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

## Organisation

Terms are organised alphabetically under sector and type headings.

### Sector

Terms and acronyms are organised by scope, with general ICT terms at the bottom, containing the largest number of terms, leaving only a few sector specific terms to be defined on top of those.

### Type

To permit users to find their work terms faster, the terms are further separated by group activities (discovery, definition, design, development, assurance, accreditation, delivery, support, etc.).

## 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

## Project Specific Terms & Acronyms

Refer to project specific addendums to this document for project specific terms.

## New Zealand Ministry of Education 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 (i.e. Puppet managed on-prem devices)*, *Cloud IaaS/PaaS (i.e. 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.

## 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.

Budget Day

: when the government announces its intentions for revenue raising (taxes and other charges) and expenditure for the forthcoming year.

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

OIA

: see *Official Information Act*.

Official Information Act

: act under which New Zealand citizens, permanent residents, and anyone who is in New Zealand to request any official information held by government agencies - including the Ministry of Justice.   
*Note: It is an important that systems are chosen that have functionality to assist Business Support Specialists with answering OIAs in a timely manner.*

Procurement.govt.nz

: NZ AoG site providing information regarding procurement constraints, objectives and processes.

NZISM: see *NZ Information Security Manual*.

NZ Information Security Manual

: the New Zealand Government's manual on information assurance and information systems security for use by agencies, vendors, contractors and consultants. It explains processes and defines *controls* essential for protecting NZ Government information and systems. It is an integral part of the Cabinet mandated Protective Security Requirements (PSR) framework.

PSR

: see *Protective Security Requirements*

Protective Security Requirements (PSR)

: sets out New Zealand Government’s expectations for the management of personnel, information and physical security *as directed by Cabinet.*

## General Industry Terms

### ISO/IEEE/RFC Standards & Acronyms

Mature organisations optimise their operations while following endorsable and certifiable standards.

ISO-26515:2018

: standard for developing systems in an Agile manner.

See also ISO/IEC 19501:2005.

ISO-42010

: Standard for defining the structure of SADs.

ISO-19505-2

: Standard for defining *Unified Modelling Language*, a diagramming methodology.

ISO-25010

: Standard for defining the Qualities of a System. See 25012.

ISO-25012

: Standard for defining the Qualities of the Data a system manages.

ISO-25022

: Standard for defining the Experience of using a system.

RFC-2119

: key words to define Permission, Recommendation, Obligation, or Prohibition Requirements.

ISO-14143

: Function size measurement standard for estimating effort required in *Work Items*.

### Role Terms & Acronyms

Services are delivered and operated and used by a variety of stakeholders:

BA

: see *Business Analyst*.

Business Analyst (BA)

: an analyst who focuses on capturing Business Sponsor a 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.

Duty

: an obligation due to being part of a system. The origin of the word is analogues to *Due*. Contrast with *Responsibility*.

EA

: may refer to *Enterprise Architect* or *Executive Assistant*.

Enterprise Architect

: manages the definition and development of an organisation’s ecology of integrated services. Compare to *Solution Architect*.

Executive Assistant

: the assistant who coordinates a manager’s appointments, meetings & calls.   
See *Project Coordinator*.

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.

RASCI

: acronym for *Role*s one can have within a *Group* or *in regards to an activity*: Accountable for the task being achieved, while may also be one of the group of persons Responsible for doing the task(s), Supported the Responsible *Person*, Consulted for input and review, Informed or changes. An Accountable may be formally Managing the Responsible, or be a participating stakeholder.

Responsible

: a person who steps forward to accept delivering on expectations within a system.  
The origin of the word is *Respondere* – “to answer a call”. Contrast to *Duty*.

SA

: see *Solution Architect*.

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*).

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).*

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*.

### Budget and Financing Terms & Acronyms

CAPEX

: a acronym for *Capital Expenditure*, which are major purchases that a company makes for use over the long term.

