?  
If so, does the solution rely on Stored Procedures?   
If so, for what reason?

#### Installability

The degree of effectiveness and efficiency in which a solution can be successfully installed/uninstalled in a specified environment.

##### QR-DEF-POR-INST-00: **Efficient Installation**

**Category**: ISO-25010/Portability/Installability

**Statement**: Applicable Solution’s System(s) Compilation, Packaging, Deployment, Configuration Provisioning processes **must** be automated, documented, rapid, idempotently repeatable.

**Rationale**: Reduces time & effort to keep systems current and rapidly available after a disaster.

**Details**: For services to be configurable by automation, [API](#Term_API)s for Configuration (e.g., Integration), System Settings (e.g., Branding), Groups, users (Identities, Personal Profiles, Memberships), and Resource Provisioning are required.

**Prompts:** Describe, at a high-level, the deployment steps, configuration, settings and provisioning process.

##### QR-DEF-POR-INST-00: **Automated Installation**

**Category**: ISO-25010/Portability/Installability

**Title**: Automated Installation

**Statement**: [Custom Code](#Term_CustomCode) **must** be deployed by automation.

**Rationale**: Reduces [documentation](#Term_Documentation) and effort while retaining IP.

**Details**: …

**Prompts:** …

#### Replaceability

Unable to define default requirements for Replaceability without mention of specific previous systems and available services. Refer to Compatibility/Interoperability.

*No requirements.*

### Regulations and Agreements

TODO

#### Data Location

TODO

##### QR-DEF-REG-DAT-00: **Data will be persisted in countries closest to Source**

**Category**: Regulations & Agreements/Data Location

**Statement**: [System Data](#Term_SystemData)[[11]](#footnote-12) **must** be persisted in datastores closest to source where cloud services are available[[12]](#footnote-13).

**Rationale**: Data Security Regulations and/or Data Sovereignty Agreements apply.

**Details**: **Do** **not** adhere to this [Statement](#Term_Statement) if it negatively impacts system performance and ultimately impacts [system user](#Term_SystemUser) efficiency and experience.

**Prompts:** Is [System Data](#Term_SystemData) persisted in countries that do **not** meet the above criteria?

# System Data Quality Requirements

Users use Systems to access Data managed by solution system(s).

They expect the data to have qualities defined by ISO-25012 quality targets.

ISO-25012 defines the qualities divided into 3 base groups:

* Inherent Data Qualities,
* Combined Data Qualities,
* System-Dependent Data Qualities.

## Inherent Data Qualities

Inherent qualities are those that the data has, irrespective of the system’s qualities.

#### Accuracy

The degree to which data has attributes that correctly represent the true value of the intended attribute of a concept or event in a specific context of use.

##### QR-DEF-DAT-ACC-00: **Data Accuracy**

**Category**: ISO-25012/Data Accuracy

**Statement**: System users **must** be provided accurate data.

**Rationale**: System users will not trust systems that provide inaccurate data.

**Details**: Data developed for this [project](#Term_Project) must be accurate before being deployed to the system.  
  
This requirement is later supported by the system validating data that is input into a system, combined with the requirement that any data provisioned into solution systems will be done via validated APIs.

**Prompts:** TODO

#### Completeness

The degree to which subject data associated with an entity has values for all expected attributes and related entity instances in a specific context of use.

##### QR-DEF-DATA-COM-00: **Data Completeness**

**Category**: ISO-25012/Data Completeness

**Statement**: Data developed for this system **must** be complete.

**Rationale**: System users will search elsewhere to complete incomplete data.

**Details**: System Resources developed for this solution’s system(s) must be completed before completion of the [project](#Term_Project)’s delivery phase.

**Prompts:** TODO

#### Consistency

The degree to which data has attributes that are free from contradiction and are coherent with other data in a specific context of use. It can be either or both among data regarding one entity and across similar data for comparable entities.

##### QR-DEF-DATA-CON-00: **Data Consistency**

**Category**: ISO-25012/Data Consistency

**Statement**: Data developed for the solution’s system(s) **must** be consistent.

**Rationale**: System users will seek consistent information from other services if data is inconsistent.

**Details**: This outcome is supported by categorising data by reference data.

**Prompts:** TODO

#### Credibility

The degree to which data has attributes that are regarded as true and believable by users in a specific context of use. Credibility includes the concept of authenticity (the truthfulness of origins, attributions, commitments).

