Project Delivery

Accreditation

Document

## Synopsis

All Organisations are constrained by obligations defined by law, regulation, agreements and internal policy.

Government agencies are further constrained by additional mandated All of Government (AoG) obligations.

A Service can only be made available to the public (i.e., Go Live) by a delivery manager raising a Request for Change (RFC) for deployment to a production data (PROD-DATA) environment. The RFC will only be processed once the service has been granted an Authority to Operation (ATO) by the Chief Digital Officer (CDO), whom will only issue the ATO upon recommendation of the Change Advisory Board (CAB). The CAB will only issue this recommendation upon confirming from its board members that they the project is meeting its legal, regulatory, and policy obligations. The meeting of these obligations is evidenced by the service having completed a Certification and Acceptance (C&A) process, a Quality Assurance (QA) process, and applicable parties have received the deliverables they require to deploy, monitor, maintain, operate, and support the service over the whole service lifecycle, without requiring assistance or further information from the original development team.

This document describes the dependencies, deliverables, processes and advised sequencing to follow to obtain the above in a manner that meets project expected scheduling.

## Author & Version

Author: Sky Sigal, Solution Architect  
V0.1 Date: 18/05/2021

## Distribution & Review List

* Amy Orr, Data Architect
* Brad Atte Le Crouche, Solution Architect
* Diane Simpson, Infrastructure Architect
* Dries Venter, Cloud Infrastructure Specialist
* Grayson Mitchell, Manager, BE&S ICT Strategy Planning & Architecture
* Jeff Grove, Security Specialist, Contractor
* Jogeshni Prasad, ITC C&A Specialist, Contractor
* Sally Murrey, ICT Change Advisor
* Sandy Britain, ITC SPA Enterprise Architect
* Sean Torley, ICT Change & Transition
* Stuart McGrigor, Solution Architect
* Werner Van der Merwe, Automation Lead
* Yujia Huang, Security Specialist, Contractor

## Contents

[1 Document 1](#_Toc78722290)

[1.1 Synopsis 1](#_Toc78722291)

[1.2 Author & Version 1](#_Toc78722292)

[1.3 Distribution & Review List 2](#_Toc78722293)

[1.4 Contents 2](#_Toc78722294)

[2 Context 5](#_Toc78722295)

[2.1 Dependencies 5](#_Toc78722296)

[2.2 Background 5](#_Toc78722297)

[2.3 Objective 5](#_Toc78722298)

[3 Obligations 6](#_Toc78722299)

[3.1 Regulations 6](#_Toc78722300)

[3.2 Policies 7](#_Toc78722301)

[3.3 Standards 7](#_Toc78722302)

[3.3.1 International Standards 7](#_Toc78722303)

[3.4 NZ Specific Standards 9](#_Toc78722304)

[3.5 NZ Specific Frameworks 9](#_Toc78722305)

[3.6 Principles 10](#_Toc78722306)

[3.7 Ethical 10](#_Toc78722307)

[4 Governance 12](#_Toc78722308)

[4.1 Design Authority (MDA) 12](#_Toc78722309)

[4.2 Technical Working Group (TWG) 12](#_Toc78722310)

[4.3 Digital and Information Design Group (DIDG) 12](#_Toc78722311)

[4.4 The Change Advisory Board (CAB) 12](#_Toc78722312)

[4.4.1 Process 12](#_Toc78722313)

[4.4.2 CAB Members – Governance & full Lifecycle Stakeholders 13](#_Toc78722314)

[5 Deliverables and Sequencing 19](#_Toc78722315)

[5.1 Objective 19](#_Toc78722316)

[5.2 Scheduling 19](#_Toc78722317)

[5.3 Design Services Engagement 19](#_Toc78722318)

[5.3.1 Solution Architecture Description (SAD) Deliverable 19](#_Toc78722319)

[5.3.2 Solution Architecture Description Summary (SADS) Deliverable 19](#_Toc78722320)

[5.3.3 Data and Information Design Group (DIDG) Endorsement 20](#_Toc78722321)

[5.3.4 Technical Working Group (TWG) Endorsement 20](#_Toc78722322)

[5.3.5 Technical Documentation (STD) Deliverables 20](#_Toc78722323)

[5.4 Deployment, Infrastructure and Operations Services Engagement 20](#_Toc78722324)

[5.4.1 Application Lifecycle Management (ALM) Deliverable 20](#_Toc78722325)

[5.4.2 Idempotent Infrastructure Environment Provisioning 21](#_Toc78722326)

[5.4.3 Idempotent Data Management Automation Deliverable 21](#_Toc78722327)

[5.5 Data Services Engagement 21](#_Toc78722328)

[5.5.1 Information Classification Deliverable 21](#_Toc78722329)

[5.5.2 Data Information Management Principles (DIMP) Alignment Deliverable 22](#_Toc78722330)

[5.5.3 NZ Government Open Access & Licensing (NZGOAL) Alignment Deliverable 22](#_Toc78722331)

[5.6 Privacy Office Engagement 22](#_Toc78722332)

[5.6.1 Privacy Threshold Assessment (PTA) 22](#_Toc78722333)

[5.6.2 The Privacy Threshold Assessment (PTA) 23](#_Toc78722334)

[5.6.3 Privacy Impact Assessment (PIA) 23](#_Toc78722335)

[5.7 Certification & Assurance (C&A) Services Engagement 23](#_Toc78722336)

[5.7.1 Scheduling 23](#_Toc78722337)

[5.7.2 Security Risk Assessment (SRA) 23](#_Toc78722338)

[5.7.3 Technical Risk Assessment (TRA) 24](#_Toc78722339)

[5.7.4 Risk Mitigation 24](#_Toc78722340)

[5.7.5 Residual Risk 25](#_Toc78722341)

[5.7.6 Control Validation Plan (CVP) Deliverable 26](#_Toc78722342)

[5.7.7 Control Validation Audit (CVA) Deliverable 26](#_Toc78722343)

[5.7.8 Control Validation Audit (CVA) (“Trust – but verify”) 26](#_Toc78722344)

[5.7.9 Risk Categorisation 27](#_Toc78722345)

[5.7.10 Risk Acceptance 27](#_Toc78722346)

[5.8 Quality Assurance (QA) Services 27](#_Toc78722347)

[5.8.1 Test Definition Reports Deliverables 28](#_Toc78722348)

[5.8.2 Testing Summary Report (TSR) 28](#_Toc78722349)

[5.9 Development Services Engagement 28](#_Toc78722350)

[5.9.1 Automation 28](#_Toc78722351)

[5.9.2 Unit Tests Suite Deliverable 29](#_Toc78722352)

[5.9.3 Use Case Tests Deliverable 29](#_Toc78722353)

[5.9.4 System-Device Server Code Deliverable 29](#_Toc78722354)

[5.9.5 Client-Device System Code Deliverable 29](#_Toc78722355)

[5.9.6 Environment Configuration Automation Deliverable 29](#_Toc78722356)

[5.9.7 Development Documentation 30](#_Toc78722357)

[5.10 Change Advisory Board 30](#_Toc78722358)

[5.11 Production Environment Go-Live Request for Change (RFC) 30](#_Toc78722359)

[6 Appendices 31](#_Toc78722360)

[6.1 Glossary 31](#_Toc78722361)

[6.2 Ministry Deliverable/Tools Resource Templates 34](#_Toc78722362)

[6.2.1 SSP Template: 34](#_Toc78722363)

[6.2.2 Application Support Guide (ASG) Template 34](#_Toc78722364)

[6.2.3 SLA Template 34](#_Toc78722365)

[6.3 Documentation Deliverables 34](#_Toc78722366)

[6.3.1 Application Support Plan (ASP) 35](#_Toc78722367)

[6.3.2 System Support Plan (SSP) 35](#_Toc78722368)

[6.3.3 Business Support Plan (BSP) 35](#_Toc78722369)

[6.3.4 Monitoring Support Plan 35](#_Toc78722370)

[6.4 Security 35](#_Toc78722371)

[6.5 Integrations 36](#_Toc78722372)

[6.5.1 Digital Identity 36](#_Toc78722373)

[6.5.2 Digital Warehouse 36](#_Toc78722374)

[6.5.3 National Archives 36](#_Toc78722375)

[6.6 Qualities 36](#_Toc78722376)

[6.6.1 Supportability 36](#_Toc78722377)

[6.6.2 Maintainability 36](#_Toc78722378)

[6.6.3 Functionality 36](#_Toc78722379)

[6.7 Quality 37](#_Toc78722380)

[6.8 Authority to Operate Dependencies (A3 Diagram) 38](#_Toc78722381)

# Context

## Dependencies

This document is a subject specific addendum to another document expected to have been read first: *IT Project Delivery – Methodologies and Processes*.

## Background

Projects started and organically grown in isolation by departments, potentially led by contractor or new managers and scrum masters -- using contractor or vendor provided developers -- will have a limited view of the required capabilities, resources, ongoing obligations -- and therefore long term cost implications -- of releasing new services.

Let alone an enterprise-wide view of work by other departments that may be duplicating the same effort.

In essence:

* Services have a longer lifecycle than the development phase, and therefore have additional stakeholders than development stakeholders,
* Service projects funded by an enterprise’s common treasury have obligations to these other stakeholders,
* As for any service, service projects have obligations to regulations and laws of the countries in which the service is produced and delivered,
* Government services, financed by treasury obtained from taxes prior to development, have further obligations than commercial services to deliver value as there is no market-based mechanism for users to signal their valuation of the service,
* Departments have a duty to not be wasteful of common treasury by working in isolation, potentially being wasteful duplicating functionality already available or planned elsewhere.

This document outlines the organisation’s Certificate & Assurance (C&A) process to ensure projects understand their responsibilities and obligations and the organisation gets the best value for the common treasury spent on them.

