ICT Project Guidance

New Zealand Government Organisation Obligations, Agreements, Commitments, Standards and Principles

Version: 0.3

Purpose

This document provides a structured overview of the external obligations and expectations that apply to digital services delivered by New Zealand government agencies. It serves to inform project teams, solution architects, and decision-makers of the legal, regulatory, contractual, and principled constraints that must be respected throughout the service lifecycle. The aim is to reduce the risk of avoidable non-compliance by making these constraints visible early in planning, architecture, and delivery processes.

Synopsis

New Zealand government agencies operate within a tightly bounded legal and regulatory environment. This guidance document identifies and explains the obligations, agreements, commitments, standards, and principles that constrain public sector ICT service design and delivery. It highlights areas that require explicit consideration by service providers and delivery teams to ensure that systems are granted Authority to Operate (ATO) and remain lawful, trusted, and effective throughout their service life. Particular attention is given to obligations derived from international treaties, national law, public sector policy, and sector-specific responsibilities, especially in education.

Contents

Purpose and Audience

This document is intended for all individuals involved in the specification, design, development, or approval of ICT-enabled services delivered by or for New Zealand government organisations. It includes those responsible for business ownership, technical design, procurement, quality assurance, change governance, and operational readiness. The document highlights external constraints that are not always visible within individual agency processes but may prevent service approval if left unaddressed.

Scope

The scope of this document includes all information and digital services that are either delivered by, or operated on behalf of, a public sector agency in Aotearoa New Zealand. This includes internal systems, public-facing services, shared platforms, and outsourced components. The document references obligations and expectations derived from statute, regulation, standards, treaties, and commitments—whether binding or non-binding. It also reflects sector-specific constraints in domains such as education, health, and information management.

This guidance does not describe how to design or implement services. Rather, it provides a reference framework of constraints that shape what is considered permissible, appropriate, or mandatory in the New Zealand public sector context.

Introduction

Before any public-facing digital service is launched, it must be evaluated to confirm that it can be responsibly operated and supported over its full intended lifespan. This evaluation requires confidence that the service has been designed with sufficient attention to operational readiness, accountability, and fitness for purpose. It must also be supported by assurance that those responsible for supporting, operating, monitoring, and maintaining the service are properly equipped and informed.

Equally important is confidence that the service complies with all relevant legal, regulatory, and ethical obligations. These may not be visible in business requirements or functional specifications but remain binding nonetheless. They include expectations relating to privacy, security, information integrity, accessibility, archiving, and transparency.

Failure to identify and meet these constraints early in the project lifecycle may result in otherwise functional systems being delayed, reworked, or denied production deployment. This is not a theoretical concern—many such systems are delayed or fail because delivery stakeholders were unaware of obligations outside their day-to-day expertise. This is not a theoretical concern—many otherwise functional systems are delayed, reworked, or abandoned because delivery stakeholders were unaware of obligations outside their

day-to-day expertise. This guidance is intended to prevent that outcome by equipping decision-makers with a high-level overview of what those obligations are, why they matter, and where to find authoritative direction.

Context

very digital service is created and operated within a layered set of intersecting obligations, resembling a set of nested contexts or overlapping domains. These contexts impose constraints not only on the system itself but also on the people and processes involved in its design, delivery, and operation.

At the outermost level are international obligations. These may arise from treaties, conventions, or widely adopted norms and standards such as those issued by the United Nations or the World Trade Organisation. Although not always legally binding, they often underpin and influence national legislation.

Next are national laws. These apply not only to the system as a product but also to the people working on it. From the moment a project is initiated, all contributors—whether public servants, vendors, or contractors—must comply with the laws of the country in which they work. Later, the product itself must comply with the laws of the country in which it is developed, hosted, and ultimately consumed.

Beneath these are sector-specific constraints. These may not be laws in the narrow sense but nonetheless carry serious consequences if breached. For instance, non-compliance with financial sector rules may result in penalties or loss of ability to operate (e.g., failing to meet PCI-DSS requirements for handling card payments).

Closer to the delivery surface are internal organisational policies and standards. These are often overlooked, yet they are essential for achieving interoperability, maintaining trust, and gaining necessary internal approvals.

Additionally, obligations can be distinguished by type. Some are duties, which arise from membership in a broader system (e.g., legal compliance, public record-keeping). Others are responsibilities, which are linked to roles and granted permissions (e.g., data access, operational authority). Duties are owed; responsibilities are undertaken in exchange for specific capabilities.

This layered, role-aware context must be understood from the outset to avoid costly rework and ensure that systems are trustworthy, lawful, and supportable from day one.

Obligation Source and Types

Understanding the source of an obligation is only the beginning. In practice, obligations may be inherited, imposed, or triggered by specific design choices, tools, and deployment decisions. For example, obligations can arise:

- from the underlying components a system uses—such as open-source licences, proprietary APIs, or data services subject to foreign jurisdiction;
- from cross-border hosting and delivery arrangements that must comply with laws in each jurisdiction where the system is developed, served, or consumed;
- from timing and state changes in the system lifecycle, where different obligations apply at design, operation, archival, or decommissioning phases;
- from standards bodies, sector authorities, or professional associations that require minimum performance or assurance levels (e.g. security standards, data retention periods);
- and from the internal policies, standards, or governance models of the organisation sponsoring or approving the service.