##### QR-DEF-DATA-CRED-00: **Data Credibility**

**Category**: …

**Statement**: Data developed for the system **must** reference sources.

**Rationale**: …

**Details**: The traditional method of referencing sources in web-ready resources is via the use of hyperlinks, preferably footnoted.

**Prompts:** TODO

#### Correctness

The degree to which data has attributes that are of the right age in a specific context of use.

##### QR-DEF-DATA-COR-00: **Data Correctness**

**Category**: ISO-25012/Data Correctness

**Statement**: …

**Rationale**: …

**Details**: …

**Prompts:** …

## Combined Data Qualities

Combined data qualities are those that describe the data itself but extend or in some other manner are, to some extent, dependent on system qualities defined separately.

### Accessibility

The degree to which data can be accessed in a specific context of use, particularly by users who need supporting technology or special configuration because of some disability.

##### QR-DEF-DAT-ACC-00: **Data Accessibility**

**Category**: ISO-25012/Data Accessibility

**Statement**: Resources developed for this solution’s service(s) **must** be developed using visually impaired TODO

**Rationale**: …

**Details**: Develop and/or use WCAG 2.2 AA+ compliant icons and imagery.  
Develop text to WCAG 2.2 AA+ compliancy.   
Develop succinct and clearly readable, simple and understandable plain-language text, avoiding sector-specific jargon and acronyms where possible.

**Prompts:** TODO

### Compliance

The degree to which data has attributes that adhere to standards, conventions or regulations in force and similar rules relating to data quality in a specific context of use.

##### QR-DEF-DAT-COM-00: **Data Compliance**

**Category**: ISO-25012/Data Compliance

**Statement**: Resources developed for this solution’s system(s) **must** be developed compliant with applicable regulations within the [operating jurisdictions](#Value_OperatingJurisdictions).

**Rationale**: Non-Compliance with regulations puts the sponsor organisation at risk of reputation and/or monetary damages.

**Details**: Aside from damages, as many regulations are in place to protect accessibility and privacy of users, meeting the outcomes outlined by these regulations is often simply the right thing to do.

**Prompts:** TODO

#### Confidentiality

The degree to which data has attributes that ensure that it is only accessible and interpretable by authorized users in a specific context of use. Confidentiality is an aspect of information security (together with availability, integrity) as defined in ISO/IEC 13335-1:2004.

TODO: Print reports

##### QR-DEF-DAT-CON-00: **Confidential Messages**

**Category**: ISO-25012/Combined/Confidentiality

**Statement**: Templates for external messages **must** not include confidential information.

**Rationale**: Confidential information that is viewable outside of a system is a security impacting design error.

**Details**: Instead, emails should contain a link back to the system where users can view a report in an authorised and audited environment.

**Prompts:** Does the system use templates for developing emails and reports?  
Are they editable?  
In multiple different cultures and languages?

#### Efficiency

The degree to which data has attributes that can be processed and provide the expected levels of performance by using the appropriate amounts and types of resources in a specific context of use.

##### QR-DEF-DAT-COM-00: **Data Efficiency**

**Category**: ISO-25012/Data Efficiency

**Statement**: Resources developed for the solution’s system(s) **must** convey information to the consumer so they can make an informed decision on what action to take.

**Rationale**: Efficiency is based on change occurring, requiring an action being taken, that should be informed.

**Details**: Resources should start by describing what they are for, followed by what [value] to expect from giving attention to them, before proceeding with the information requiring communication, ending with describing what actions are recommended to take.  
Remember that the domain of ITC is the domain of communicating Information efficiently between parties, using Technology, not the subset of Technology itself.

**Prompts:** …

#### Precision

The degree to which data has attributes that are exact or that provide discrimination in a specific context of use.

##### QR-DEF-DAT-PRES-00: **Data Precision**

**Category**: ISO-25012/Data Precision

**Statement**: Resources developed for the system **must** be sufficiently precise to summarise state to inform decisions required to take actions.

**Rationale**: …

**Details**: Precision for precision’s sake, beyond system purpose, is not required, as it can unnecessarily increase the cost of research, validation and storage.

**Prompts:** What is the purpose of the system?  
Does the resource support the purpose?  
Do the facts within the resource make it easier to choose the correct action towards advancing the purpose?