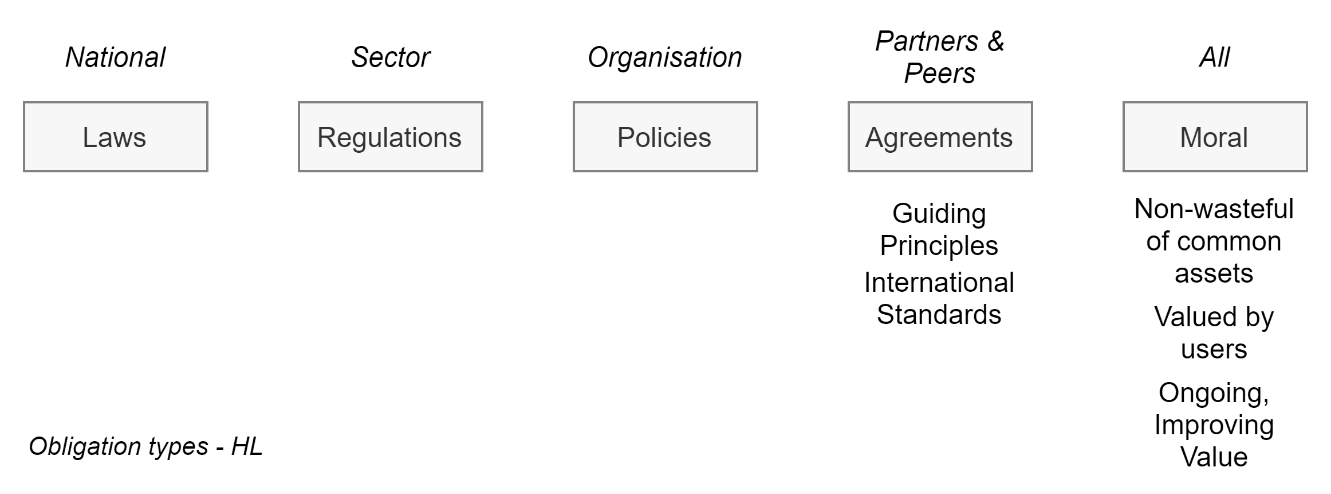
## Objective

The objective for an implementation and delivery manager is being enabled to issue a Request for Change (RFC) for a service to be deployed to a production data (PROD-DATA) environment for access by a full or limited set of users.

All RFCs raise automated workflow processes comprised of multiple steps – the first one being to verify that the project has received an Authority to Operate (ATO) from the Chief Digital Officer (CDO) upon being advised by the Change Advisory Board (CAB) that Obligations to relevant Stakeholders have been fulfilled, or temporarily delayed with a plan in place to address them in a timely manner.

After going live, services must continue to demonstrate to the CAB that the Obligations continue to be met, with evidence that any temporary exemptions have been addressed, and the service and system continues to be improved to address new risks as they evolve.

# Obligations



Obligations come in the form of laws & regulation, sector and enterprise policies, and sector and enterprise governance agreed guiding principles.

Laws, Regulations, policies and principles in turn dictate the use of international standards to enable system integration and lower costs over a service’s lifecycle.

## Regulations

All organisations that manage internal or public facing government IT services are required by law and regulation to adhere to acts and regulations:

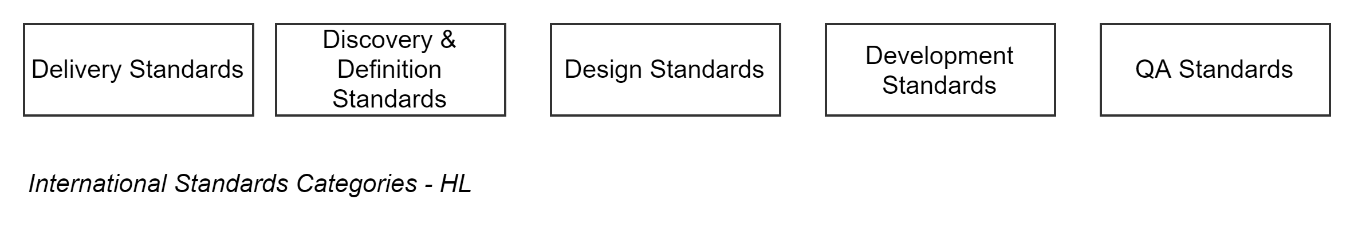
* The Privacy Act - to protect the privacy of users of the published system, to provide the public to correct the information held on them, to provide them the certainty of being warned in a timely manner if a breach has occurred, and deter organisations -- with stiff fines and/or penalties -- from being careless with the protection of citizens personally identifiable information.
* The Official Information Act – to provide public accountability on demand as to the actions and decisions of their government,
* The Public Records Act – to keep records for long term research and learning opportunities to improve governance over time.
* The Education Act – to provide education sector wide collaboration across independent education provider organisations, while not contravening the Privacy Act.
* Cabinet Decisions:
  + Requirement to use Protective Security Requirements (PSR), including the use of the NZ Information Security Manual (NZISM):  
    CAB MIN (14) 39/38 (<https://bit.ly/3xKfoFr>)
  + Requirement to use the NZ Government Web Standards (NZGWS):  
    CAB Min (03)41/2B (<https://bit.ly/2UruwJt>)
  + Requirement to adhere to NZ Data and Information Management Principles  
    [Cabinet Minute CAB Min (11) 29/12](https://www.data.govt.nz/assets/Uploads/cab-min-11-29-12-8-august-2011.pdf) (<https://bit.ly/3BgbBSl>)
  + Requirement to adhere to the NZ Government Open Access and Licensing Framework (NZGOAL)  
    (<https://bit.ly/3hPm13L>)
* The NZ Procurement Regulations, Rule 61[[1]](#footnote-2), ensures that any digital web service procured by an organisation must enforce the NZ Government Web Standards.

## Policies

The organisation’s policies dictate the use of governance bodies to enforce the use of design principles, standards & regulations, ensuring value is maximised and reputation is protected for the whole organisation, as opposed to a single project’s objectives.

The governance bodies are described later.

## Standards



### International Standards

NZ Government spends significantly on participating in the development of international standards to help NZ governments develop better quality results.

Hence the obligation by NZ government standards to adhere to International Standards to deliver solutions to the highest standard, when standards are available.

Key standards that government agencies are obligated to follow unless explicitly exempted include:

#### Software System Delivery and Lifecycle Management

The following standards provide common terminology, guidance, expected deliverables for software system delivery to be followed and led by project managers:

* ISO/IEC/IEEE 12207 Systems and software engineering
* ISO-15288 – Systems and software engineering — System life cycle processes
* ISO-15289 – Systems and software engineering — Content of life-cycle information items
* ISO-29110 – Systems and Software Life Cycle Profiles and Guidelines for Very Small Entities

#### Stakeholder Analysis Standards

The following standards provide common terminology, guidance, expectations for software system requirements gathering, to be adhered to by Stakeholder Analysts:

* ISO/IEC/IEEE 29148:2011 Systems and software engineering — Life cycle processes — Requirements engineering

#### Design Standards

The following standards provide common terminology, guidance and expectations for software system design & documentation, to be adhered to by architects presenting technical options and solutions:

* ISO-42010 – Systems and software engineering — Architecture description – is used to define how SAD documents are developed to ensure correctness, completion and comprehension by qualified stakeholders,
* ISO-19505 – UML defines how diagrams within information system documentation are to be developed for correctness, completion, clarity by relevant qualified stakeholders.
* ISO-13028 - Information and documentation - Implementation guidelines for digitization of records

#### Development Standards

The following standards provide common terminology, guidance and expectations for software system design by architects and technical leads, and subsequent development by development specialists:

* ISO-8601 – Data elements and interchange formats for dates and times (applicable to API design).
* ISO/IEC 9834-8:2008 – UUID – defines the development of client side sequential (i.e., time based) UUIDs to allow for international synchronisation, and faster performance via non-locking tables than locking integer-based table clustered indexes.
* ISO-3166 – Country Codes (Numeric/ALPHA-2/ALPHA-3) – relevant in international systems, as well as enforcing national embargoes on certain countries.
* ISO-6390-2 – Language Codes – relevant for providing systems in both of NZ’s spoken national languages, as well as other languages within NZ’s multi-cultural society.
* ISO-4217 – Currency Codes – relevant in international systems
* ISO-5218 – Sex – defines the sex (not natural/stated/preferred gender) of a Person.

#### Data Standards

* ISO-25012 – Data Quality Model – defines an international agreed set of Qualities to assess the information of a system.

#### Security Standards

* ISO 27001 relates to the way an organisation keeps data accurate, available and accessible only to approved employees.

#### Privacy Standards

* ISO 27701 relates to the way an organisation collects personal data and prevents unauthorised use or disclosure.

#### Quality Assurance Standards

The following standards provide common terminology, guidance and expectations for software system QA specialists to test services for their delivery on expected qualities and functionality:

* ISO-25022 – Product Quality Requirements and Evaluation – standards to evaluate offerings *before* they are procured, and after they have been delivered.
* ISO-25010 – Systems and software Quality Requirements and Evaluation – provides an agreed set of Qualities to assess a system by.
* ISO-25012 – Data Quality Model – defines an international agreed set of Qualities to assess the information of a system.
* ISO-25045 –
* ISO-25030 – Quality Evaluation – instruction on how to evaluate 25010/25012.

#### Support Services

* Refer to ISO-9000

#### Organisation Delivery Maturity Standards

All the above standards contribute to the maturity of the organisation’s practices and its ability to adhere to the following overarching standards:

* ISO-9000 Series[[2]](#footnote-3)
* ISO 30071-1: Embedding Accessibility in business activities

In-house documentation summarizing cost-effective, key applicable/expected aspects of the above standards for easier application in projects is often available upon request from the ITC SPA group.

## NZ Specific Standards

#### Accessibility Standards

* The NZ Government Web Standards (NZGWS)[[3]](#footnote-4) – to ensure digital services are available to the widest range of citizens, irrespective of their abilities, by meeting at least minimum standards of international Web Accessibility Standards. In addition, to provide trust in the services provided by government agencies, Government, Ministry, Agency, Crown Entity branding specifications must be followed.

## NZ Specific Frameworks



In addition to International ISO standards, NZ Government Agencies are mandated to adhere to NZ specific frameworks.

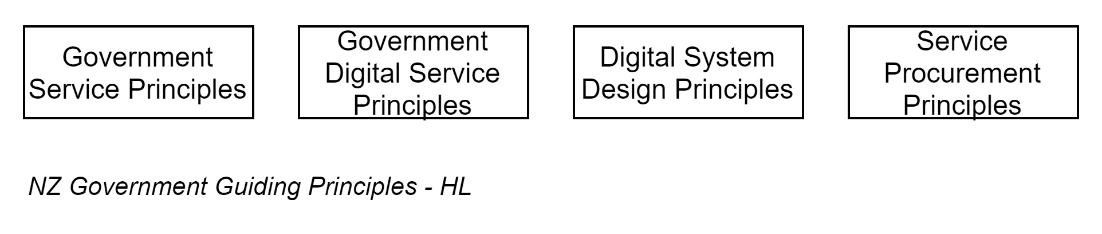
#### Information Security Guidance

* The NZ Government Security Classification – classifies data which in turn determines the minimum controls required to mitigate risks associated to managing the data,
* The NZ Government Open Access and Licensing Framework (NZGOAL) is mandatory for the development of new content.