These obligations may sometimes conflict or require interpretation. A cloud-hosted system that complies with NZ privacy law may still be subject to foreign government access under foreign law. A service designed for deletion on user request may violate public recordkeeping rules. Navigating these situations requires structured review, cross-disciplinary input, and clear documentation of decisions.

It also requires recognising that not all obligations are attached to the system itself. Some are attached to roles—what a person is allowed to access, or change depends on both what they are authorised to do and how well they uphold their responsibilities. Obligations must therefore be treated as dynamic, context-sensitive, and embedded in both technical and human layers of service delivery.

Legal Obligations

These are the most enforceable obligations and include legislation enacted by Parliament and regulations made under delegated authority. Legal obligations may apply internationally, nationally, or to specific domains such as education or health. They govern matters such as data privacy, recordkeeping, disclosure, and operational transparency.

Regulations and Standards

Some obligations are not primary legislation but are still legally enforceable. These include delegated regulations and formal standards that have legal backing, such as those governing information security or disability access.

Binding Agreements

These include treaties, trade agreements, and other formal international or inter-agency arrangements. Though sometimes distant from daily delivery work, these agreements may impose constraints on technology use, data sharing, or system design choices.

Non-Binding Commitments

Some expectations do not carry legal weight but are politically or culturally significant. These include adherence to international declarations (such as UNDRIP), and national commitments (such as Māori Data Sovereignty principles). These shape public expectations and ethical obligations.

Sectoral and Professional Obligations

Where government agencies operate within defined sectors, they are also subject to obligations imposed by oversight bodies, sectoral regulators, or professional standards. These may include performance thresholds, certification requirements, or data handling protocols.

Organisational Policies and Enterprise Standards

At the most immediate level, obligations also arise from an agency's own governance arrangements, risk tolerance, and internal strategy. These may include enterprise architecture principles, patterns, and technologies, acceptable use policies, or service onboarding checklists. Even if not externally mandated, they often determine whether a service is permitted to operate.

Project and Contract Requirements

While a complete discussion of requirement types, purposes, and formats is beyond the scope of this document, a high-level overview is included here. A more detailed explanation is provided in a separate guidance document.

Requirements are contractual obligations, recommendations, permissions or prohibitions[1] on outcomes. They are defined before, during, and after procurement, and correspond to different phases of the delivery lifecycle. The IIBA's Business Analysis Body of Knowledge (BABOK) remains the industry benchmark for structuring and clarifying requirements. When followed, it helps avoid costly misunderstanding, indecision, and rework across analysis, design, development, deployment, and support.

[1] MUST, SHOULD, MAY, MUST NOT

There are several groupings of requirements, which can be categorised more or less as follows:

- **Pre-RFP**: Business (why the change and service is needed), User (how is the service be used), Quality (how is the service to made available), Capability (what capabilities must the service have), and Transitional (how will the service be delivered).
- **Pre-Procurement**: System Requirements composed of both Functional and Non-Functional Requirements, defining what the system must do and how well.
- **Post-Procurement**: Technical requirements addressing specific technologies, hosting, integration, or operational dependencies.
- **During Development**: Real-world changes, missed considerations, or evolving understanding often result in new work. These take the form of **Work Items**—scoped, prioritised tasks or fixes that must be defined, scheduled, and delivered during the project. Agile methodologies are typically used to manage this emergent workload and absorb late-breaking insights or adjustments without losing project momentum.

An all-too-common error is not knowing about and therefore the distinction between Non-Functional System Requirements (NFRs) and Transitional Requirements. NFRs are Quality requirements that specify acceptable performance, usability, integrity, and reliability standards of the *service*. Transitional requirements, by contrast, govern the *project*—not the service or its underlying system. Transitional requirements often include data migration, access provisioning, media preparation, temporary licences or rentals, communications, and change management – all aspects that cannot be addressed by the system itself or its provider.

Another common – often critical -- error is incorrectly understanding Agile as being a substitute for early planning, using it to jump directly into delivery. This bypasses foundational scoping, sequencing, and clarity, leading to underestimations that in turn produce Missing Valuable Planning (MVP)s.

A mature organisation reuses standardised requirements wherever possible—especially for qualities—and adds project-specific refinements only when necessary to address project specific unique conditions or elevated expectations. ISO 25010, 25012, and 25022 provide useful models for consistent definition and evaluation of Non-Functional Requirements. To proceed without reliance on these standards is to unnecessarily implement incompleteness of thought or planning.

Policies and Principles

Policies and principles are both forms of obligation, but they serve different purposes and respond to different conditions.

Policies

A policy encodes a route through *charted* territory. It is a decision that has already been made based on known conditions, risk appetite, and organisational precedent. Policies define what must be done, how it is to be done, and often in what sequence. Policies are by their very nature fixed.

Policy typically vary organisation and are not treated in depth here.

