Default Project

Baseline ICT Terms & Acronyms Glossary

# Document

## Synopsis

A catalogue of ICT specific Acronyms and Terms common to most projects, including this one, for reference by other project documentation. Referencing a central list reduces duplication and potential imprecision and risk.

## Purpose

This document is to develop an extensive glossary of general project terms for reference by other project delivery documents to reduce their need to duplicate terms and acronyms already defined here.

## Metadata

Lead Author: Sky Sigal   
Commencement: 2021

## Structure

The acronyms and terms are organised in an alphabetical manner within operation groups to permit easier discovery of terms related to a person’s role, as opposed to a whole project, which can be overwhelming.

# Terms & Acronyms

## Role Terms & Acronyms

BA

: see *Business Analyst*.

Business Analyst (BA)

: an analyst who focuses on capturing Business Sponsor an Business User Stakeholders desires as SMART & CLEAR objectives.   
See *Stakeholder Analyst*.

Business Support Specialist

: a specialist delegated to support Business Users and Business Service Consumer Users (end users). Common tasks may include being allocated delegated permissions to allocating Roles to Users within tenancies, etc. *Support Specialists* route calls for support first to them if they are available, falling back to routing inquiries to *Operations Specialists*.

CDO

: See *Chief Digital Officer*

Chief Digital Officer (CDO)

: Upon advisement from CAB, provides deployments with an Authority to Operate.

DA

: see Data Architect.

Data Architect

: architect of interoperability schemas, whether over the wire, or in storage resources accessed by other services.

Maintenance Specialists

: specialists who manage the infrastructure network, routes and devices, and deployment to them of systems and their configuration, including integration needs. Maintenance Specialists may also be involved with managing the reviewing system traces to inform development specialists of unexpected behaviours.

Operations Specialist

: a specialist role in charge of performing changes to System Settings (e.g.: Notifications) and User Configuration (e.g.: Roles) that are not handled by *Business Support Specialists* (either because there is no such Resource, or the functionality is not exposed in an intuitive way such Resources can use). *Operations Specialists* may route or handle inquiries that necessitate the involvement of *Maintenance Specialists*.

Program Manager

: manager of several Program Manager, coordinated to deliver an overall program of work’s expected outcomes.

Project Manager

: coordinator of a team’s resourcing and efforts to meet project sponsor outcome expectations. Traditionally delivery to user stakeholders to their expectations of quality and capability, while meeting

Project Coordinator

: coordinator of a Project Manager’s tasks.

SA

: see *Solution Architect*.

Stakeholder Analyst

: an analyst who queries the needs of *all* Stakeholders – not just focusing on Business Stakeholders to develop *Transition* and *System Requirements* (i.e., both *Quality* and *Functional Requirements*) comprised of both *CLEAR* and *SMART* requirements.  
A more inclusive, therefore correct, list of *Stakeholders* would include the following:

* Users,
* Business,
* Business Support,
* General Support,
* Operations,
* Maintenance,
* Assurance,
* Development
* Delivery Managers
* Project Managers
* Sponsors

Stakeholder Analyst (BA):

* an analyst that collects the Desires of all Stakeholder groups, to *Note The acronym ‘BA’ is still used, to disambiguate from Solution Architects (SAs).*

Solution Architect

: delivery Role tasked with diminishing risk of non-delivery to stakeholder expectations by developing coordination artefacts to Governance and *Project Managers (PMs)* in the form of *Solution Architecture Descriptions* (SADs) and subsequent *Technical Design Descriptions* (*TDDs*).

Support Specialist

: specialist capable of offering general support to end users, directing their inquiry according to information within the Application Support Guide (ASG), to Business Support Users, Operations Specialists or Maintenance Specialists.

Test Analyst (TA)

: a specialist skilled at defining Tests of SMART Objectives that can be converted into QA as Code by a developer, which in turn can be run by a project’s Delivery Pipeline.   
Compare to *Tester*.

Tester

: a person performing testing functionality & *qualities* of a *service*. Traditionally testing is done by hand, following Test Plans.   
Note: manual testing is expensive in time and resources and interferes with automated delivery to a level that adds significant risk to delivering IT projects on time, to expected functional qualities and functional levels. See *Test Analyst*.