#### Procedural and System Security Guidance

* The NZ Protective Security Requirements (PSR) are mandatory and INFOSEC2 enforces the use of the NZ Government Security Classification System and following NZISM recommendations for minimum controls for information.
* The NZ Government NZ Information Security Manual (NZISM) regulates how any information is to be managed by a government ministry, agency, crown-entity system and the personnel who maintain it.

## Principles



In addition to regulated objectives and using international and national standards and guidance to get there, government agencies are required by regulation to manage projects to deliver on objectives according to specified sets of Principles:

* The Digital Service Design Standards – specify Principles to be adhered to when delivering public services digitally, over its whole of service lifecycle.

## Ethical

Although not enforceable by regulation, law, or prior agreement, there are ethical obligations to others.

Government resources are funded by treasury collected from tax contributing members of society prior to projects being completed or even begun.

In effect, users do not have market mechanisms (e.g.: avoiding the service, switching to a competitor, etc.) at their disposal to indicate their valuation of the services provided. Nor can they in many cases as governments are the only legal service provider in certain service categories.

In addition, it is the nature of current government funding to prioritise capital expense over operational expense. Funds will be allocated for initial development to meet the stated objectives of approved business cases, and some will be approved for minimal maintenance over the service’s lifetime – but little to none allocated for ongoing meaningful improvement of the service.

In addition, it is the nature of current government funding practices that obtaining funds to enhance or replace existing services before imminent failure is difficult -- even if the service has become unfit for purpose – before its initial capital investment has been devaluated.

Therefore, it is morally correct for developers & deliverers of government services to expend sufficient effort to deliver services with appropriate qualities[[4]](#footnote-5) -- by adhering to guiding principles, international standards and industry best practices.

Common traits of maintainable services include the following:

* Using automation for infrastructure and code development, deployment, QA, and DR, to encodes critical knowledge long after key personnel are no longer available
* Are deployed to environments that are secured, monitored, cost-effective and modern
* Use Analysis, Development and QA practices that do not jeopardise security, while decreasing reliance on costly manual capabilities and in-depth documentation.
* Custom development is done using Modular design & development practices (Client-Server system architectures, DDD component architectures, GRASP/SOLID development practices).
* A Certificate & Assurance (C&A) specialist will have interviewed key delivery stakeholders, have the system technically investigated, develop an assessment of the service’s probable risks[[5]](#footnote-6), prepare a plan[[6]](#footnote-7) to mitigate them, ensure they are applied, and have any residual risks accepted by the business owner.

# Governance

Different governance bodies will oversee the completion of the obligations and reduction of risk.

## Design Authority (MDA)

The Ministry Design Authority ensures that funding of business plans that have a technical element align with overall digital strategies.

Endorsement from the MDA is a pre-requisite for a Biz Case being approved.

## Technical Working Group (TWG)

The TWG oversees the application of design and development standards and principles, and the project’s adherence to what was previously endorsed by the Design Authority (DA).

The TWG is composed of Information and System design (ITC) stakeholders from the ITC SPA group.

## Digital and Information Design Group (DIDG)

The DIDG overseas and advices on

* By reviewing and advising the shape & attributes names of messages between systems
* By reviewing and advising on the shape & attributes of internal system data that is intended for sharing with a data warehouse or archives, such that the data aligns where possible with agreed standards.

Changing the shape of data storage is not possible with third party services, in which case the discussion becomes about the shape of the data that is extractable from the system.

## The Change Advisory Board (CAB)

For the CAB to advise the CDO that a service is acceptable in a Production Environment it relies on receiving assurances from its members (multiple ITC group managers) that their teams are satisfied with handling the system in production.

This assurance is given after the various parties have verified:

* the accessibility, quality, correctness and completeness of the documentation deliverables issued with the service enable the service to be Monitored, Maintained, Enhanced and Supported without recourse to the original delivery stakeholders
* the service itself is secure, operable, supportable, maintainable, while meeting its security, privacy, accessibility, usability, branding, discoverability obligations.

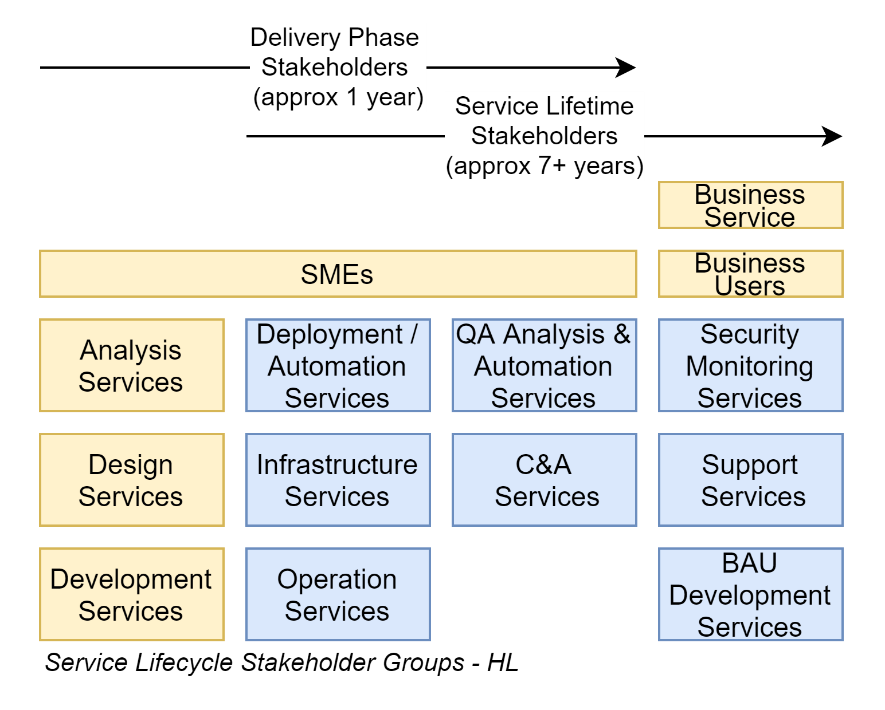
### Process

Large organisations have different departments to provide qualified input to the CAB’s summarised recommendation and endorsement to the CDO’s decision as to whether to provide a service the Authority to Operate.

When a Project Manager believes that all the CABs stakeholders have received their expected deliverables, he requests the project architect to align a meeting with the Change Authority Board (CAB).

Upon successful acceptance by the CAB, a Memo is issued confirming by email to the project manager that production environment RFCs can be raised.

### CAB Members – Governance & full Lifecycle Stakeholders



#### Design Services

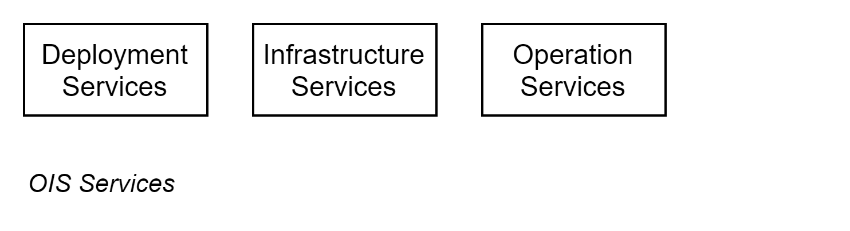
The Design Services provided project architect reports to CAB that the solution’s design meets enterprise obligations. Namely:

* The project’s Architect(s) develop an architecture that meets the multiple stakeholders needs and document them in a Solution Architecture Description (SAD).
* A Summary of the Solution Architecture Description, covering the project’s architecturally significant points is presented to the Technical Working Group (TWG).
* Endorsement of the design of the Stored data and Messages from the Data and Information Group (DIDG).

The Design Services will report to CAB that they have reviewed the services’ technical systems deliverables and design and concur that they received endorsement due to following international design and development standards, trade best practices, and both sector and organisation design principles.

The project architect is also called on to endorse that the system’s implementation aligns with the endorsed design.

#### Operations and Infrastructure Services



Operations & Infrastructure Services (OIA) will report to CAB that have been provided the automation – or failing that, documentation – for the project to be deployed and managed by the organisation’s OIA specialists for its whole service lifetime (measured in years) without requiring assistance or communication with the original development team.

OIA will report whether they have received a System Support Plan (SSP) (or equivalent electronic project wiki based deliverable) deliverable from the project team that describes how to run the automation, or failing that manually perform the infrastructure provisioning, system deployment, system configuration.

##### Deployment Services

If the service is not a SaaS, but a PaaS, IaaS or VM based system, deploying the service to real or virtual local or cloud infrastructure or platforms will be the responsibility of a deployment automation specialist provided by OIS.

Their requirements for accepting to do so are outlined in their departments DevOps Guidelines document, with the following being key objectives to lowering long term risk:

* The delivery of a cloud hosted Continuous Build & Deployment (CB/CD) Pipeline that encode the idempotent deployment process to both NON-PROD-DATA (BT, DT, ST, UT, IT, etc.) and PROD-DATA (PROD) environments, whether they are new or already existing.
* the hand-over of a cloud-hosted Application Lifecycle Management (ALM) Service that triggers the above CD pipeline.
* access by the whole OIA team to the Production Wiki within the ALM, where developers have written instructions on how to run and maintain the deployment pipeline,
* Any necessary deployment instructions are to be developed using Deployment as Code (DaC) instructions to encode steps in a predictable, automated, repeatable manner, reusable long after current personnel have moved on,

##### Infrastructure Services

The devices on which the service will be deployed will be the responsibility of the Infrastructure Specialists to manage and keep running.

Their requirements for accepting to do so are outlined in their departments DevOps Guidelines document, with the following being key objectives to lowering long term risk:

* If the system isn’t a SaaS, but a PaaS, IaaS or VM based system, it is to be deployed to organisation-approved cloud infrastructure, unless agreed to otherwise by themselves, the project’s architect & Technical Working Group (TWG).
* Any necessary infrastructure or platform are to be developed using Infrastructure as Code (IaC) instructions to encode steps in a predictable, automated, repeatable manner, reusable long after current personnel have moved on,

##### Operation Services

Operations Specialists will report to CAB that they have the means to determine that the system installed to infrastructure is operating as expected, so that business specialists can configure the system’s business parameters and assist end users.