While policies play an important role in enforcing consistency and compliance, they tend to be rigid, require oversight, and can slow responsiveness. Principles, by contrast, are fewer in number, portable across projects, and allow disparate teams to act with aligned intent without requiring constant coordination or external enforcement. They enable faster, more accountable decision-making under changing or ambiguous conditions, making them especially valuable in complex or evolving delivery environments.

Principles

Principles, unlike policies, are not fixed instructions. They are structured, pre-agreed decision-making frameworks—obligations of thought—that support consistent reasoning when navigating uncertainty or novelty. They exist to guide interpretation and resolve ambiguity, particularly when operating in unfamiliar or evolving circumstances.

Where policies encode settled routes through charted territory, principles offer insight into how to chart new routes when none yet exist. A good principle makes visible the underlying rationale behind decisions, allowing diverse teams to act consistently even when circumstances differ.

For example, a principle like “Services are designed for consumers before operators” does not dictate an exact sequence of tasks but instead clarifies a consistent prioritisation logic. It makes the rationale explicit so that trade-offs and options can be assessed in alignment with shared priorities.

Principles reflect values and priorities. They may be defined at enterprise, programme, or project level and require active application—thinking, not merely following. They are not rules, but structured heuristics, intended to be enduring across project stages, architectures, and personnel turnover.

A common mistake is to treat all principles as one large list. In practice, principles should be few in number (ideally no more than six per domain) and categorised by area of concern. Domains might include Evaluation, Funding, Security, Privacy, Accessibility, Development, Integration, Onboarding, and Operation. Stakeholders should only need to internalise those relevant to their role. For instance, a developer may apply Development and Security principles, while an operator may follow Privacy and Operational principles.

Principles should not be confused with policy, standards, or values. They enable scalable decision-making in novel contexts. A principle like “prefer reversibility over commitment”

does not dictate a design but shapes how trade-offs are framed. A different context—say, an emergency system—may prioritise stability instead.

Principles are a discipline. They demand clarity of thought, consistency of application, and deliberate maintenance. When well-formed, they reduce delay, disagreement, and incoherence during delivery, especially where conditions are complex or change is rapid.

Requirements

While a complete discussion of requirement types, purposes, and formats is beyond the scope of this document, a high-level overview is included here. A more detailed explanation is provided in a separate guidance document.

Requirements are contractual obligations on outcomes. They are defined before, during, and after procurement, and correspond to different phases of the delivery lifecycle. The IIBA's Business Analysis Body of Knowledge (BABOK) remains the industry benchmark for structuring and clarifying requirements. When followed, it helps avoid costly misunderstanding, indecision, and rework across analysis, design, development, deployment, and support. At a minimum, requirements should distinguish between Business, User, System, and Transitional needs—an approach often abbreviated as BUST.

There are several phases in which requirements are developed, which can be grouped more or less as follows:

- **Pre-RFP**: *Business* (why the change and service is needed), *User* (how is the service be used), *Qualities* (how is the service to made available), *Capabilities* (what capabilities must the service have), and [Delivery] *Transitional* (how will the service be delivered).
- **Pre-Procurement**: *System* Requirements, composed of both *Functional* and *Non-Functional* Requirements, defining what the system must do and how well.
- **Post-Procurement**: *Technical* requirements addressing specific standards, technologies, hosting, and integration dependencies.
- **During Development**: Real-world changes, missed considerations, or evolving understanding often result in new work. These take the form of *Work Items*—scoped, prioritised tasks or fixes that must be defined, scheduled, and delivered during the project. Agile methodologies are typically used to manage this emergent workload and absorb late-breaking insights or adjustments without losing project momentum.

A common almost industry wide error is treating Agile as a substitute for early planning, using it to jump directly into delivery. This bypasses foundational scoping, sequencing, and clarity—resulting in Missing Valuable Planning (MVP).

A common error is confusing Non-Functional System Requirements (NFRs) with Transitional ones. NFRs are Quality requirements that specify acceptable performance, usability, integrity, and reliability standards. Transitional requirements, by contrast, govern the project—not the system. These include data migration, access provisioning, media preparation, temporary licences or rentals, communications, and change management.

A mature organisation reuses standardised requirements wherever possible—especially for qualities—and adds project-specific refinements only when necessary to address project specific unique conditions or elevated expectations. ISO 25010, 25012, and 25022 provide useful models for consistent definition and evaluation of Non-Functional Requirements.

Conclusion

Public sector digital services do not operate in isolation. They are embedded within a network of legal, regulatory, professional, and organisational expectations that define what is acceptable, appropriate, and mandatory. These expectations apply not only to systems but also to the people who design, build, procure, operate, and approve them.

This document has outlined the nature and sources of these obligations, explained their practical implications, and introduced key constructs—policies, principles, and requirements—that frame how these obligations are met in practice. Project teams and decision-makers should not treat these matters as compliance afterthoughts. They are essential design inputs that affect architecture, procurement, service operations, and public trust.