## Contractual Terms & Acronyms

Master Agreement

: a base contract defining common agreements that can be reused as the base of several SoWs.

Memorandum of Understanding

: a legally non-binding agreement to achieve a mutual understanding as to vision, expectations and responsibilities before parties undertake actions, transactions or partnerships. Compare and contrast to SOW.

MOU

: see *Memorandum of Understanding*.

MVP

: see *Minimum Viable Product*.

*Note that MVP is also an apt description for projects that immediately begin delivering the business desired functionality without prior planning what else is to be delivered, and how to do so, and therefore the result is one that is missing key service Qualities (see ISO-25010).*

Minimum Viable Product

: the first publicly useable iterative delivery of a new service, that has Qualities and Functionality to be usable by a small subset of Users.

SOW

: see *Statement of Work*.

Statement of Work (SOW):

a narrative description of a project’s constraints, requirements, activities, timelines, deliverables expected from a vendor or other service provider. A SoW should be an extension of a base *Master Agreement*.

RASCI

: *Responsible, Accountable, Supporting, Consulted or Informed:* An acronym for defining the relationship of Stakeholder groups to project delivery.

## Delivery Terms & Acronyms

ADO

: see *Azure DevOps*.

Azure DevOps

An Application Lifecycle Management (ALM) suite provided by Microsoft to licensed users.

ALM

: see Application Lifecycle Management Suite.

Appication Lifecycle Management (ALM) Suite

: a suite of integrated tools to facilitate the delivery of ICT projects. Often composed of one or more of the following services: Work Item Management Service, Code Management (repository) Service, Test management Service, Pipeline Management Service.

Epic

: an epic is a grouping of Features and/or User Stories that cannot be accomplished within an single iteration of a sprint.

Feature

: a Feature is a categorisation of User Stories, generally released together.

Task

: a discrete WorkItem required to deliver a *User Story*. Depending on the system used, Tasks should be nestable as subtasks, etc.

User Story

: a *WorkItem* expressed in a manner that remains understandable for Stakeholders. A User Story is deemed incomplete without Acceptance Criteria developed by Test Analysts, and Tasks developed by implementors (eg: developers).

Work Item

: a statement of outcome & effort required, expressed as a *Epic,* *User Story, Task, Defect*. WorkItems of any type should not be referenced from Contracts as they introduce risks of ambiguity that are less present in Requirement statements. (in other words, SOWs and other contracts should reference agreed catalogues of Requirements, as opposed to referencing a list of User Stories).

Work Item Management Service

: a service to manage the categorisation, prioritisation, allocation, etc. of WorkItems digitally. Classic examples are JIRA, ADO Boards, etc. Mature work item management services can be integrated with other related services, and may be part of an Application Lifecycle Management (ALM) Suite, such as Azure DevOps (ADO).

## Discovery, Definition and Design Terms & Acronyms

CLEAR

An acronym for an approach used by Stakeholder Analysts to collect *Requirements* from designated *SMEs* of *Stakeholder groups*. The acronym stands for

* COLLABORATIVE: discussed with SMEs, developed by *Stakeholder Analysts (BAs)*, completed with *acceptance tests* developed by *Test Analysts* (TAs) design checked by *Solution* and/or *Data* *Architects* (SAs), and implementability by implementors (*Developers*).
* LIMITED: focused on a singular concern, following *Separation of Concerns* principles.
* EVALUATED: Effort-scaled and Prioritisation-rated (by implementors).
* APPROPRIATE: reduces risk of missing expectations of quality and functionality within available resources.
* RESOURCE CONCIENCE: delivers positive Value compared to Cost of delivery.

Desire

: an unstructured statement of desire by a stakeholder group’s SME or member. A Desire requires conversion to one or more Definitions as Requirements or directly

Definitions

A definition is a structured requirement that expresses a Requirement (Permission, Recommendation, Obligation, or Prohibition) or directly as a *User Story* with *Acceptance Tests*.

FR

: see *Functional Requirements*.

Functional Requirements

: the definition of the operations the system must *permit* the various *Roles* of *User* *Stakeholders*.

NFR

: see *Non-Functional Requirements*.