Financial Year

: A fiscal year is a 12-month accounting period that a business uses for financial and tax reporting purposes.   
*Note: NZ Fiscal years are named per the year they end in, such that 1 April 2023 to 31 March 2024 is called FY24.*

OPEX

: Operational Expenditure are the BAU/day-to-day expenses that a company incurs to keep its business running.

### Contractual Terms & Acronyms

Services are procured for business providers to optimise their delivery of service to business service consumers:

Contract

: a contract between parties outlines expected outcomes, constraints, governance, methods of working, governance, and penalties for missed expectations. They must be accompanied by or include Requirements. Forms of Contracts include but are not limited to *Master Agreements* and *SOW*s.

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.

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.

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). Hence the acronym can also mean “Missing Valuable Planning”.*

POC

: acronym for *Proof of Concept*.

Proof of Concept

: a small piece of technical effort to validate a design assumption’s feasibility and cost prior to engaging additional effort to develop the desired outcome as deliverables.

RASCI

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

Requirements

: statement of expectation, given as a Permission, Recommendation, Obligation, or Prohibition, attached to Contracts.

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*.

Terms & Conditions

: Also known as Terms of Service, are constraints and Expectations on users and their behaviour for access to a Service.

### Delivery Terms & Acronyms

Acceptance Criteria

: developed by *Test Analysts*, the statements that accompany a *SMART*-ly developed *Work Item*s.

ADO

: see *Azure DevOps*.

Azure DevOps

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

ALM

: see Application Lifecycle Management Suite.

Application 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 Work Item required to deliver a *User Story*. Depending on the system used, Tasks should be nestable as subtasks, etc.

JIRA

: the name (it’s not an acronym) of the arguably the most widely used work item management service. While able to be integrated to *Confluence* (a wiki based CMS) and other services, it is not considered part of an *ALM*. Contrast to *ADO’s Board*.

User Story

: a *Work Item* 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 (e.g.: developers).

Work Item

: a statement of outcome & effort required, often expressed as an *Epic,* *User Story, Task, Defect*. Work Items of any type should not be referenced from Contracts as they introduce risks of ambiguity that are not present in correct Requirement statements. Work Items descriptions should be *SMART*. Work Items should not be considered complete and ready until they are accompanied with multiple *Acceptance* statements.

Work Item Management Service

: a service to manage the categorisation, prioritisation, allocation, etc. of Work Items 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).

User Voice Service

: a Service to collect and manage User support, feedback and issue tracking. Not to be confused with a *Work Item Management Service* -- which it is beneficial to be integrated with.

### Discovery, Definition 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 reasonable feasibility and effort required 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

Definition

: a structured Requirement (Permission, Recommendation, Obligation, or Prohibition) or *User Story* \*with *Acceptance Tests)* Work Item.

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

4+1

A term to describe the deprecated 90’s structure for *SAD* documents. A 4+1 *SAD* was comprised of:

* *Logical View*, describing the logical functionality made available by a system
* *Process View*, describing dynamic sequence flows between system aspects
* *Development View*, describing how the system logic is packaged into discrete elements
* *Physical View*, describing how the system packages are deployed to target devices
* *User Scenarios*, describing a series of indicative examples of how the service is used.

*Note: superseded by the structure advocated within ISO:42010:2011, popularised by Rozanski & Woods seminal industry book.*

Layer

: to improve maintainability correctly designed services are developed into isolated layers. The most common stack of layers is Presentation, Interface/Validation, Logic, Technical Integration (a subset of which is Data Storage). See *Tier*. See *DDD*.

DDD

: acronym for *Domain Driven Design*.

Domain Driven Design

: a design approach to develop moderate to complex systems (most enterprise services fall in this category) using mature design decisions to deliver a service that remains modular, modifiable, enhancable and maintainable.