#### Traceability

The degree to which data has attributes that provide an audit trail of access to the data and of any changes made to the data in a specific context of use.

##### QR-DEF-DAT-TRA-00: **Traceability** **Metadata**

**Category**: ISO-25012/ Traceability

**Statement**: Resource auditing [metadata](#Term_Metadata) **must** be sufficiently defined and managed to audit changes, by whom and when.

**Rationale**: Improvements to processes is supported by evidence of when issues occurred.

**Details**:

**Prompts:** What traceability attributes are collected?

#### Understandability

The degree to which data has attributes that enable it to be read and interpreted by users, and are expressed in appropriate languages, symbols and units in a specific context of use.  
Some information about data understandability is provided by [metadata](#Term_Metadata).

##### QR-DEF-DAT-UND-00: **Understandability**

**Category**: ISO-25012/Understandability

**Statement**: System Resources Development **must** follow guidance developed by subject matter experts (SMEs).

**Rationale**: Resources

**Details**: Consider the Language, Culture, Age and sophistication of the audience and/or Domain of the resources.

**Prompts:** Will Resources require development?  
With what key characteristics (dual language, age bracket, etc.)?  
What types of SMEs will be required?

## System Dependent Data Qualities

System Dependent Data Qualities are qualities of the data that are wholly dependent on the qualities of the system in which they are managed.

### Availability

The degree to which data has attributes that enable it to be retrieved by authorized users and/or applications in a specific context of use.

##### QR-DEF-DAT-AVA-00: **TODO**

**Category**: …

**Statement**: …

**Rationale**: …

**Details**: …

**Prompts:** …

### Portability

The degree to which data has attributes that enable it to be installed, replaced or moved from one system to another preserving the existing quality in a specific context of use.

##### QR-DEF-DAT-POR-00: **TODO**

**Category**: …

**Statement**: …

**Rationale**: …

**Details**: …

**Prompts:** …

### Recoverability

The degree to which data has attributes that enable it to maintain and preserve a specified level of operations and quality, even in the event of failure, in a specific context of use.

##### QR-DEF-DAT-REC-00: **TODO**

**Category**: …

**Statement**: …

**Rationale**: …

**Details**: …

**Prompts:** …

# System User Experience Quality Requirements

The degree to which a product or system can be used by specific users to meet their needs to achieve specific goals with effectiveness, efficiency, satisfaction, and freedom from risk in specific contexts of use.

Systems are used by users. Therefore, a high degree of user experience qualities are essential for the use of an automation system to tried, adopted and not rejected as being a waste of investment.

## Effectiveness

The degree of accuracy and completeness with which users achieve specified goals.

##### QR-DEF-USR-EFFE-00: **Effectiveness**

**Category**: …

**Statement**: The solution’s system(s) **must** enable users to perform tasks so that their managers and/or sponsors recognise an improvement in the outcome and its value.

**Rationale**: Users may like the new processes, but the solution’s sponsors must also see a return on their investment in improvement.

**Details**: …

**Prompts:** TODO

## Efficiency

The degree to which resources are expended in relation to the accuracy and completeness with which users achieve goals.

##### QR-DEF-USR-EFFI-00: **Efficiency**

**Category**: ISO-25022/Efficiency

**Statement**: The solution’s system(s) **must** be sufficiently efficient that users do not attempt to avoid using it or return to replaced methods.

**Rationale**: …

**Details**: …

**Prompts:** …

## Satisfaction

The degree to which user needs are satisfied when a product or system is used in a specified context of use.

### Usefulness

The degree to which a user is satisfied with their perceived achievement of pragmatic goals, including the results of use and the consequences of use.

##### QR-DEF-USR-USE-00: **Usefulness**

**Category**: ISO-25022/Satisfaction/Usefulness

**Statement**: The solution’s system(s) **must** be sufficiently useful that users do not wish to return to processes existing prior to the system’s introduction.

**Rationale**: Users resist change if the change is not more rewarding than continuing with existing patterns.

**Details**: …

**Prompts:** …

### Trust

The degree to which a user or other stakeholder has confidence that a product or system will behave as intended.

##### QR-DEF-USR-TRS-00: **Trust**

**Category**: ISO-25012/Satisfaction/Trust

**Statement**: The solution’s system(s) **must** **not** cause enduring distrust by users.

**Rationale**: Users that trust a service accept to use it, explore features, derive more value from it. Users that distrust a service avoid using the system, and if used, only using what they perceive as not yet failing them.