Non-Functional Requirements (NFR)

: legacy term, internationally deprecated by ISO/IEEE. See *Quality Requirements*.   
*Note: the term was Deprecated due to being unclear, and often became the dumping ground for Quality Requirements combined with all Functional Requirements that were not Business Requirements.*

Obligation

: a MUST type of requirement (which can be either Permissions, Recommendations, Obligations or Prohibitions).

Permission

: a MAY type of Requirement (which can be either Permissions, Recommendations, Obligations or Prohibitions).

*Note that Permissions (MAY) and Recommendations (SHOULD) types of requirements add no contractual value and should be avoided in favour of using Obligations (MUST) and Prohibitions (MUST NOT).*

Prohibition

: a MUST NOT type of requirement (which can be either Permissions, Recommendations, Obligations or Prohibitions).

Recommendation

: a SHOULD type of requirement (which can be either Permissions, Recommendations, Obligations or Prohibitions).   
*Note that Permissions (MAY) and Recommendations (SHOULD) types of requirements add no contractual value and should be avoided in favour of using Obligations (MUST) and Prohibitions (MUST NOT).*

Quality Requirements

: requirements defining the Qualities of a service, irrespective of its Functional Requirements. The Qualities expected are defined by ISO-25010 (for Systems), ISO-25012 (for the data the systems manage), and ISO-25022 (Systems in Use Qualities).  
*Note: traditionally captured in one (Word) document, Views can also be captured as separate areas within a project Wiki, assuming the Wiki’s permission structure permits access by relevant stakeholders which include but are not limited to: Consultants, Reviewers, Governance, Maintenance specialists.*

System Qualities

: the *logical* combination of the *Functional* Requirements (meeting User Requirements) and Qualities Requirements. Does not include Transitional Requirements.

SMART Objectives

: requirements that are Singular, Measurable, Achievable, Rational, Testable (preferably by Automation). See *CLEAR*.

SME

: see *Subject Matter Experts*.

Subject Matter Experts (SME)

: a Stakeholder group’s designated representative for access by a project’s stakeholder’s analyst (BA).

Transition Requirements

: are what needs to be done to transition to the solution. Below is a list of various types of activities to transition from the current state to the desired future state, and off again. These may include:

* Temporary & Persistent Security Rights & Access paths
* Temporary & Persistent Data Conversion & Migration, Validation & Testing,
* Transitional User Provisioning, Support, Training, Operations, Support, covering Users, SuperUsers, etc.
* Business Continuity, Documentation, Testing, etc.

User Requirements

: the requirements of end users, defining their expectations of working with the operations made available via the *Functional Requirements*.

## Design Terms & Acronyms

SAD

: see *Solution Architecture Description*.

Solution Architecture Description (SAD)

: a coherent set of Views describing aspects of a complex model, as described within ISO-42010. Depending on the scale of the project Expected Views will include several or all the following:

* [System] Context View, covering Background, Objectives, Constraints (Regulations), Obligations (Agreements, Principles, Requirements and Governance)
* Delivery View, covering Deliverables, Expectations, Methods of Working, etc.
* Functional View, covering how the service meets its functional requirements, illustrated by Use Cases by various Stakeholder Roles
* Integration View, covering Components and their integration
* Interoperability View, covering how Components are accessible to other services
* Qualities View, covering how the system meets its Quality Requirements
* Development View, covering expected development practices,
* Quality Assessment View, covering how quality is assured,
* Privacy View, covering how the service adheres to its (legal) privacy obligations
* Security View, covering how the service adheres to its security obligations
* Deployment View, covering automation of quality assurance and delivery

## Privacy Terms & Acronyms

Identity:

a *Person* may have one or more projected sets of *Personal Identifiable* (PI) Attributes that they share with different Groups. An Identity may have multiple Names. For example, Helen may be known as Mom while a mother in a family group, but is known as Ms. Smith in her role as PM in an office *Group*.

Identifier

: a unique attribute, sufficient to identify an object within a larger known set. Example include national identifiers (TaxID, National Student Number, etc.)

Person:

a logical (company) or physical (human) being, who will have multiple *Identities*, associated to multiple *Group*s they have a *Role* within.