Their requirements for accepting to do so are outlined in their departments Operation Configuration Guidelines document, with the following being key objectives to lowering long term risk:

* the system is configured with a configurable rolling diagnostics logging, set to a minimum of 31 days.
* in PROD-DATA environments, the system’s diagnostics data is configured to be transmitted or retrieved by a 3rd party enterprise diagnostics service so that it can be aggregated with other services is so desired for analysis.
* the service to collect metrics to which alerts can be attached in PROD.   
  The most common alerts they will expect to be configured include alerts of:
  + Abnormally high traffic
  + Abnormally high transfer of data bytes
  + Abnormally high transfer of data records
  + Abnormally high levels attempted but denied operations
  + Abnormally high levels of exceptions
* data from systems in environments from ST onwards is automatically regularly and incrementally backed up to a different environment than the service, inaccessible by project personnel, decreasing the risk of erasure of data.
* Note  
  will require the project meeting with the OIS DevOps team to provision an ALM project space, develop a Work Item progress Dashboard.  
  It also implies the project will engage an internal or external infrastructure automation development specialist de develop the necessary Infrastructure as Code, Database Schema as Code, develop the continuous delivery pipeline, the deployment, backup and restoration workflows.

#### Customer Support Services

Support Specialists will report to CAB whether they have been provided a deliverable – an App Support Guide (ASG) -- outlining adequate information for them to provide Level 1 Support to end users.

Level 1 Support is generally not system specific and includes tasks such as the following:

* reset user passwords
* provision the system with users within groups
* knowing whom to contact for further support, whether it be system or business support.

Note:  
This compliance will require the project meeting with client support services, to either prepare an *App Support Guide* (ASG) or agree on an acceptable equivalent (usually an accessible section wiki within the project wiki).

#### System Support Services

System support services will be taking on the responsibility of handing system specific requests that customer services will direct to them.

They will report to CAB whether the system design has delivered the following functionality:

* As per the Privacy Act, informing users of their Privacy, Data Use, Tracking rights, as well as User Responsibilities.
* alerting end users to planned downtime
* reassuring end users by explaining the cause and resolution of unexpected downtime that occurred,
* as per the Privacy Act, alerting all users to security breaches that have occurred
* collecting feedback from users about the service’s qualities, to improve the service,
* reporting to governance boards whether the system is being used more or less over time, informing decisions to further invest or not,
* can restore logically deleted records on behalf of users who inadvertently deleted them.

#### Security Monitoring Services

The Certificate & Assurance (C&A) Specialist engaged by the project will report that a

XXX TODO

* Review the service’s Solution Architecture Description (SAD)’s Security section seeking information to address requirements within:
  + NZISM
  + ISO-27002 (Information Controls)
  + ISO-27017 (Cloud Services)
* Ensure the SAD was endorsed by TWG as using technology and design patterns that are meet expected design qualities,
* Commission either an internal or external Technical Security Review (TSR) of the service to review the deployment is capable and actually:
  + enforcing country-specific embargos,
  + protecting against DoS attacks by firewall, potentially backed by a HA architecture,
  + encrypting all communication channels, whether internal or external to the system,
  + using only short lived (90 day) freely issued Certificates, adhering to current security design standards,
  + implementing OWASP’s recommendations – especially the Top 10 – to protect web services against well-known attack attempts,
  + encrypting all databases so that if they are copied/downloaded they are inaccessible,
  + permanently auditing all operations by end users
  + audit messages are transferred off system to a central SEIMs.
  + secures configuration settings in a secure storage vault to which developers do not have access (only the service account used by the continuous deployment pipeline)
  + automatically, regularly fully & incrementally backs up the data
  + the restoration of the backup is automated and regularly tested
  + has a HA design to decrease down-time,
* has a DR plan in case the system data has been compromised and cannot be restored in a timely manner
* Which will include a review of operations seeking whether:
  + users are removed from the system when they leave the organisation,
  + users roles in the system are only temporary (re)assigned,
* the service as installed in PROD protects against DoS attacks

The development of a security test and report by a 3rd party is arranged by the Certificate & Assurance (C&A) specialist.

#### BAU Development Services

If the service is customizable by code, the organisation’s development services will report to CAB that they have reviewed the service and believe it is maintainable and/or improvable to meet expected needs.

#### Compliance Officer

Whether the system can:

* meet GDPR expectations by permitting user records be made anonymous,
* meet Records Act & Archiving directives by never deleting records from the system (only *logically/state* deleting them),
* meet General Disposal Authority (GDA 6) 8.1.1, 8.1.2. and 8.1.7. obligations to keep system procurement & design documents.
* meet NZWAG obligations by being capable translate system (not media) UX and API text to at least all of the national spoken and read languages of the country,
* meet Privacy Act obligations by obtaining consent from end users regarding tracking cookies, data use retention & sharing, and providing information on how to correct personal identifiable information held in the system
* meet the Official Information Act obligations by providing a means one or more of the following in a format that can be subsequently blacked out, or imported into software where certain information may be replaced with blackout characters:
  + reporting on all messages back and forth between two parties,
  + the records accessed by the person
  + the current and projected trends as to use of the system

Note:  
This required skillset implies the project Compliance verification requires the project to engage an internal C&A Specialist to coordinate the verification of the above as part of their C&A process.

#### Certification and Assurance (C&A) Services

The Certificate & Assurance (C&A) Service will report to CAB that they have performed a Security Risk Assessment (SRA)[[7]](#footnote-8) exercise, from which they developed a Control Validation Plan (CVP) which was followed and audited via a Control Validation Audit (CVA), and the residual risk accepted by the business owner, and the SRA was updated to reflect the new current risk profile.

#### Quality Assurance Services

The testing services will report to CAB that:

1. they been provided access to a NON-PROD-DATA system where they have run tests to ensure the system meets ISO-25010 qualities, and the data the system provides meets ISO-25012 qualities.
2. They have the means to run these tests again in the future, to ensure that changes and new deployments do not break existing functionality.

This is reported using a Test Summary Report (TSR).

Whereas Testing has traditionally been done manually, current service deployment expects the TSR to be automatically generated by automated tests run in the pipeline.

Note:  
This required skillset implies the project would do best to include an internal or external test automation specialist to convert test analyst scripts, developed by test analysts earlier, to automation. Note that a test automation’s skillset is generally distinct from the skillset for a general or system full-stack developer.

# Deliverables and Sequencing

## Objective

As a recap, the objective is for a project manager to be able to issue an Request for Change (RFC) that will eventuate in a system being deployed to a Production data environment.

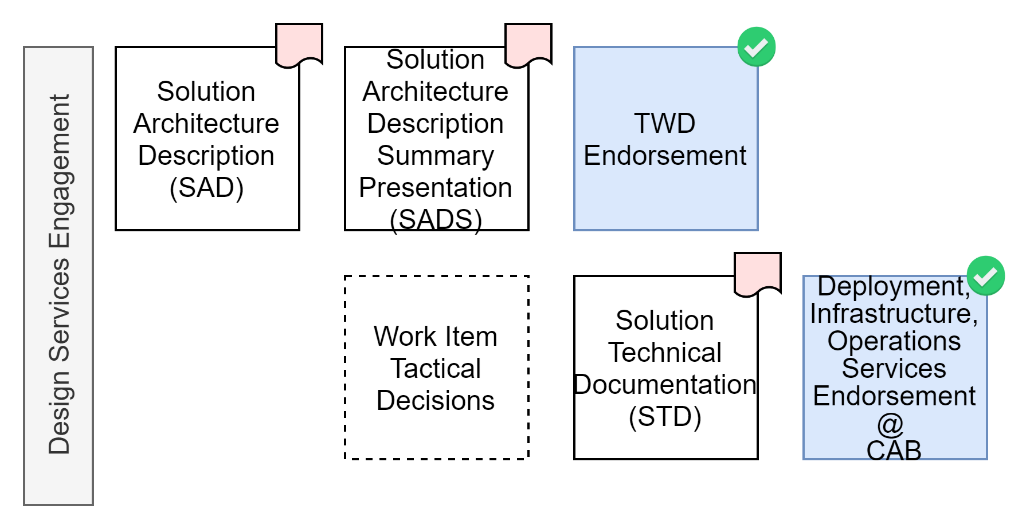
For such an RFC to not be denied, the service must have received an Authority to Operate (ATO) from the Chief Digital Officer (CDO), upon advice from the Change Advisory Board (CAB) that the project’s service has a Privacy Officer endorsed Data Categorisation, the project and its service has participated in a satisfactory Certification & Assurance (C&A) process, the service has passed a QA inspection, and CAB board members have received the deliverables they have expected.

## Scheduling

Many of the expected processes the processes to develop expected deliverables take considerable time and should be started as early as practical.

## Design Services Engagement

Project managers are advised to engage the ITC Strategy Planning Architecture (SPA) services early so that they can develop a valuable design that reduces the risk of failure of meeting expectations of stakeholders.



### Solution Architecture Description (SAD) Deliverable

The project’s assigned Solution Architect (SA) interacts with the project’s Stakeholder Analyst and develops an architecture that meets the multiple stakeholder objectives, while meeting the organisation’s obligations, and documents it in a Solution Architecture Description (SAD), according to ISO-42010 (Complex Models defined as Views) and ISO-19505 (UML) standards.

SADs are complex documents taking into account multiple stakeholder group viewpoints.

### Solution Architecture Description Summary (SADS) Deliverable

A Solution Architecture Description Summary (SADS), covering the project’s architecturally significant points is presented to the Technical Working Group (TWG) for endorsement.

TWG is interested in architecturally significant features of the project, so should not delve into every detail.

### Data and Information Design Group (DIDG) Endorsement

The system’s design of its messages and stored data requires review and endorsement by the DIDG.

DIDG is interested in ensuring that data interchange between systems adheres to common standards where applicable, to reduce the cost of system integration.

### Technical Working Group (TWG) Endorsement

TWG will first ensure the project has previously received Design Authority (DA) endorsement, then DIDG endorsement, then verify the presented SADS that the design meets legal, regulatory, and guiding principle obligations.

This endorsement from TWG will be required later by the Change Advisory Board (CAB).