**Details**: The most basic steps to keeping a system user’s trust is to act predictably, repeatedly, and permit the undoing and/or correction of most (if not all errors) commands.  
This requirement is supported by several previously defined Quality Requirements (see requirements under ISO-25010/Reliability/Fault Tolerance).

**Prompts:** Does the solution’s service permit the undoing of user editing errors, e.g.. by permitting a user to re-edit posted comments, records, etc. – at least for a limited time, such as the next 5 minutes?  
Does the solution’s service permit the undoing of user deleting errors, e.g., by only logically deleting, avoiding physically deleting records?  
Does the solution’s service permit the undoing of message sending errors, e.g., by delaying sending by 10 seconds, providing an option to abort the operation.

### Pleasure

The degree to which a user obtains pleasure from fulfilling their personal needs.

##### QR-DEF-USR-PLS-00: **Pleasure**

**Category**: ISO-25012/Satisfaction/Pleasure

**Statement**: The solution’s system(s) **must** deliver user pleasure by efficiency, value derived and [user interface](#Term_UserInterface) aesthetics.

**Rationale**: A solution that provides pleasure leads to users returning to using a system, whereas one that displeases repels users from using the service.

**Details**: Users can gain pleasure by being surprised by positive qualities.   
Speed of login, user interface rendering, task completion are all potential examples. Completeness of outcomes is another.

**Prompts:** Are there any parts of the system that you expect would delight users?  
Are there any unique parts of the solution’s system(s) that you would expect to delight users by surprise?

### Comfort

The degree to which the user is satisfied with physical comfort.

##### QR-DEF-USR-COM-00: **Comfort**

**Category**: ISO-25012/Satisfaction/Comfort

**Statement**: The solution’s system(s) and data **must** not discomfort users.

**Rationale**: Systems gain value by being useful and used by more people and vice versa lose impact and value by being rejected by users.

**Details**: Consider the following for being inclusive rather than exclusive:  
- User Interface  
- Generated Reports  
- Resources

**Prompts:** Were culture SMEs hired to assist with the development of culture specific user interfaces, reports, resources?

## Freedom from Risk

The degree to which the quality of a product or system mitigates or avoids potential risks to economic status, human life, health, or the environment.

### Economic Risk Mitigation

The degree to which a product or system mitigates the potential risk to financial status, efficient operation, commercial property, reputation or other resources in the intended contexts of use.

##### QR-DEF-USR-FREE-00: **Economic Risk Mitigation**

**Category**: ISO-25022/Freedom from Risk/Economic Risk Mitigation

**Statement**: The solution’s system(s) **must** authenticate, limit, authorise and audit access to production data, including confidential and financial information.

**Rationale**: Users will not use a system of a [sponsor organisation](#Term_SponsorOrganisation) that puts their personal, family, or economic situation at risk.

**Details**: This requirement is supported by several system quality requirements defined earlier.

**Prompts:** Will the “Defence in Depth” Design Principle be applied to the solution’s system(s)?   
Will this include supplier organisation resource training?  
Will this include making sure that production data is only used production environments?  
Will this include implementing access controls to system functionality or data?   
Will access be permanently audited?

### Health and Safety Risk Mitigation

The degree to which a product or system mitigates the potential risk to people in the intended contexts of use.

##### QR-DEF-USR-FREH-00: **Health & Safety Risk Mitigation**

**Category**: …

**Statement**: …

**Rationale**: …

**Details**: …

**Prompts:** …

### Environmental Risk Mitigation

The degree to which a product or system mitigates the potential risk to property or the environment in the intended contexts of use.

##### QR-DEF-USR-FREN-00: **Environmental Risk Mitigation**

**Category**: ISO-25022/Freedom from Risk/Environmental Risk Mitigation

**Statement**: The solution’s systems **must** reasonably minimise environmental risk

**Rationale**: Produce less carbon by not needlessly consuming less energy.

**Details**: Design [Environments](#Term_Environment) to be built as needed, removed most of the time.  
Design [Custom Systems](#Term_CustomSystem) to be efficient.

**Prompts:** What is an expected number of permanent environments required?  
Will the service horizontally scale up and down as needed?

## Context Coverage

The degree to which a product or system can be used with effectiveness, efficiency, satisfaction, and freedom from risk in both specified contexts of use and in contexts beyond those initially explicitly identified.