Personal Identifiable Information (PII):

a set of information sufficient to identify an Identity, and hence a Person, to a high level of certainty within a larger set. A minimum may include a DOB, Location of Birth, Sex. Or a DOB, Given name and Surname, etc.

PIA

: see *Privacy Impact Assessment*.

Privacy Statement

: a statement on an digital service that explains to users how data collected from them will be used, by whom, for what purpose, and how it can be corrected. Generally referenced from a *Terms & Conditions Statement*. See *Tracking Statement*.

Privacy Impact Assessment (PIA)

: a more complete privacy impact assessment.

Privacy Threshold Assessment (PTA): completed by the project team and forwarded to the Organisation’s Privacy assessment services.   Depending on the result of the PTA, the Privacy team may require the project to complete a Privacy Impact Assessment (PIA).   The results of the PTA and/or the PIA are forwarded to the Solution Architects and the ICT Assurance teams to inform the design and SRA requirements.

PTA

: see *Privacy Threshold Assessment*.

Tracking Statement

: a statement describing how a Session is associated to a User, whether Identified or not, and what system use analytics is collected and for what purpose (Performance, experience Personalisation, Usage, Flow). Sometimes referred to as a “*Cookie Statement*”. See *Privacy Statement* and *Terms & Conditions Statement*.

## Quality Assurance Terms & Acronyms

Quality Assurance as Code (QAaC)

: Current best practice approach to testing the qualities of services by developing a set of tests that can be automated – rather than developing manual processes that can take weeks to months to perform.

Test Summary Report (TSR)

: the summary of the Quality Assurance performed by *Test Analysts*.

TSR

: see *Test Summary Report*.

## Accreditation And Governance Terms & Acronyms

Accreditation

: the formal acceptance of the residual cyber security risks posed by a solution and grants permission -- from a security perspective -- for that solution to operate.

The risk acceptance is in 2 parts:

1. the Business Owner accepts the risks on behalf of their business unit,
2. the Accrediting Authority (i.e., the CDO) accepts the risks on behalf of the Organisation.

Note: For the organisation the certification sign-off is combined with the accreditation as part of the C&A Memo.

ATO

: see *Authority to Operate*.

Authority to Operate

: what a CAB provides to a system when it has determined that all relevant stakeholders are satisfied with the system going live.

C&A

: see *Certification & Accreditation.*

Certification & Assurance

: the process which a Security Specialist follows to ensure

* the system’s data classification has been obtained,
* a PTA/PIA has been developed and signed off on,
* an S*TA* for the solution and develop
* the C&A document circulated for signature on behalf of a project before it is presented to the CAB board, along with evidence that the ASG, SSP, DI, TSR have been accepted.

C&A Memo

: the outcome of the C&A process.

Summarises:

* the business purpose of the solution (see *SAD*)
* the activities undertaken
* the state of the control environment (see *CVA*)
* the residual risk profile
* any remedial work required to address control deficiencies (see *CVP*).
* formally requests certification and accreditation until a specified date.

Certification

: issued by the Certifying Authority to signify a robust security design, build, and assessment process has been completed; and that as a result the residual risk statements are a fair reflection of the risks posed by the solution.

Controls Validation Audit

: once the CVP’s defined risk controls are built and implemented, the CVA establish their effectiveness by testing them according to the CVP’s instructions.

Control Validation Plan (CVP)

: identifies the key Security Risk Assessment (SRA) controls that must be operating effectively to mitigate risks to an accepting level, *and the method by which they will be tested*.

Developed and made available to the project right after the initial SRA is completed, so that developers can implement the controls.

CVA:

See *Controls Validation Audit.*

CVP

: see *Control Validation Plan*.

Security Risk Assessment (SRA)

: during the design phase, the Security Consultant identifies and assesses the cyber security concerns based on several inputs – Solution Architecture Design (SAD) (from which the business purpose and context, information involved, and intended audience can be determined), Privacy concerns (PTA/PIA); workshops; environmental/external factors.

The design’s mitigating controls are considered.

Mitigating controls to address the remaining identified risks are selected from the organisation’s control catalogue, which is based on NZISM and the Secure Controls Framework (SCF).

The output of this assessment is then documented in a SRA.