Rozanski & Woods

: the authors of a seminal industry book on how to structure *SAD*s in accordance with *ISO-42010*. They popularised SADs comprised of the following views:

* [Service] Context View, describing the business context of the service,
* Functional View, describing the functions provided by the system
* Information View, describing the HL entities the system is managing
* Integration View, describing systems the system integrates with, and messages transmitted to and from,
* Infrastructure View, describing the target devices and zones the system components are deployed to,

The following Perspectives could be appended as sub sections within the above Views -- or developed as additional Views:

* Security
* Privacy

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

Note that a *Description* does not have to be a *Document*. A SAD can be developed in Word or Confluence, or any medium that provides both sufficient access to contributors and consultants, and versioning sufficient to support the accountability required of an accreditation process.

UML

: acronym for *Unified Modelling Language*.

Unified Modelling Language

: an *ISO* defined diagramming standard for modelling structural, behavioural, architectural aspects of systems. See *ISO-19505*-2.

### System Data 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*.

### Service 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.

### System Integration Terms & Acronyms

ETL

: acronym for *Extract Transform Load*. Prefer to extract and load by API rather than direct storage access. This enables validation logic being applied. Logic should be in a logic layer, above and protecting the data storage layer/tier.

ELT

: acronym for *Extract Load Transform*. A variation to ETL.

Tier

: a physically separate *Layer* of a system.

### System Interoperability Terms & Acronyms

**API**: acronym for *Application Programming Interface*.   
*Note that the term Programming is possibly an unfortunate choice of word, as It implies a highly capable programming interface, a legacy concept, whereas current REST based interfaces is about messages and not operations.*

Discoverability

: the ability for a service endpoint to be discovered, by being published or self-publishing itself in a directory elsewhere.

Self-Describe

: the ability of an API to self-catalogue its endpoints, their arguments, and their request and response messages, greatly diminishing errors in documentation and implementation.

WADL

: a REST equivalent of WSDL as a technical option for a service to [self-]describe its available endpoints. See *ODATA*’s metadata, which is CSDL.

CSDL

: Conceptual Schema Definition Language. A machine readable description of a *schema*. Used by ODATA to describe its endpoints, their messages, and relationships.

GraphQL

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

OAuth

: open standard for access delegation, used to permit other services (not physical Persons) access to a service. OIDC, used to grant Persons, is built on top of it.

ODATA

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

OIDC

: an authentication layer built on top of *OAuth* to authenticate end users to systems.

REST

: an acronym for *Representational State Transfer*, a modern approach to developing a system’s APIs for consumption by other systems (not human users). Prefer to using *SOAP* based intergration. See *Queryability*.

Queryability

: the capability of APIs (generally REST based APIs) to be extended by service clients to filter, sub-select, 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

: an open standard for authentication, based on XML, capable of being used across multiple channels, including the web.   
*Note: Prefer OAuth & OIDC on the web.*

SOAP

: acronym for *Simple Object Access Protocol*, an older messaging protocol specification for exchanging structured information in the implementation of web services in computer networks.  
*Note: prefer using REST.*

JSON

: an acronym for *JavaScript Object Notation*, is an open standard file format for data interchange on the web. Has overtaken XML for general use cases due to its comparative simplicity.

XML

: a markup language for defining any data. Used for many purposes, including the interchange of data between systems across multiple channels. See *JSON*.

### System Data Storage Terms & Acronyms

Datastore

: any form of data storage. The primary types are classified as:

* Relational (traditional databases)
* Non-Relational (no-SQL, blob, key-value, etc.)

Key

: an attribute (column) or a set of attributes that help to uniquely identify a tuple (or row) in a table within a datastore or table. See *Primary Key*.

Natural Key

: a key derived from the data itself (e.g.: a national person identifier), as opposed to an attribute generated by the database (e.g.: row number or a guid).

Natural Primary Key

: a *natural key* used as the table’s *primary key*.   
*Note: It is also a design error, due to severely impacting performance negatively.*

Normalised

: the process of structuring *relational databases* in accordance with a series of so-called *normal forms*  in order to reduce data-redundancy and improve data-integrity.

Primary Key

: the *key* in a relational database table that's distinctive for each record. See *key*.