Further guidance is available on interpreting and applying these obligations across specific service lifecycles, project stages, or sector domains. While many obligations originate outside individual agencies, responsibility for understanding and fulfilling them rests with those delivering and approving the service. Success depends not just on compliance but on clarity, structure, and intentionality throughout delivery.

Obligations

Besides meeting stakeholder expectations, Services are subject to a collection of Constraints outside of a project’s control, in the form of Obligations, as Regulations, and/or Agreements.

Obligations in Practice (NZ)

Laws

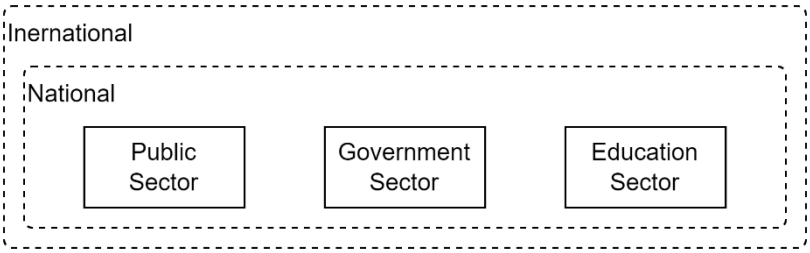

Figure 1: Applicable Legal Contexts

International Legal Obligations

While the laws of other countries are not applicable to this country's citizens and services, some international laws may apply to providers of procured SaaS services used to distribute services.

The following are laws of other countries to note:

- The **Clarifying Lawful Overseas Use of Data Act (CLOUD) Act**[2] is a United States (US) federal law, allowing federal law enforcement to compel U.S.-based technology companies via warrant or subpoena to provide requested data stored on servers regardless of whether the data are stored in the U.S. or on foreign soil.
  Note: Australia, where instances of Azure and AWS and Google Cloud are located, is a CLOUD Act partner of the United States[3][4].
  While New Zealand is not currently a partner, it may consider being one as well[5].

- The **General Data Protection Regulation (GDPR)**[6] is a European Union regulation on information privacy in the European Union (EU) and European Economic Area (EEA). It also governs the transfer of personal data outside the EU and EEA.

> *Note:*
> *Regarding the Right to be Forgotten, the law does not describe how PI data must be erased. The decisive element is that as a result it is no longer possible to discern personal data without disproportionate effort.*

---

[2] CLOUD Act - Wikipedia
[3] Criminal Division | Cloud Act Agreement Between the Governments of the U.S. and Australia (justice.gov)
[4] Australia-US CLOUD Act Agreement (homeaffairs.gov.au)
[5] Privacy Act 2020 | Department of the Prime Minister and Cabinet (DPMC)
[6] General Data Protection Regulation - Wikipedia

> *Additionally, the requirement makes exemptions for Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.*

National Legal Obligations

Whomever provides services within the country is subject to the country's public sector laws and regulations.

In addition to these general baseline laws, services provided by government agencies are subject to additional regulation.

New Zealand Public Sector Legal Obligations

NZ Acts, Laws & Regulations applicable to systems offered within New Zealand:

- **Privacy Act 2020[7]:** including disclosing and getting permission for tracking, data collection purpose, sharing, use and opt-out.

New Zealand Government Sector Legal Obligations

- **Public Records Act 2005[8]:** including limiting physical data deletion and archiving obligations.

- **Official Information Act 1982[9]:** including ensuring transparency to taxpayers via reports cleansed of sensitive personally identifiable information.

New Zealand Education Sector Legal Obligations

In addition to NZ public domain legal obligations, services within the education sector are bound by sector specific regulation:

- **Education and Training Act 2020[10]:** of note, the limitations on using NSNs as cross-system identifiers.

Considerations

- It is a common error to conclude that both GDPR and/or New Zealand Privacy Act prescribes the means of erasure as being physical. However, both regulations are clear that the decisive element is that as a result it is no longer possible to discern personal data without disproportionate effort[11].
  Therefore, the recommended approach is to not delete the data, but reassociate it to an anonymous user or person. This keeps both historical values, without risk to a person, and keeps auditability as to who changed what, when.
  For more in depth analysis of this refer to *IT Project Guidance - On the removal of Personal Information from Systems.*

---

[7] Office of the Privacy Commissioner | Privacy Act 2020 and the Privacy Principles
[8] Public Records Act 2005 No 40 (as at 01 September 2022), Public Act Contents – New Zealand Legislation
[9] Official Information Act 1982 No 156 (as at 01 September 2022), Public Act Contents – New Zealand Legislation
[10] Education and Training Act 2020 No 38 (as at 01 September 2022), Public Act Contents – New Zealand Legislation
[11] Right to be Forgotten - General Data Protection Regulation (GDPR) (gdpr-info.eu)

Regulations

Whereas Acts are bills that have been passed by Parliament and have received the Royal assent, Regulations are law-making actions – including the developing of standards and rules -- made under the delegated authority of an Act.

Government Domain Obligations

NZ Government agencies are obligated by regulation[12] to adhere to All of Government (AoG) Digital Standards.