A CVP is prepared immediately.

*Note: Replacing the older STA approach.*

Security Risk Management Plan:

identifies any remedial activities required to address control deficiencies found during the CVA & TSA.

SRA

: see *Security Risk Assessment*.

SRMP

*: see security Risk Management Plan.*

STA

: see *System Threshold Analysis*

System Threshold Analysis (STA)

: a document prepared by a Security Specialist during the C&A process. The NZISM based process is about determining and measuring risks, along with proposed technical or procedural mitigations, and define what remains: the residual risk.    
This assessment is what is signed of on in the C&A process.

## Integration & Interoperability Terms & Acronyms

Discoverability

: ---

GraphQL

: a well-known, non-standards based, non-REST based query language for REST APIs. See *ODATA*.

OAuth

: ---

ODATA

: an industry OASIS based standard for providing *Queryability* to REST based APIs. See *GraphML*.

OIDC

:---

REST

: an acronym for a modern approach to developing a system’s APIs for consumption by other systems (not human users). See *Queryability*.

Queryability

: the capability of APIs (generally REST based APIs) to be extended by service clients to filter, subselect, order & page results. See ODATA.   
 *Note that enabling APIs to be Queryable improves usability while reducing development and testing efforts but does require more care in not introducing the ability for permit* Denial of Service (DoS) *attacks.*

SAML

:---

SOAP

:---

## Development Industry Terms & Acronyms

DRY

: an acronym for a Don’t Repeat Yourself, a key development approach to decrease development effort while increasing analysability and maintainability qualities.

Immutable

: non-changing data. Examples include system categorisation lists which remain the same throughout the service’s lifespan. See Mutable.

Mutable

: authorised user entered data, that can subsequently be corrected or even logically deleted (data should not be *physically* deleted). Contrast to *Immutable*.

OO

: ---

Object Oriented

:---

SOC

: see *Separation of Concerns*.

Separation of Concerns

: a key development approach to diminish the cost of development, analysis, maintenance and may improve portability and reuse.

SOLID

: ---

## Infrastructure Terms & Acronyms

Component

: a single (logical or physical) nestable element within a system, deployed to a Device within an Environment.

Device

: a physical or virtual device within an *environment* on which an execution environment is running, within which *components* can be nested and run.

Database Schemas as Code

: current best practice approach to developing database requirements, by describing what storage needs you need (tables, etc.) and letting automation built it to your specifications – rather than developing databases manually, which is time consuming, costly error prone, and practically impossible to maintain in a working state over a services full lifespan.

Environment

: a named, isolated virtual or physical space where a system -- composed of nested components -- is deployed to for secure access by end users.  The common list includes:

* Development Test (DT) Environment
* System Test (ST) Environment
* User Test (UT) Environment
* PreProd (PP) Environment
* Training (TR) Environment
* Compliance Test (CT) Environment
* Production (PROD or PR) Environment

Note that in mature organisations, all environments except for PROD are deployed to NON-PROD Data networks, and PROD is deployed to a PROD Data network.

Headless

: industry term for web services which have no user interfaces but do have APIs that to be invoked by separate Service Clients which do have user interfaces.

Infrastructure as Code

: a modern approach to developing system environments, by describing what you want as a set of instructions then letting automation built it to your specifications – rather than developing environments manually, which is time consuming, costly error prone, and practically impossible to maintain in a working state over a services full lifespan.

NON-PROD DATA Environment

: a network environment containing one or more system environments (DT, ST, UT, TR, CT, etc.) that do not manage production data, whether in cleartext or obfuscated, full or truncated. Contrast with *PROD DATA Environment*.

Permission

: the right for a User to perform an *Operation* within a *Request* to a *System*. Given to or restricted from *Users* as part of a *System* *Role*.

PROD DATA Environment

: a network environment containing one or more system environments (PROD).   
See *NON-PROD Environment.*

[System] Role

: a logical collection of *Permissions* to facilitate the assignment/revocation of Permissions to a System *User*.

Service

: the consumable service that a system delivers. Services can range from technical services (web services, caching services, data storage services, identity services) consumable by Systems, to business services (accounting services, HR services, etc.) consumable by end users.