### Technical Documentation (STD) Deliverables

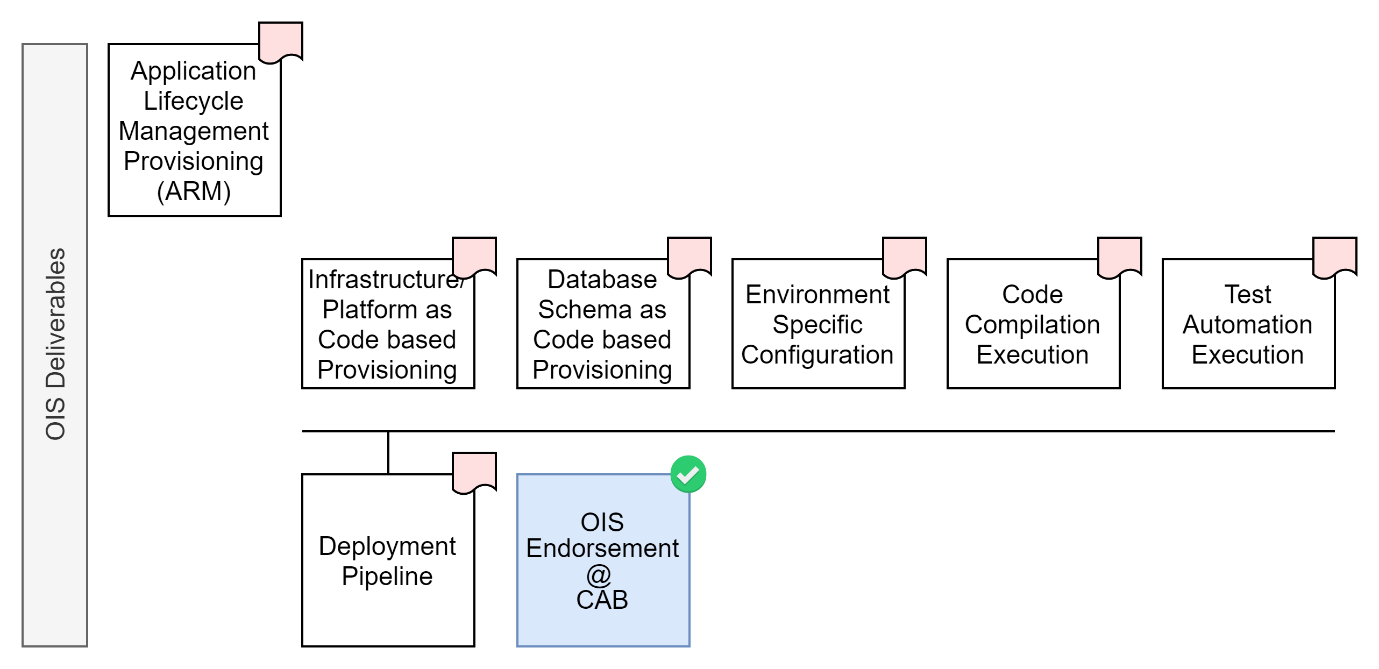
The solution architect (SA) is retained to provide tactical decision guidance throughout the project, which is documented in the project’s Work Items and Technical Wiki (i.e., in the Project’s ALM User Stories, pointing to further information within the ALM based technical version controlled Wiki).

The work items and technical documentation will be an deliverable artefact that will be reviewed for completeness, to obtain endorsement from OIS stakeholders before CAB.

Tip: Do not leave technical documentation to the end as it will be generally too thin to be of value, and therefore acceptable by the OIA services.

Tip: Periodically schedule maintenance of the documentation to refresh material and remove retired information.

## Deployment, Infrastructure and Operations Services Engagement



There is logic to engaging the Deployment, Operations, Infrastructure, Services (OIS) earlier than development services, to employ their capabilities to configure an ALM based project management space, pipelines, etc.

### Application Lifecycle Management (ALM) Deliverable

The DevOps specialists within OIS will develop a configured project specific ALM, containing the work item management service, technical wiki documentation service, code repository service, automation pipeline services that are dependencies for other deliverables.

A key deliverable will be the Work Item Service with a summary dashboard that can communicate to stakeholders the amount of work still desired, the velocity at which it is progressing, the quality, error and rework rate, and therefore the estimated delivery date.

### Idempotent Infrastructure Environment Provisioning

A key deliverable from the team is the ability to develop environments from scratch, in an idempotent manner.

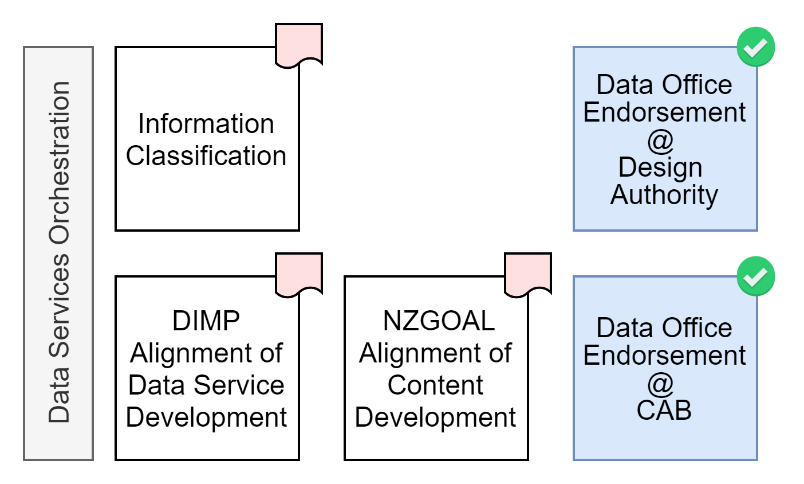
Modern infrastructure provisioning can only be achieved by relying on Infrastructure/Platform as Code approach.

### Idempotent Data Management Automation Deliverable

A key deliverable from the OIA team is the development of an idempotent solution to incrementally and fully backup data regularly and the capability to restore it on demand via automation.

Modern data management can only be successfully achieved by relying on automation.

## Data Services Engagement



Some of the following tasks can be undertaken by the project architect – but it is practical to engage a Certification and Assurance (C&A) Specialist as soon as practical to coordinate the delivery of the following deliverables:

### Information Classification Deliverable

The service’s Information Classification is determined at the start of a project – generally when the business case is being developed.

Fill in the [MinEdu Information classification template.docx[[8]](#footnote-9)](https://docs.moe.govt.nz/navigator/bookmark.jsp?desktop=MinistryDocuments&repositoryId=FNMinistryDocuments&repositoryType=p8&docid=DMOE%2C%7B1C5A444A-9678-4E41-96C4-A8365566408A%7D%2C%7B6777B926-EE01-C16D-84A0-78A90B700000%7D&mimeType=application%2Fvnd.openxmlformats-officedocument.wordprocessingml.document&template_name=DMOE&version=released&vsId=%7B7B550A52-DAD9-4AAB-8C72-4F220C3AB231%7D)  to determines whether the service’s data is UNCLASSIFIED, IN-CONFIDENCE, or SENSITIVE[[9]](#footnote-10), and ensure it is endorsed and signed by the *Chief Data Steward[[10]](#footnote-11)*.

Most systems will be classified as IN-CONFIDENCE rather than SENSITIVE.  
The classification will dictate the NZISM controls that are obligated, in turn informing the development of the architecture, SAD, SADS, tasks, and therefore costs.

### Data Information Management Principles (DIMP) Alignment Deliverable

Per cabinet decree the information managed by NZ Government systems must align to DIMP principles wherever it does not contravene Information Classification and Privacy Act obligations.

The Data Services will require filing of evidence the above is a driving design decisions.

### NZ Government Open Access & Licensing (NZGOAL) Alignment Deliverable

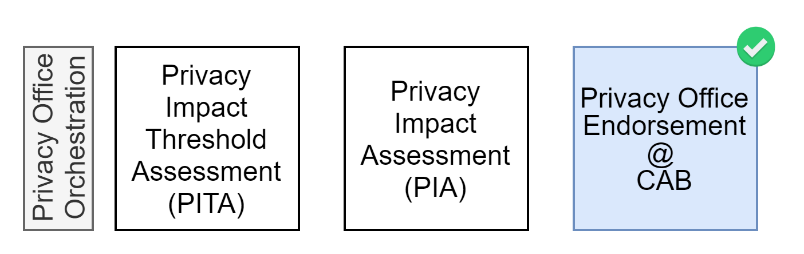
System information is often comprised of records about people, objectives, and their actions to achieve them.

But many systems require the development of media.

Media content that is commissioned or developed by a government must be, where possible, free to use or recombine in full or partial, share, and made available under a Creative Commons license.

Although conceptually related, copyright does not equate to or supersede cultural rights. Culturally owned artifacts and their digital reproductions – which are understood to be as culturally important as the original -- may only be temporarily and conditionally lent. Practically, in a digital system, this translates to ensuring specific terms & conditions are accepted, as well as limiting requests for the media from NZ only, before granting access.

## Privacy Office Engagement



### Privacy Threshold Assessment (PTA)

Often at the same time as the Information Classification is being determined, a Privacy Threshold Assessment (PTA) exercise is run, using a spreadsheet available here:

* https://bit.ly/3B1zz3x.

The PTA score dictates (which it almost always does) whether a more in-depth Privacy Impact Assessment (PIA) exercise is also performed.

The score requires the Privacy Officer’s signoff.

### The Privacy Threshold Assessment (PTA)

The PTA i

* Security Risk Assessment (SRA)
* Technical Risk Assessment (TRA)
* Certification & Acceptance (C&A Memo)

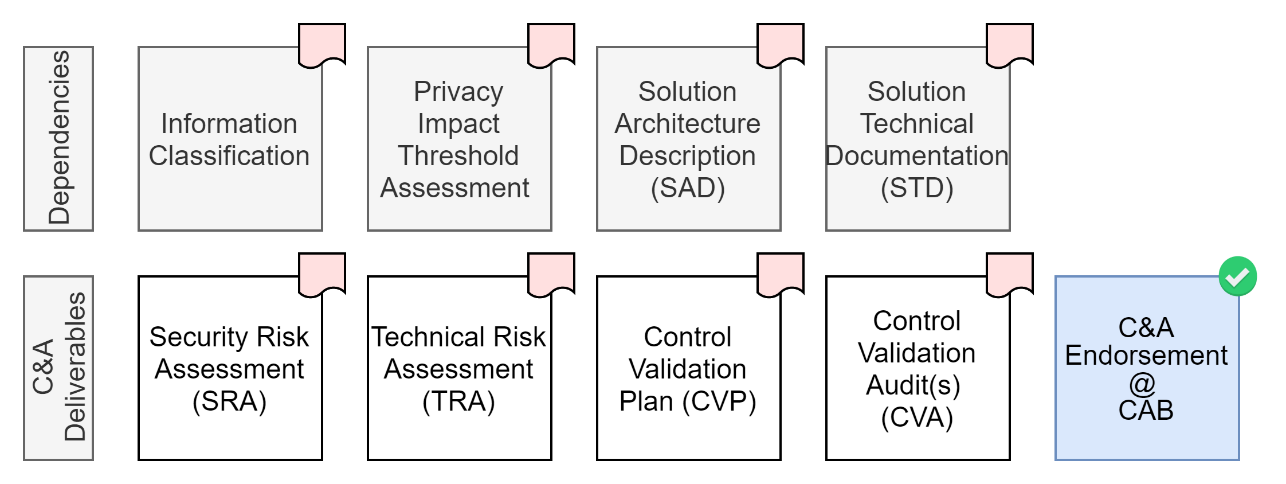
As a government agency delivered service used by a work staff of over 50,000, even our simplest systems handle a vast amount of PII – hence it is very easy to pass the minimum score that indicates a more full PIA is required.