### Context Completeness

The degree to which a product or system can be used with the required levels of effectiveness, efficiency, satisfaction, and freedom from risk in each of the specified contexts of use.

##### QR-DEF-USR-CON-00: **Context Completeness**

**Category**: …

**Statement**: …

**Rationale**: …

**Details**: …

**Prompts:** …

### Flexibility

The degree to which a product or system can be used with acceptable levels of effectiveness, efficiency, freedom from risk, and satisfaction in contexts beyond those initially specified in the requirements.

##### QR-DEF-USR-FLEX-00: **Flexibility**

**Category**: …

**Statement**: …

**Rationale**: …

**Details**: …

**Prompts:** …

# Transitional Requirements

Transitional Requirements, which do not describe a Solution’s System(s) are listed separately.

See *ICT Project Guidance – Definition – Requirements – Default Solution Transitional Requirements (TR)*.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | ID |  |  |  |  |  |
|  | QR-DEF-DEF-POR-REP- 00 | Default/ Portability/ Replaceability/ Integrations | If the solution’s service(s) is/are replacing an existing service, it must be able to integrate with the existing service’s required integrated services. | If delivery is dependent on changes to the integration approach, it becomes dependent on other services being able to be changed, which they may not be. | Services can be integrated using the same channels, same protocols. | Note: Being able to integrate using current approaches does not preclude the integration actually being done a new way if more secure, more maintainable, or more performant.  Integrations to check for include but are not limited to: - Directory Services (AAD) - Systems of record - Notifications (email) - Reporting - BI & Analysis - Data warehouse |

Default Functional Requirements

##### FR-INFO-META-00: **Information Metadata Management**

**Category**: TODO

**Statement**: The solution’s system(s) must provide functionality to tag information for to support discoverability and display.

**Rationale**: …

**Details**: Supports Information and Records Management Standards.

**Prompts:** …

Appendices

Appendix A - Document Information

### Versions

* 1. Initial Draft
  2. Addition of Data and user Experience Quality Requirements
  3. Preparation to remove Transitional Requirements
  4. Consolidation of Duplicates

### Images

[Figure 1: IIBA's BABOK defined Requirement types 5](#_Toc157583988)

### Tables

### References

* *ITC Project Guidance – Definition – Requirements Development*
* *ITC Project Guidance – Definition – Requirements Development – System Non-Functional Requirements*
* *ITC Project Guidance – Definition – Requirements Development – Transitional Requirements*

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

### Review Distribution

The document was distributed for review as below:

|  |  |
| --- | --- |
| Identity | Notes |
| Sandy Britain, Enterprise Architect |  |
| Duncan Watson, Enterprise Architect |  |
| Amy Orr, Data Domain Architect |  |
| Russell Campbell, Project Manager |  |
| Rodney Snell, Team Lead |  |
| Gareth Philpott, Solution Architect |  |

### 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 [international standard](#Value_Standards)s, industry 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.

##### 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.

Appendix B – FAQ

**Note:** This section to be moved to another document when completed.

**Maybe too long?**

: concerns as to length/number of requirements is practically immaterial to valuable requirement development. The number of requirements is the number of statements required to diminish misalignment of expectations and therefore project risk.   
That said, *presentation* can be employed to good effect. For one, RFx can go out with two versions of Requirements - one Short Form, and one Long Form, with and without Comments and/or Details.

Additionally, ongoing collecting feedback, monitoring use and regular maintenance of the requirements provides an opportunity to consolidate requirements as long as requirements deviate from the requirement that they are atomic/singular (see [SMART](#Term_SMART)).

**No use of Tables or Excel?**

: Excel requires licensing costs to access, provides a poor user experience whether for input or output, is practically unprintable, nor provides hyperlinks to glossaries of defined terms. Tables in Word are practically worse. While they provide hyperlinks, and better table formatting for printing purposes, they do not provide equations, references, or other basic spreadsheet functionality. Confluence pages or tables provide the lowest set of features while improving access to [sponsor organisation](#Term_SponsorOrganisation) members.

**No mention of technologies?**

: while Design Principles may dictate preferences (e.g., suite-first), quality requirement statements benefit from being defined in a technology agnostic manner.

**No mention of training?**

: training to use a system is not a quality of a system itself, hence not included in System Non-Functional Requirements. It is a Transitional concern.