Stakeholder Groups

: all Persons directly or indirectly affected in some way (RASCI) by the development and delivery of the Service.

System

: a collection of *Components* deployed to a set of *Devices* within a single *Environment*, configured, and programmed with Logic, to be Fit for the Purpose of delivering Quality Functionality that meets Users Expectations.

TSA

See *Technical Security Assessment*.

Technical Security Assessment (TSA)

: depending on the solution type, where its hosted, and its interfaces/exposure to the outside world, a TSA may be required to identify any technical vulnerabilities in the implementation.

A TSA may include some or all the following: design review, System Pen Test, configuration review, network scanning, & vulnerability assessments.   TSAs are mostly performed by 3rd party Security vendors.

UI

: see *User Interface*.

User

: a *User* is linked for authentication to a external *Person*’s Digital *Identity* managed by a *Digital Identity [Token] Provider (IDP)*. A User may be physical *Person*, or virtual (e.g. another system’s machine account authorised to use the system’s APIs).

User interface (UI)

: the service client views used to make data accessible and usable by users.

User Experience

: the combination of service client views and dynamic client-side behaviour that make system data accessible, easily understandable, and easy to use by users.

Users

: a subset of *Stakeholders* who directly engage with the *Service*.

UX

: see *User Experience*.

## Change Management Terms & Acronyms

CAB

: see *Change Advisory Board*

Change Advisory Board

: a governance board used to ensure that all stakeholders are satisfied with the state of deliverables before a solution can go live.

## Support & Operations Terms & Acronyms

ASG

: see *Application Support Guide*.

Application Support Guide

: an artefact presented for acceptance by the Support team indicating they are satisfied with the documentation available to them.

## New Zealand Government Sector Specific Terms & Acronyms

AoG

: see *All of Government*.

All of Government

: a policy or regulation that affects all sectors and departments of the government.

DIA

: See *Department of Internal Affairs*

Department of Internal Affairs

: the NZ Government Department in charge of digital.govt.nz

Digital.govt.nz

: the online source of information, tools and guidance to support digital transformation across the New Zealand public sector. Of note, they publish Standards that must be implemented and Guidance on how to do so in multiple areas including the following that MUST be considered and met where they are *Obligations*:

* Digital Service Design
* NZ Government Web Standards
* Privacy Security and Risk
* Governance
* Technology & Architecture

## Ministry Specific Units, Terms & Acronyms

The Ministry of Education’s term for organisation units and other aspects of delivery in ways that differ from other organisations. Of note:

Te Puna Hanganga, Matiko

: the group in charge of *Infrastructure & Digital*.

Digital Solution Support

: the parent group of *Support Services* (providing *Support Specialists*), *infrastructure Services (ie Puppet managed on-prem devices)*, *Cloud IaaS/PaaS (ie Azure based infrastructure)*, Cyber Security Centre (providing *Monitoring*), *Change & Transition* (providing *CAB*), *Application Support Services* (providing an aspect of *Maintenance Specialists*).

Sector Products & Service Delivery

: group in charge of providing Operational Specialists and Maintenance Specialists for services offered directly to the sector (NSI, Te Rito, etc.).

Ministry Products & Platforms Delivery

: group in charge of providing both *Operational Specialists* and *Maintenance Specialists* for services exposed to the sector, including the Ministry’s *education.govt.nz* website.

Business Product & Service Delivery

: group in charge of providing *Operational Specialists* for Ministry business systems (ENROL, etc.)

OIS

See *Operations Infrastructure Services*.

Operations, Infrastructure Services (OIS)

: now *Infrastructure Services*, under *Digital Solution Support*.

Analysis and Design

: group in charge of providing *Stakeholder Analysts* to Discover Desires and Define Requirements.

## Uncategorised Terms & Acronyms

SR

: see *Service Request*.

Service Request

A request to the organisation’s service desk for infrastructure changes done by internal resources and/or delegation to contracted services.

*Examples of their use are by development specialists to implement changes to on premise devices, firewall rules, service accounts, service account role changes, etc.*

# Appendices

## Related Documents

Consider reviewing the following documents:

Default Project Deliverables

: a list of *Deliverables* to consider from the start of a new project.