### Privacy Impact Assessment (PIA)

For applications that manage information of high risk to end users or the ministry, the PTA will indicate that full PIA will be required.

This process can take months, so if indicated by the PTA, should be started sooner than later.

## Certification & Assurance (C&A) Services Engagement



### Scheduling

Delivery Managers are advised to engage the services of a C&A Specialist early – during the biz case. If that opportunity is unavailable or missed, the C&A Specialist should be engaged soon after procurement, influencing the manager’s understanding of procedural risks, and influencing the architect’s understanding of technical Risks.

The C&A process is an ongoing one as it is not a one-off technical analysis of a system -- that’s more the role of the TSA task -- but of ongoing and evolving system and project technical and procedural risks.

### Security Risk Assessment (SRA)

The C&A specialist develops Security Risk Assessment (SRA) soon after procurement has decided on an acceptable proposal. Even earlier -- before contracts are signed – would be best, so the Certificate & Assurance (C&A)’s specialist’s analysis can influence the procurement selection process if need be. If only started after procurement has completed, at least the SRA influences behaviour and processes.

Either way -- whether the SRA is done during or just after procurement – an SRA is done much earlier than when a system is actually up and running and available to test. This is important to notice as an SRA is looking at *whole*-process risks, including people, processes and environments – not just the service system itself.

For example, a system may be technically secure, but if developers, test analysts and stakeholder analysts have direct access to production data, the development processes cannot be deemed secure (any one of these resources have access to high value production data).

Other classic examples are a service having no Disaster Recovery (DR) or Business Continuity (BC) planning in place in case the system needs to be rebuilt from scratch, or the service is offline for a considerable amount of time (e.g.: in an earthquake).

### Technical Risk Assessment (TRA)

When a system does become available for testing –months after procurement has completed -- the Certificate & Assurance (C&A) specialist will employ an independent 3rd party specialist to assess[[11]](#footnote-12) the system in a deployed environment.

The cost of external Technical Risk Assessments is not trivial. Experienced managers pre-allocated sufficient budget for it[[12]](#footnote-13).

The completed TSA will list risks due to discovered technical design or implementation issues with the system or environment in which it is deployed.

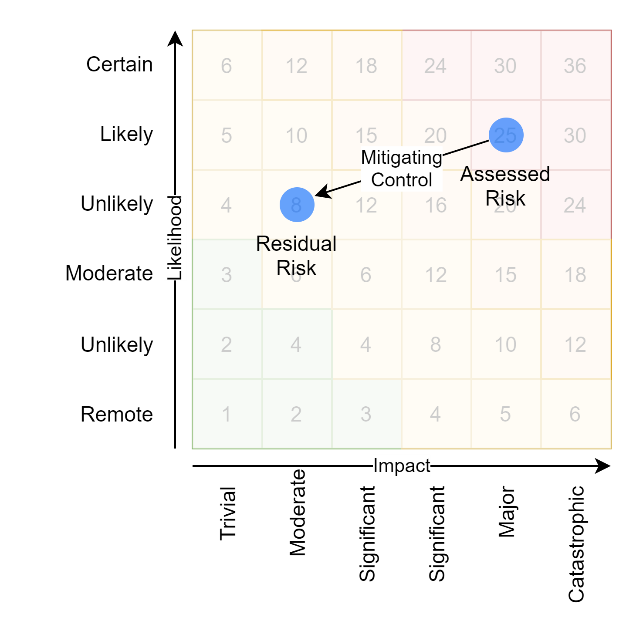
The TSA will also include recommendations on how best to address the technical issues found, which will be incorporated into the Risk Mitigation Plan which the Certificate & Assurance (C&A) specialist will prepare next.

### Risk Mitigation

It is wise to adhere to policy reflecting current best practices specific that systems should not be permitted to go live with any high-level risks, or any medium risks.

Hence SRA and TRAs will be include recommendations on how to reduce the impact and/or likelihood of any people, procedural, environment or system risks.

Project managers schedule effort to mitigate the procedural and/or technical risks according to the recommendations made by the Q&A specialist.

[[13]](#footnote-14)

#### Control Validation Plan (CVP)

In addition to making recommendations on how to mitigate the risks, the Certificate & Assurance (C&A) specialist will also prepare a plan to be used in the future to validate[[14]](#footnote-15) the controls have been implemented as planned.

##### Procedural Risks Controls

Common procedural risks mitigations that projects will spend effort on include examples such as the following:

* Analysts, Developers, Testers will develop a small subset of test data representing production data cases to allow work to progress without accessing production data, whether cleartext or obfuscated, full or partial.
* A automated deployment pipeline will be developed, whether it be used to deploy a whole service, or just the configuration of the service.
* the project will add to its deliverables the completion of DR/BC planning, hopefully completely automated.

##### Technical Risk Controls

For systems that are being developed by the organisation, these technical risk mitigation recommendations can be enforced, closing the outlined technical and or maintenance weaknesses.

On the other hand, non-compliant *procured* services (e.g.: SaaS) over which the organisation has no direct influence will require other forms of controls – e.g.: work processes -- being developed as work arounds to lower and/or mitigate the non-compliance risks.

### Residual Risk

Not all the recommended controls will successfully be implementable, or mitigate all risks completely, leaving some – even potentially uncomfortable -- residual risk.

### Control Validation Plan (CVP) Deliverable

The Control Validation Plan (CVP) is prepared by the C&A Specialist, summarizing the Procedural and Technical Risks that require mitigation.

The CVP also outlines the method in which they will be tested.

### Control Validation Audit (CVA) Deliverable

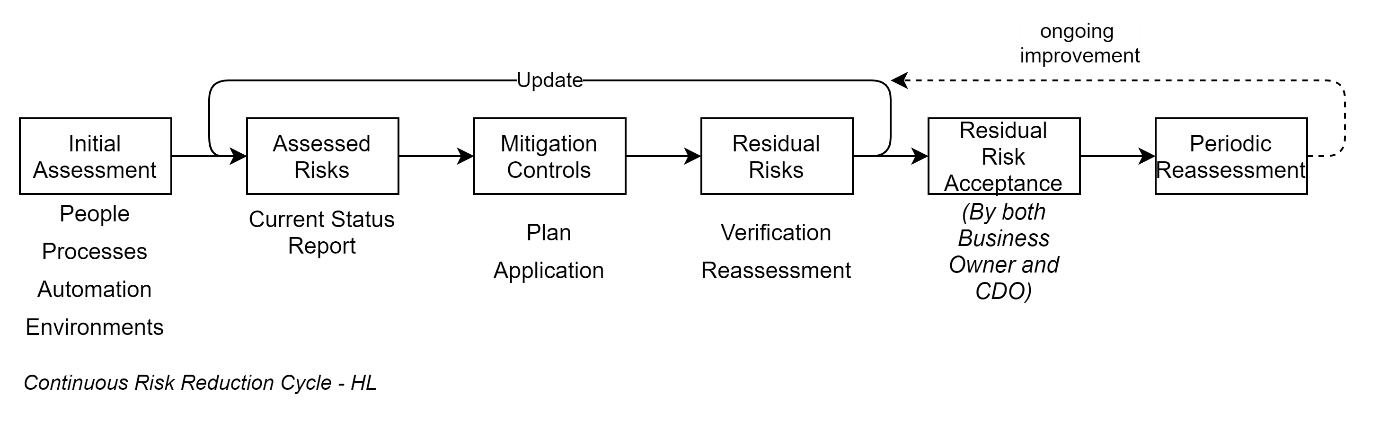
TODO

and the residual risk accepted by the business owner, and the SRA was updated to reflect the new current risk profile.

### Control Validation Audit (CVA) (“Trust – but verify”)

When the project team has implemented the SRA/TRA’s recommendations and believes it has no more high or medium ranked risks, the Certificate & Assurance (C&A) specialist is invited to audit the changes.

When the Certificate & Assurance (C&A) specialist has completed the audit, the Security Risk Assessment (SRA) for the service is updated to reflect the new current state.



Almost all services, whether procured or developed in house will be non-compliant to some extent.

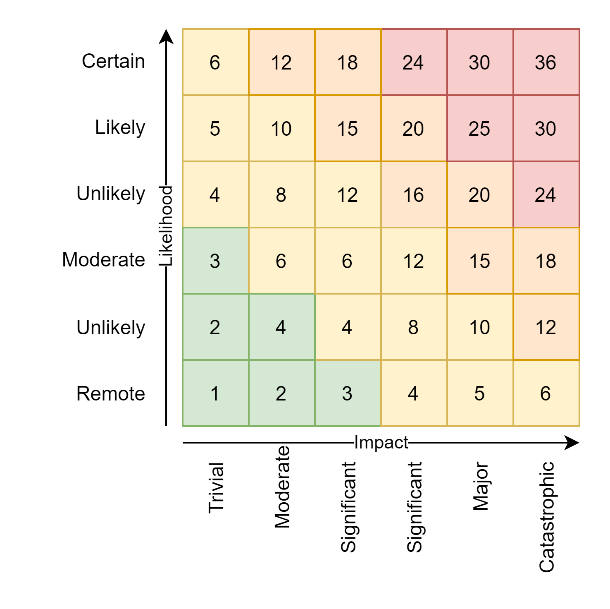
The inherent risk may be due to development processes used, or technical limitations of the system due to non-compliance to national laws, regulations, obligations, technical limitations, design or security weaknesses.

Simple common examples of this condition may include one or more of the following:

* the procured SaaS has no capability to adhere to national embargo laws limiting requests from certain countries (e.g.: North Korea),
* the procured service has no capability to adhere to national privacy laws as it does provide an in-system notification service to notify all users that a security breach has occurred,
* the procured service has no capability to adhere to the Official Information Act, as it has no functionality to collect all information requested via an OIA Request,
* the procured service does not have capabilities recommended in NZISM. For example, users are assigned system roles for an indefinite duration, and there is no automated mechanism to remove users once they leave the organisation,
* the system does not have the capability of being integrated with the organisation’s preferred Identity Provider (IdP) Service,
* the analysis, design & development service personnel all have access to test data that is developed from restored production data,
* the analysis, design & development service personnel have relative ease accessing the credentials used for environments where the above stale production data is being used,
* the analysis, design & development service personnel are sharing infrastructure credentials by Slack, Teams, Email -- all accessible remotely in an unaudited manner.