The following is a catalogue of the standards applicable to AoG agencies:

AoG Digital Standards

Table 1: AoG Digital Standards

NZ Government Digital Standards
NZ Information Security Manual (NZISM) Standards: Guiding security of information and communication decisions
NZ System Data and Information Management Standards: Guiding the management of data and information within government systems[13] including ensuring data be Open, Protected, Readily Available, Trusted and Authoritative and Well Managed[14].
NZ Digital Service Design Standards: Guiding digital based service design, including providing services that are specific, clear, secure, inclusive, ethical, empowering, open, accessible, etc.[15]
NZ Government Web Standards:[16] Guiding digital accessibility & usability of government provided services, comprised of the Web Accessibility (1.1) and Web Usability Standards (1.3).
NZ Digital Standards: Guiding system procurement & development[17]

[12] Web Standards Cabinet Minute and Paper | NZ Digital government
[13] https://www.data.govt.nz/manage-data/policies/new-zealand-data-and-information-management-principles/
[14] https://www.data.govt.nz/manage-data/policies/new-zealand-data-and-information-management-principles/
[15] https://www.digital.govt.nz/standards-and-guidance/digital-service-design-standard/
[16] NZ Government Web Standards | NZ Digital government
[17] https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/government-enterprise-architecture/government-digital-standards-catalogue/digital-standards-principles

Agreements

NZ Government agencies are required to meet agreed agreements the government has committed the country to upholding.

International

The NZ Government is a member of the United Nations (UN) and must meet its member obligations and uphold its commitments, including adhering to the following inclusion principles:

Table 2: International Agreements

International Agreements
Universal Design principles: promoting equitably accessible, flexible, intuitive, and simple use that is forgiving of errors, avoiding reliance on special attributes.
United Nations Declaration of the Rights of Indigenous People (UNDRIP) New Zealand has accepted UNDRIP ass a non-legally binding document and been a signatory since 2010. UNDRIP establishes a universal framework of minimum standards for the survival, dignity, and well-being of the Indigenous peoples of the world and it elaborates on existing human rights standards and fundamental freedoms as they apply to indigenous peoples.
United Nations Convention on the Rights of the Child[18] New Zealand is a signatory to the UNCRC since 1993. Every child has the right to survival, protection and education, and to have their voice heard.
United Nations Convention on the Rights of Persons with Disabilities[19] Since 2008 NZ has been a signatory of the convention to promote, protect and ensure the full and equal enjoyment of all human rights and fundamental freedoms by all persons with disabilities, and to promote respect for their inherent dignity.

Sanctions

New Zealand's has current sanctions against Iran, North Korea, etc., in specific domains.

> *Note:*
> *none currently that overlap with the domain of education.*

[18] https://www.msd.govt.nz/about-msd-and-our-work/publications-resources/monitoring/uncroc/

[19] United Nations Convention on the Rights of Persons with Disabilities - Office for Disability Issues (odi.govt.nz)

Other

Other agreements may exist or develop at a national, sector or organisational level and should be investigated at the start of projects.

Commitments

Binding

As a member of the WTO[20], and signatory of the TBT, we are bound by WTO's Code of Practice, to use international standards where applicable[21]. These international standards generally reflect the best practice of industry and regulators worldwide and cover conditions in a variety of countries.

Non-Binding

While not Obligated, nor formal Agreements, the following are non-binding Commitments that are expected to be upheld by services offered by government agencies.

International: United Nations Declaration of the Rights of Indigenous People (UNDRIP)[22]

New Zealand has accepted UNDRIP ass a non-legally binding document and been a supporter since 2010.
UNDRIP establishes a universal framework of minimum standards for the survival, dignity and well-being of the Indigenous peoples of the world and it elaborates on existing human rights standards and fundamental freedoms as they apply to indigenous peoples.

National Commitments: Te Mana Raraunga[23]

The Government has made non-binding commitments to actively try to implement Māori Data Sovereignty (MDS) objectives where possible.

MDS recognises that Māori data should be subject to Māori governance. Māori data sovereignty supports tribal sovereignty.

> *While governance of data by Māori is addressed by the establishment of* Te Rito Kaitiakitanga *(see below), the development of data storage infrastructure in NZ, managed by Māori or not, is not a current project objective due to envisioned latency impacts on all other users.*

---

[20] https://www.mfat.govt.nz/en/trade/our-work-with-the-wto/
[21] Home (iso.org)
[22] National Govt to support UN rights declaration | Beehive.govt.nz
[23] Te Mana Raraunga

Standards

As a member of the World Trade Organisation (WTO), and signee of The Agreement on Technical Barriers to Trade (TBT), New Zealand has made commitments to ensuring technical regulations, standards, and conformity assessment procedures are non-discriminatory and do not create unnecessary obstacles to trade. The TBT Agreement strongly encourages members to standardise on international standards.

International ICT Standards

Government projects are expected to reduce risk by reducing the reliance on novel processes and approaches, using internationally agreed standards first.