**Removal of user provisioning?**

That is an incorrect statement. The requirements removes a requirement for facilitating the provisioning of unconfirmed users and assignment of [roles](#Term_Role) to them before they have formally consented to joining a system and accepting its associated [duties](#Term_Duty) and then accepting the [responsibilities](#Term_Responsibility) of a specific [roles](#Term_Role). This is done by instead preferring a process of [optionally Applying to] being Invited to Accept a [Role](#Term_Role), JIT creating a system user and identity if needed.

Appendix C – Requirement Record Template

Following guidance within *ITC Project Guidance – Definition – Requirements Development* the schema template for Requirements in this document is as shown below.

##### ID: **Title**

**Category**: …

**Statement**: …

**Rationale**: …

**Details**: …

**Prompts:** …

Appendix D – Continuous Improvements

Continuous Improvements tasks to consider:

* Continue to scan [Requirement](#Term_Requirement) [Statements](#Term_Statement) for removing reliance on the following ambiguous terms: ‘All’, ‘Any’, ‘Shall’, ‘Will Be’, ‘Should’, ‘Ever’, ‘Never’

Appendix E - TODO

* As Principles
  + NFR – Defence in Depth
* As Transitional Requirements:
  + NFR – Information Security Management

h

TODO

TODO: Print reports

* Multiple Sessions
* Integrations:
  + Corp site
* OWASP
* Transitional:
  + Workforce Experience & Makeup
  + Common Training
  + Common Tooling
  + Common Repositories
  + Processes
  + Media [for this and supporting docs]
  + Legal doc/disclosures development [where?]
* Where?:
  + Supporting systems [Not sure where to mention this]
    - Corp Site
    - Brochureware/Landing page/
    - Self-Help
    - User Support
    - User Feedback
    - Etc.
  + User Agreement
  + User Organisation [Tenancy?] Agreement 🡨---- often not thought of.
    - Translated…
  + Escrow For: Custom Modifications.
* UNI Character!!!

1. The other four types are Business Requirements (essentially, the Why, explaining the value of the change in service), Stakeholder Requirements (essentially the What is needed to deliver the changed service), Functional Requirements (How to provide for those needs), and Transitional Requirements (how to change from current to target state). [↑](#footnote-ref-2)
2. [ISO 25010 (iso25000.com)](https://iso25000.com/index.php/en/iso-25000-standards/iso-25010) [↑](#footnote-ref-3)
3. [ISO 25012 (iso25000.com)](https://iso25000.com/index.php/en/iso-25000-standards/iso-25012) [↑](#footnote-ref-4)
4. [ISO/IEC 25022:2016 - Systems and software engineering — Systems and software quality requirements and evaluation (SQuaRE) — Measurement of quality in use](https://www.iso.org/standard/35746.html) [↑](#footnote-ref-5)
5. Note that Archiving is never a business improvement or records keeping outcome, but only a performance and resource utilisation related requirement. Appropriate Indexing is a preferred means of sufficiently improving performance that negates the need to physical removal of records, which introduces other security risks (by storing in another storage location that may not have sufficient access controls and/or auditing). [↑](#footnote-ref-6)
6. which almost by definition includes all large enterprise intern services as well as all national and internationally accessed services. [↑](#footnote-ref-7)
7. [OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation](https://owasp.org/) [↑](#footnote-ref-8)
8. Functional Suitability Requirements are **not** to be confused with Functional Requirements. They instead describe the qualities of the Functional Requirements – an important difference. [↑](#footnote-ref-9)
9. [New UUID Formats (ietf.org)](https://www.ietf.org/archive/id/draft-peabody-dispatch-new-uuid-format-01.html) [↑](#footnote-ref-10)
10. [Optimizing Python: Why Python Is Slow & 4 Optimization Methods (granulate.io)](https://granulate.io/blog/optimizing-python-why-python-is-slow-optimization-methods/#:~:text=However%2C%20like%20the%20languages%20above,compiler%2C%20C%23%20performs%20considerably%20better.) [↑](#footnote-ref-11)
11. whether Non-Production and Production data. [↑](#footnote-ref-12)
12. As an example, until there is a Cloud Provider within NZ, ISO-27001-Level 2 compliant services within AU are acceptable for storage of data sourced from NZ. [↑](#footnote-ref-13)