### Risk Categorisation

The Risks uncovered by the SRA or the TRA will be scaled by each risk’s Impact and its Likelihood of occurring, according to the Enterprise Risk Management Framework (https://bit.ly/3kgqMoE):

[[15]](#footnote-16)

### Risk Acceptance

This residual risk will be summarised by the Certificate & Assurance (C&A) specialist for acceptance by the business owner.

Acceptance by a business owner does not guarantee that a service will be able to deployed. A service still requires CAB endorsement in order to obtain an Authority to Operate by the Chief Digital Officer.   
Irrespective of a business owner’s acceptance of the risks, if the CDO is advised by CAB that the service poses too high a risk to the whole organisation the service will not receive an ATO till the organisation impacting risks are sufficiently mitigated.

## Quality Assurance (QA) Services

Projects decrease their risk of non-delivery to expectations by engaging QA Services early – before the development Services.

This is so that QA Specialists can add value to Stakeholder Analyst Services by completing their Tasks with specific Quality Assurance Test definitions before development services strive to meet these defined objectives.

### Test Definition Reports Deliverables

QA Specialists develop their Test Definitions within the project ALM suite’s WorkItems.

They work with the OIS team to develop reports that can show governance

* How many work items have associated tasks and tests,
* How many tests have been converted to automation,
* How many tests are passing,
* What ISO-25010 qualities are demonstrated by automated testing.

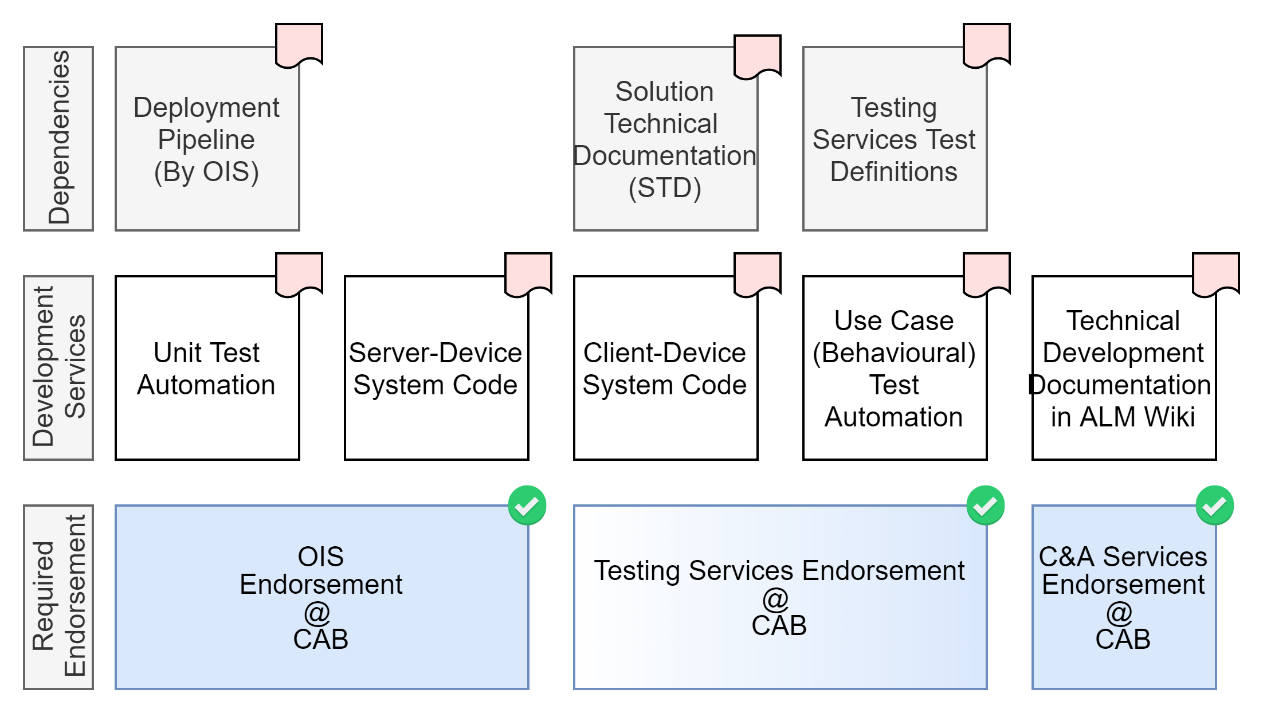
This deliverable is required in order for test services to report to the CAB that the software has enough automated testing to be alerted to failure due to changes in the future.

### Testing Summary Report (TSR)

CAB will require a TSR having been developed by the Testing Team, from the automated pipeline tests.

The TSR covers the ISO-25010 Qualities, demonstrating that the service is accessible, performant, usable, supportable, maintainable, improvable, while meeting obligations.

## Development Services Engagement



### Automation

A key risk to projects is thinking the information service intended for use by end users is the first and only form of automation that is expected. It is not -- it’s the last.

IT is the encoding as automation the tasks of as many stakeholders group as necessary to remove the dependency on the original development team’s personnel, so that the service can continue to be maintained and enhanced successfully long after the original development team members have moved on.

If the product is not a SaaS – which often are not customizable and therefore do not require development services -- Project Managers are advised to hold on bringing development services on board until OIS services has configured an ALM, has a repeatable means of developing secure environments on demand, and has a prototypical means of demonstrating QA using automation.

Although all eyes are on the delivery of the information service’s desired business functionality, it is up to the project manager to inform stakeholders as to why this is deferred until prototypical automation and QA foundations has been developed first.

### Unit Tests Suite Deliverable

Unit Tests provide Maintainability, enabling both Operations and BAU Development Services to endorse the service at CAB.

This test suite deliverable is distinct from any other deliverable, and will go a long way towards enabling BAU Development Services to endorse the service at the CAB.

### Use Case Tests Deliverable

Use Case Test Automation automate the logic of Test Analysts, enabling Testing Services to endorse the service at CAB.

This test suite deliverable is distinct from any other deliverable, and will go a long way towards enabling Testing Services to endorse the service at the CAB.

### System-Device Server Code Deliverable

The service provides

This deliverable is what the client system will be accessing. Test analysts will generally be developing tests against the Client-Device System described below.

### Client-Device System Code Deliverable

If procurement and/or the architect has defined a system that adheres to current Design Guidelines, it will be a Server/Client based architecture, following “API First” design guidelines. In such cases, the interface used by end users is \*not\* webpages developed on the server-device, but a separate client-device based system dedicated to consuming the service’s APIs and making them accessible.

Contrary to the common terminology used in the industry, managers -- when delivering modern server/client based systems -- are not responsible for delivering a single webserver service, but two distinct deliverables – the server-device system, and the client-device system – and should plan accordingly.

This deliverable is what test analysts will be writing test scripts to test, which will be executed by the build, deployment & test pipeline.

### Environment Configuration Automation Deliverable

In poor security environments, developers are also assigned the task of configuring environments.

This is to be avoided at all cost, leaving environment configuration to automation, developed by the OIS DevOps team.

In government service development environments this is considered a high risk due to multiple factors:

Constantly rotation of contractors with unmonitored and unaudited access to configuration data, providing ongoing complete access to information data even after leaving the organisation

When combined with the poor security legacy practice of using full or partial production data for testing purposes, this risk is even higher (it’s almost a Certainty).

In legacy environments, configuration is applied by hand, according to deployment instructions. Current best practice is to develop a configuration step or full pipeline to apply configuration, configured per environment.

Automated configuration pipelines ensure that developers don’t do it by hand, and most importantly, ensure that they don’t have access to key information that compromises the whole system.

### Development Documentation

Even with the best of design planning, the spread between the plan and execution can only be reduced – never eliminated completely.

Hence documentation of what has been really developed is required by support specialists who will be maintaining the system in different environments for many years afterwards.

It is a continuous practice to keep the documentation up to date, generally in a Application Lifecycle Management (ALM) Wiki.

At first, the documentation is about manual processes – but as the project matures, documentation should quickly move on to describing the development and running of *automation* of those manual processes.

## Change Advisory Board

## Production Environment Go-Live Request for Change (RFC)

Once CAB has notified the manager that the service has received the Authority to Operate, the manager can raise RFCs.

All RFCs raise automated workflow processes comprised of multiple steps.

All Production Environment RFC workflows have an initial step requiring a Change & Transition representative’s oversight and verification that this RFC’s system has already obtained an Authority to Operate (ATO).

Once that above verification step is completed, the workflow moves on to then instruct an implementor in the Operations & Infrastructure (OIA) Team to deploy the service to the target production environment.

If a Service Pipeline has been built the only operation the OIA specialist will actually do is either Initiate a new deployment pipeline operation, or simply Approve a confirmation step in a workflow already started previously (e.g.: by a production team member).

# Appendices

## Glossary

#### 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:

the Business Owner accepts the risks on behalf of their business unit,

the Accrediting Authority (i.e., the CDO) accepts the risks on behalf of the Ministry.

Note: For the ministry the certification sign-off is combined with the accreditation as part of the Certification & Assurance (C&A) Memo.

#### ASG

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

#### ATO

*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

*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 Certificate & Assurance (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 Certificate & Assurance (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.

#### CAB

*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.

#### CDO

Chief Digital Officer, who issues the Authority to Operate (ATO) to a system, based on the recommendation of the Change Advisory Board (CAB).

#### CVA

*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.

#### CVP

*Control Validation Plan*: identifies the key 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.

#### Environment

A name, isolated virtual or physical space where a system is deployed and is securely accessible by end users.

#### PIA

Privacy Impact Assessment: a more complete privacy impact assessment.

#### PTA

*Privacy Threshold Assessment:* completed by the project team and forwarded to the Ministry’s Privacy team. 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.

#### RRA

*Residual risk assessment*: (replaced by SRA/CVP/CVA).

#### SRA

*Security Risk Assessment*: during the design phase, the Security Consultant identifies and assesses the cyber security concerns based on a number of 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 Ministry’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.

#### SRMP

*Security Risk Management Plan:* identifies any remedial activities required to address control deficiencies found during the CVA & TSA.

#### STA

*System Threshold Analysis:* a document prepared by a Security Specialist during the Certificate & Assurance (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 off on in the Certificate & Assurance (C&A) process.

The template is available here: <https://bit.ly/2TbwzAM>

#### SRA

Security Risk Assessment:

#### SRMP

Security Risk Management Plan:

#### System

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

#### TSA

*Technical Security Assessment:* 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 of the following: design review, System Pen Test, configuration review, network scanning, & vulnerability assessments. TSAs are mostly performed by 3rd party Security vendors.

#### TSR

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

#### UI

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

#### UX

*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.

## Ministry Deliverable/Tools Resource Templates

The following are the URLs to available Delivery Templates and/or Instructions.