These include, but are not limited to the following:

Table 3: Context View - ICT Standards

ICT Standards
ISO-9000 A set of 5 standards to manage Qualities of Delivery, Systems, Data. Operations.
ISO-12207 Software Life cycle processes A standards-based description of the processes, artefacts, and deliverables to follow to decrease risk of delivery system or software. See ISO-29110.
ISO-15288 Processes and Lifecycle stages
ISO-15289: Information Item Development during system lifecycles In essence describes the types of information artefacts (requirements, design, information, schemas, test definitions, change control processes, etc.) that benefit the delivery of systems.
ISO-29110: System and Software Lifecycle Profiles & Guidelines for Very Small Entities In essence, describes Agile processes, artefacts and expected deliverables as an internationally agreed standard,
ISO-42010: System and Software Architecture Description Design documentation benefit by following internationally understood conventions of breaking down complex models into distinct views/chapters for the benefit of specific stakeholders. This convention is followed to develop SADs such as this document.
ISO-19505: Unified Modelling Language Design documentation benefit from the use of diagrams, especially when widely accessible by professionals due to using international industry standards – such as the use of UML diagram conventions.
ISO-13028: Information and Documentation Implementation guidelines for digitation of Records In essence guides documentation to be managed as digital assets.

ISO-25010: Qualities of Systems

While a system is expected to deliver functionality as expected by stakeholders, it is expected to be delivered to at least an ISO defined list of minimum qualities: Functionality (completeness, etc.), Usability, Accessibility, Performance, Security, Supportability, Maintainability, etc.

ISO-25012: Qualities of Data

While a system's purpose is to facilitate actions, based on decisions, based on information, based on managed data, the data is expected to have an ISO defined list of qualities, including appropriateness completeness, accuracy, currency, etc.

ISO-25022: Qualities in Use

While a system and its data may have measurable technical qualities, a system can be measured as to its ability to meet its business purposes objectives in terms of effectiveness, efficiency, satisfaction, safety, and context coverage.

Guiding Principles

Services are expected to follow agreed applicable Guiding Principles.

Public Domain Principles

The following are Principles that are applicable to all systems delivered within New Zealand, irrespective of whether they are in or out of the Government Sector or Education Sector.

Privacy Guiding Principles

NZ Regulation requires adherence to the NZ Privacy Act 2020, which defines 13 Principles, organised into 3 groups, listed below with a summarised explanation of their intent:

Table 4: Context View - Privacy (Collection) Guiding Principles

Collection Principles
IPP1: Purpose for Collection Essentially, purpose but be lawful, and associated to the agencies purpose, and necessary.
IPP2: Source of Personal Information – collection from the individual Preference collecting from the person themselves, unless impractical and can collect from an authorized delegate.
IPP3: What to tell the individual about collection Essentially, inform the user that information is being collected, by whom, for what purpose, accessed by whom, regulatory context and ramifications if not provided.
IPP4: Manner of collection

Essentially, Collection must be lawful, fair and reasonable in scope and impact

Table 5: Context View - Privacy (Storage) Guiding Principles

Storage Principles
IPP5: Storage and Security of Personal Information
Essentially, Safeguards must be in place to prevent loss, misuse and disclosure of PI.
IPP6: Providing People Access to their Information
Essentially, Provide people the means to request access to their own Personal Information.

Table 6: Context View - Privacy (Use & Sharing) Guiding Principles

Use and Sharing Principles
IPP7: Correction of Personal Information
Essentially, provide people the means to request corrections to their Personal Information.
IPP8: Ensure accuracy before using information
Essentially, before disclosure, Organisations must ensure personal information is accurate, current, complete, relevant, and not misleading.
IPP9: limits of Retention on personal information
Essentially, organisations should not keep personal information for longer that it is lawfully usable for intended purposes.
IPP10: Use of Personal Information
Essentially, with few exceptions, collected information must be used for what it was collected.
IPP11: Disclosure of Personal Information
Essentially, personal information can only be disclosed for the lawful purpose it was originally collected.
IPP12: Disclosure outside New Zealand
Essentially, disclosure of information to organisations outside of NZ may only occur if they will protect the information, are subject to laws comparable to NZ's Privacy Act, are subject to NZ's Privacy Act due to doing business in NZ.
IPP13: Unique Identifiers Essentially, sets restrictions on assigning unique identifiers to individuals across systems.

Government Sector Principles

Government Agencies are bound[24] to follow the following principles.

New Zealand Data and Information Management Principles

Table 7: New Zealand Data and Information Management Principles

New Zealand Data and Information Management Principles
GDIMP1: Open Note: Open does not mean it includes Personal Information (PI).
GDIMP2: Protected
GDIMP3: Readily Available
GDIMP4: Trusted and Authoritative
GDIMP5: Well Managed
GDIMP7: Reusable

Archives New Zealand Information and Records Management Standards

The Records Act 2005 obligates every public office to create and maintain full and accurate records of its affairs in an accessible form until their disposal is required by an Act[25].

Archives New Zealand, empowered via delegation under the Records Act 2005, has mandated that government agencies the following principles[26].