Relational Database

: a relational database is a collection of information that organizes data in predefined relationships where data is stored in one or more tables (or "relations") of columns and rows, making it easy to see and understand how different data structures relate to each other. The organisation of these tables is referred to as a *schema*.

Schema

: the definition of how information is persisted in a datastore (generally a relational database).

Secure keystore

: a non-relational key-value datastore for confidential information, usually integration information.   
Note: a relatively common high value example use case is to only permit a deployment pipeline to be a member of the secure keystore, to retrieve confidential integration credentials which it then injects into deployments, removing the risk of humans accessing, knowing and disclosing these credentials.

Indexed

: a table that is indexed upon insertion of new records, to speed up subsequent finding of records.

Unoptimised

: a database who’s performance is impacting system performance. The causes are often one or more of the following:

* Tables are not effectively *normalised*
* tables miss useful indexes
* tables have too unnecessary non-valuable indexes and omission.

Optimised

: a table or database on which work has been done to remove causes of for it being unoptimized.

### System 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

: see *Object Oriented*.

Object Oriented

: a computer programming model that organizes software design around data, or objects, rather than functions and logic. See *SOLID* which provides principles on how to deliver OO, and *DDD*, which outlines how to organises OO code into deployable components and pakages that maximise *maintainability* and *modifiability* while minimising *complexity*.

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

: a mnemonic acronym for five design principles intended to make object-oriented designs more understandable, flexible, and maintainable:

* Single Responsibility principle (see *Separation of Concerns)*.
* Open-Close Principle (open for extension, closed for modification).
* Liskov’s Substitution Principle (use interfaces rather than concrete classes).
* Interface segregation Principle (use smaller interfaces).
* Dependency Inversion Principle (see *Injection*).

*Note it may be of interest to know that SOLID only captures the first 5 principles of Uncle Bob’s 10 principles.*

GRASP

: an acronym for General Responsibility Assignment Software Principles. Another well known and valuable set of development patterns to guide development towards delivering long term value:

* controller,
* creator,
* indirection,
* information expert,
* low [coupling](https://en.wikipedia.org/wiki/Coupling_(computer_science)),
* high [cohesion](https://en.wikipedia.org/wiki/Cohesion_(computer_science)),
* [polymorphism](https://en.wikipedia.org/wiki/Polymorphism_(object-oriented_programming)),
* protected variations, and
* pure fabrication

### System 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.*

LAN

: acronym for Local Address Network

Local Address Network

: contrast with WAN.

[System] Role

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

Router

: device used to route traffic between *networks* and *subnets*. Contrast to Switch.

Subnet

: a network within a network that provide two notable benefits: making for more efficiency traffic between devices by not requiring routers, and permit traffic to devices be limited to known source devices outside the network.   
  
*Note: when designing the infrastructure requirements of information services, it remains best practice is to use a subnet for data storage devices, and limiting traffic to it from only another subnet, containing the logic of an information service.*

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 *Person*s 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.

Switch

: a device to route traffic within a network (contrast with Router).

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*.

### Service Change Communications & Management Terms & Acronyms

CAB

: see *Change Advisory Board.*

Change Advisory Board

: a governance board to ensure that before a solution can go live all stakeholders are satisfied with the state of deliverables required to support, operate and maintain the service over its service lifespan.

Corporate Website

: see *Enterprise website*.

Enterprise Website

: enterprise’s website, on which information about the new service is made available and the service is made discoverable by linking to the service.

*Note: Information about the Service commonly will include Purpose, Objectives, Background, Terms & Conditions, Use Cases, Usage Examples, Scope, Scheduling, Applicability (e.g.: phased roll outs), a FAQ, direct Contact information to a Business Support Specialist group, or General Support that can direct inquiries to them.*

### Service 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.

### Uncategorised Terms & Acronyms

BOSSCARD

: an acronym for *“Background, Options, Stakeholders, Scope, Constraints, Assumptions, Risks, expected Deliverables”* – the subject matters to include in a synopsis of current state of a project.

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.