Note:   
The URLs provided may change. It is up to you to ask their owners whether there are later versions to consider, or whether their objective is now managed by a different document template all together.

### SSP Template:

The following is the URL to the SSP template used by Certificate & Assurance (C&A) Specialists to develop a plan to mitigate the risks with implementable manual or automated controls: <https://bit.ly/3ejX12e>

### Application Support Guide (ASG) Template

The following is the link to the template for the minimum information expected by the OIS team: <https://bit.ly/3B4nF9j>

The template handles legacy system deliveries as well as current ones – hence it’s terminology not being especially appropriate to either delivery.

Current best practices is to develop living – but curated and managed -- documentation in a Wiki to which the necessary stakeholders have access, and providing that URL to them, and getting their approval that they have reviewed the Wiki and it contains sufficient information for the OIS team to do their job supporting your project.

### SLA Template

The following is the URL to the template used to agree on the Service Level Agreements which the BAU support teams will adhere to: <https://bit.ly/2VKiPhl>

## Documentation Deliverables

The documentation CAB members are expecting include:

### Application Support Plan (ASP)

The OIS Team is expecting complete documentation that includes:

* How to Create Target Environments
* How to Create Deployable Packages
* How to Configure Deployed Packages
* How to regularly Backup and Test System Data Restoration operations.
* How to Recreate an Environment and redeploy and configure a services packages in case of a Disaster Recovery (DR) operation.
* How to Configure Monitoring from an Organisation provided SIEM service
* How to Configure exporting to the Data warehouse.

### System Support Plan (SSP)

The Customer Support Team is expecting correct and complete documentation that includes:

* How to instruct users -- or perform on their behalf – simple system tasks (eg: reset passwords)
* How and to whom to pass on Business specific requests.

### Business Support Plan (BSP)

The Business Unit will be expecting correct and complete documentation to instruct users – or do on their behalf – to perform changes to system business records, change permissions and roles, personal profiles, manage issues and user feature desires, etc.

### Monitoring Support Plan

Monitoring specialists will expect instruction on what metrics the system produces that they can monitor. This

## Security

Security is determined by CAB being provided by a project representative (e.g. the project manager) evidence from the Certification and Acceptance (C&A) group that Security is acceptable.

This involves:

* ensuring the system’s Information Classification has been determined,
* a PTA (and maybe PIR) exercise has been run and signed off by the Privacy Officer,
* an Security Risk Assessment (SRA) exercise has been run by a Security Specialist for the project, and kept updated as the project progressed,
* a Technical Security Assessment (TSA) – involving a Pen Test -- has been run internally or externally by an independent certified 3rd party organisation,
* a Control Validation Plan (CVP) has been developed by a Security Specialist,
* a Control Validation Audit (CVA) has been run by a Security Specialist, to show the CVP has been implemented.

If all the above have been completed (at cost to the project), the project is issued a Certificate & Assurance (C&A) Memo that has been signed by:

* a representative of the certified 3rd party security checking organisation
* this organisation’s C&A officer, before it is circulated[[16]](#footnote-17) for signature by:
* the head of Certificate & Assurance (C&A),
* the CDO, and finally,
* the DepSec or a delegate thereof.

The project representative proceeds with submitting the project to CAB for approval.

## Integrations

### Digital Identity

Organisation systems are expected to be reliant on an organisation’s approved trusted Identity Services.

### Digital Warehouse

CAB does not have a representative from the organisation’s digital warehouse service on the Board, so this lack of integration usually slips through.

### National Archives

CAB does not have a direct representative ensuring our compliance to our Obligations to Archives as per the Digital Act. This lack of record keeping usually slips through as well.

## Qualities

### Supportability

Supportability is determined by CAB being provided by a project representative (e.g. the project manager) evidence (e.g.: an email) that Support Services are satisfied with the documentation made available for them – generally described within an *Application Support Guide (ASG)*.

### Maintainability

Maintainability is determined by CAB being provided by a project representative (e.g. the project manager) evidence (e.g.: an email) that the Operations & Infrastructure team are satisfied with the documentation made available for them – generally described with a *System Support Processes (SSP)* document, or email pointing them to the project ALM Wiki.

### Functionality

Maintainability is determined by CAB being provided by a project representative (e.g. the project manager) evidence (e.g.: an email) that the Testing Team are satisfied with the documentation they have received and they have been able to develop a *Testing Summary Report (TSR)[[17]](#footnote-18).*

## Quality

The TSR is also used to provide evidence that the following expectations (ISO-25010, ISO-25012 and ISO-25022 are met):

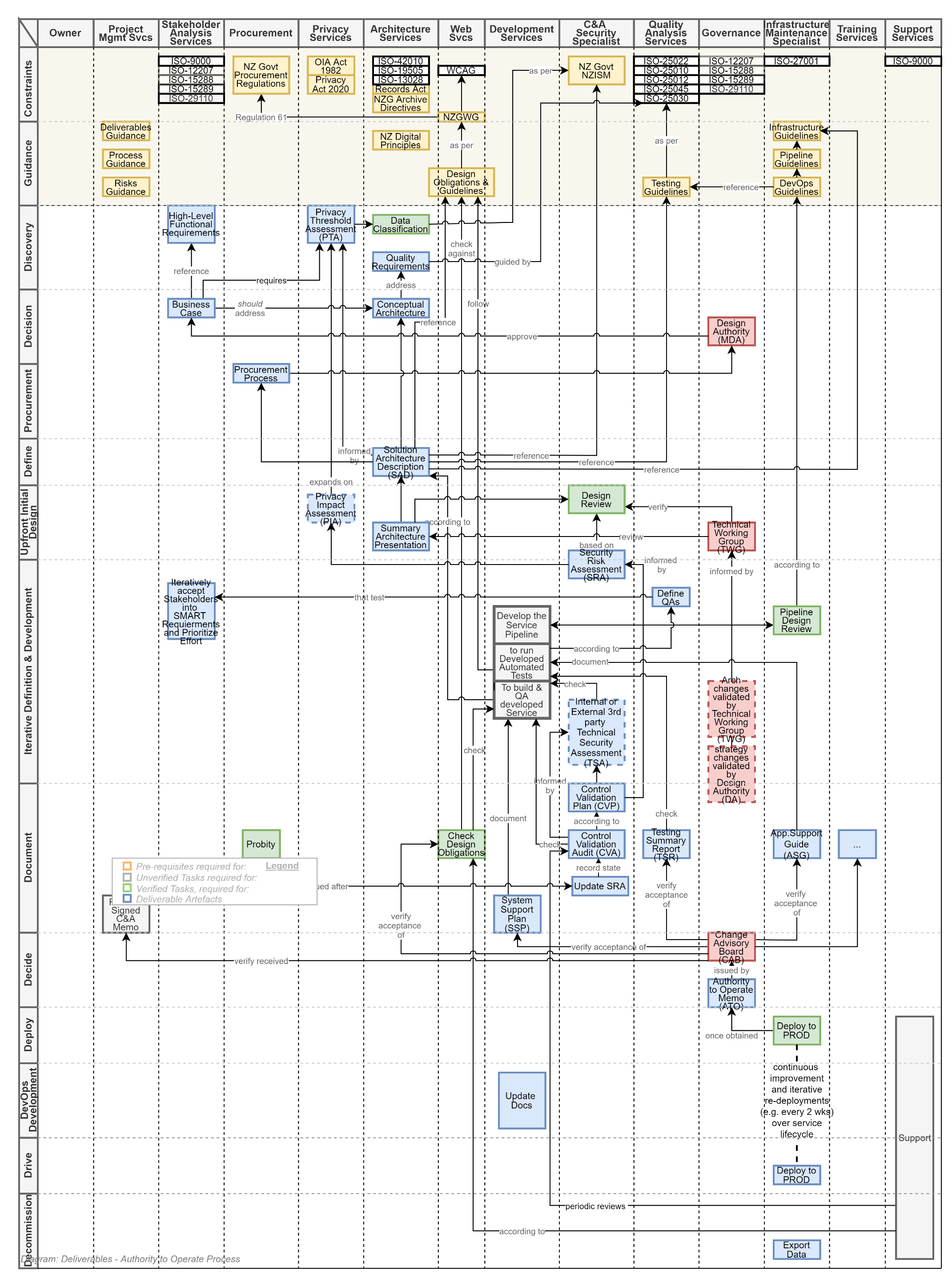
* Performance
* Availability
* Recoverability

Note that ISO based Qualities that TSRs do not account for well include:

* Disaster Recoverability
* Portability
* Reusability

Hence projects should make alternate plans to ensure these expectations are delivered on.

## Authority to Operate Dependencies (A3 Diagram)



1. See: <https://bit.ly/3eypem7> [↑](#footnote-ref-2)
2. https://en.wikipedia.org/wiki/ISO\_9000 [↑](#footnote-ref-3)
3. [↑](#footnote-ref-4)
4. Follow ISO-25010 recommendations to deliver a service that is highly Secure, Functional, Maintainable, Enhanceable, Performant by being designed according to Modular, Demonstrable (ie, Testable), Automated development practices. [↑](#footnote-ref-5)
5. A Security Risk Assessment (SRA) [↑](#footnote-ref-6)
6. A Control Validation Plan (CVP) [↑](#footnote-ref-7)
7. in many cases -- but not all – supported by a Technical Risk Assessment (TRA). [↑](#footnote-ref-8)
8. https://bit.ly/3ktAJ2j [↑](#footnote-ref-9)
9. https://bit.ly/36AztCg [↑](#footnote-ref-10)
10. In 2021, Wendy Hamilton [↑](#footnote-ref-11)
11. A Technical Security Assessment (TSA) [↑](#footnote-ref-12)
12. As a ballpark figure, budget 40K+, up to 100K for medium to higher risk projects. [↑](#footnote-ref-13)
13. Note that this organisation manages risk with a simplified 3x3 matrix: [Enterprise Risk Management Framework (moe.govt.nz)](https://intranet.moe.govt.nz/assets/Organisation/Business-group-documents/EnterpriseRiskManagementFramework2015.pdf) [↑](#footnote-ref-14)
14. the Control Validation Plan (CVP) [↑](#footnote-ref-15)
15. Note that this organisation uses a simplified 3x3 matrix: [Enterprise Risk Management Framework (moe.govt.nz)](https://intranet.moe.govt.nz/assets/Organisation/Business-group-documents/EnterpriseRiskManagementFramework2015.pdf)

    . [↑](#footnote-ref-16)
16. By Sonia [↑](#footnote-ref-17)
17. See Colleen Meads for a template. [↑](#footnote-ref-18)