Standards
AP1: Organisations are responsible for managing information records This principle outlines that (1.2) agency senior management are responsible for (1.1) their agencies developing strategies and policies, (1.3) overseen by an Executive Sponsor managing (1.4) trained staff, and (1.8) monitoring of (1.5) business owners being responsible for their (1.6) staff and contractors, and (1.7) communicating responsibilities in contractual offers and instruments.
AP2: Information and records management supports business This principle outlines that (2.1) information required for business must be identified, (2.2.) calling out high risk/high value areas, so that they can be (2.3) met by system

[24] Information and records management standard – Archives New Zealand (Section 27 of the Public Records Act)
[25] Public Records Act 2005 No 40 (as at 01 September 2022), Public Act 17 Requirement to create and maintain records – New Zealand Legislation
[26] Information and records management standard – Archives New Zealand

designs, to (2.4) support monitoring across all operating environments, (2.6) address the needs of transitioning across systems over (2.5) the full length of its value.

AP3: Information and records are managed well

This principle outlines that (3.2) accurate, correct Records must be (3.1) routinely developed as BAU, (3.3) such that they are discoverable, identifiable, retrievable, accessible, viewable and usable as long as they have value, while (3.4) / (3.5) being protected from unauthorised and/or unlawful access, dissemination, alteration or destruction, and (3.6) kept as long as needed for business, legal or accountability reasons, then *transferred to Archives New Zealand* or alternate approved repository, or (3.7) disposed of only *when authorised to do so,* and *the disposal process is recorded for later auditing.*

Enterprise Principles

Guiding Principles have been developed by this organisation. These are documented elsewhere[27] and are expected to be adhered to unless exempted by the appropriate governance mechanisms[28].

Recommendations

Taking into account the above constraints, the following is a list of recommendations to consider when developing functional, quality and transitional contractual requirements for an education sector system.

Discovery and Definition Considerations

- Follow BABOK guidance for the development of requirements.
  Namely, develop:
  - Business requirements, met by
  - User Requirements, which in turn influence the querying for and development of:
  - System Requirements, developed as:
    - System Functional Requirements
    - System Quality Requirements (according to ISO-25010)
    - Information Quality Requirements (according to ISO-25012)
  - Delivery requirements, developed as:

[27] Refer to the organisation's intranet.
[28] Via the Ministry Design Authority (MDA)

    - Transitional Requirements
- Most government systems are information systems. Therefore, consider referencing and incorporating outcomes and guidance defined within ISO-13028**.**

Documentation Considerations

- Develop Solution Architecture Description (SAD) documentation according to ISO-42010 guidelines. Namely, as a series of curated Views developed from the perspective of different stakeholder and user groups: Sponsors, Business Service Users, Business Service Support, System Support, System Operations, System Monitoring, System Maintenance, System Development, System Quality Assurance, Solution Accreditation, System Deployment.
- Primarily use ISO based UML diagrams intended for a technical audience. [29]

Delivery Process Considerations

- Follow *ISO-29110: System and Software Lifecycle Profiles & Guidelines for Very Small Entities* guidance, which defines an Agile process to delivering software-based systems, while integrating with other international ISO frameworks.

Service Infrastructure Considerations

- Persist data on infrastructure maintained by organisations who have obtained ISO-27001 Level 2+[30] compliance.
- Persist data in an encrypted manner where reasonably possible.
- Persist data on or developed by Māori citizen in New Zealand when practical and not diminishing security considerations or significantly impacting usability (e.g.: latency).
- Noting that if Azure or AWS services are used when these services become available in New Zealand, they may become susceptible to data requests by the US if NZ becomes a CLOUD Act partner in the future.
- Either by external WAF or system-based controls, limit traffic from specific countries (“geo-block”) when the type of transaction makes it applicable.

[29] Simpler box/line diagrams should be used for non-technical audiences.
[30] The key difference being that level 1 is *self*-assessed, and 2 indicates having been accessed by a third party.

> *Noting -- and accepting -- that this approach is easily circumventable with the use of Virtual Private Networks (VPNs), it remains a recommendation of NZISM.*

Service Discovery Considerations

- Ensure the system is made discoverable by end users by being associated to a government DNS top-level domain (TLD) (i.e., ".govt.nz"), and/or associated to a government agency's DNS subdomain (i.e. "education.govt.nz").

Service Design Considerations

- Consider only using logical deletion of data, not physical, thereby being able to offer functionality to undo "Delete" operations, lowering support costs.
- Consider leveraging cloud Services to decrease development, testing and deployment effort. These become available once hosted in a cloud provider.

> *I.e., don't continue to develop using an IaaS or even a CaaS based approach if you are developing for the cloud. Prefer instead a PaaS based approach to decrease the development, testing, maintenance, and security areas that you are responsible for.*

Service Rendering Considerations

- Consider offering supporting sites to address the following concerns:
    - Subsite in the organisation's public website (improving discoverability)
    - Summary Information (i.e., a dedicated separate brochure site)
    - Self-Help (i.e., documentation)
    - Support (i.e., ticketed assistance)

Service Disclosure Considerations

- Ensure the service provides a self-help channel to correct or ask correction of personal information. After all, a person is expected to know themselves best.
- Ensure the service provides a tracking statement.
- Ensure the service provides a data use statement explaining:
    - what personal information is collected,
    - for what purpose,
    - how it may be corrected,
    - with whom it is shared, and
    - how to request it be removed.

Service Data at Rest Considerations

System Data

- Ensure backups of service databases (transactional, reporting, PI – if doing it very well) are encrypted as well.
- Ensure physical access to encrypted data stores is not permitted (e.g., by being remote, in an ISO-27001 Level 2+ compliant data facility).
- Ensure remote access to encrypted data stores is limited to service accounts for automation, and excludes stakeholders, including users, stakeholders, user SMSs, quality assurers, system supporters, operators, maintainers, etc.
- Provide non-production environments with the functionality required by stakeholders, user SMEs, quality assurers, supporters, operators, maintainers, to perform their expected tasks.
- For usability and system stability, auditability, and maintainability reasons, it is recommended to never *physically* delete records of any kind, but only *logically* change their state (Current, Replaced, Merged, Removed, Restored, Deleted)[31]. Higher quality systems will provide Versioning as well.
- For correctness quality reasons, noting that the data is stored, processed, and viewed in one or more time zones, ensure that data models are developed using universal formats. The use of UUIDs[32] for data store identifiers instead of integers is recommended as is the use of UTC+offset based formats for dates and times).

Personal Data

- Consider persisting Personal Identifier information in a table separate from the system User table. Merging the two only for presentation purposes.
- Consider persisting Personal Identifier (PI) information in a separate datastore than operational datastore than the transactional database of a system.
- Whereas the Privacy Act and GDRP state that personal information is to be deleted from the service when no longer required or upon request, it makes exceptions if the data is still required legally.
    - The requirements of the regulation developed by the National Archives are a legal requirement.

[32] Preferably generated on the tier closest to the User using an agreed sequential date/time prefix + random suffix algorithm.

- The process of making personal information impersonal is achievable via the disassociation of system data from *personal* information. Specifically, deleting the Personal Identifying Information (PII) Attributes of the Person the Personal Information (PI) is associated to -- making the records Anonymous -- is sufficient in most cases[33].

Service Data in Transit Considerations

Channel & Message Considerations

- Redirect unsecured HTTP traffic from external service consumers towards HTTPS equivalent endpoints.[34][35]
- Ensure Session Tracking Cookies are marked secure so that they are only transmitted from the server to the service client if the request was made over HTTPS.
- Ensure Session Tracking Cookies are marked HTTP-Only so that they cannot be retrieved, viewed and/or manipulated via [JavaScript] code executing on the service clients.
- Use Encrypted channels between Components where technically and reasonably possible, falling back to encrypted messages when technically and reasonably possible. In other words, consider using secure flags on SQL Server connection strings, etc.
- Do not transmit to service consumers (browsers or otherwise), System Identifiers[36] that could be used to correlate data between systems.

> *Note: this mirrors regulation in the Education and Training Act around the use of the NSI as a correlation identifier.*

Service Accessibility and Usability Considerations

- Ensure the service is accessible to this country's visually impaired users by its HTML interface implementing ARIA tags and other requirements of WCAG AA+.
- Ensure that the system can persist a User [System] Profile for the User, where User Preferences can be persisted.

---

[33] Notes require deletion as well if they could contain PI (e.g.: IDs of medical records in other systems, etc.).
[34] This is a configuration at the web server level, generally outside of the application logic.
[35] Only for www resources that may be directly addressed by end users. All other components (eg: caching, static, imags, etc.) should be limited to HTTPS only as users should not be addressing them directly.
[36] Consider XORing system storage identifiers that are roundtripped outside the system.

- Ensure an Authenticated User can persist their preferred presentation layer Culture-Language.
- Ensure the system permits unauthenticated users select and persist a Session User's Culture-Language preference (i.e., via a Session or Persistent cookie that is updatable from an Authenticated User's Profile Culture-Language Preference).
- It is recommended that the presentation layer run in a service client (i.e., Single Page Application (SPA) in a browser) to cleanly separate it from the service interface layer (i.e., API endpoints) to facilitate user interface work listed next.
- In some specific cases, separate interfaces, copy and media may be required to be presented to different users (e.g., mi-NZ interfaces may be completely different than en-NZ interfaces).

  > *for example, teachers who may require a more complex adult oriented interface, and pre-schoolers who would benefit from a simpler, more engaging, interface).*

- Ensure system is translatable to this country's national languages (en-NZ, mi-NZ).
- Ensure the system's header and footer adhere to the organisation's standards, which *should* meet NZ Web Usability Standards as well as well as NZ Accessibility Standards.
- Irrespective of the last point, ensure the system's header and footer and disclosures meet the latest *NZ Web Usability Standards*[37] (which covers logo usage, links to disclosures, etc.) and *NZ Accessibility Standards*.
  - The website's home page must include
    - the name and logo of the NZ Government organisation primarily responsible for the website.
    - a link to https://www.g ovt.nz must be provided, preferably with a suitable and approved current all-of-government logo.
    - a "Contact Information" link for contacting the organisation responsible for the site, and/or obtaining help related to the site, via at least one of a regularly monitored email, postal address, and call centre phone number, and link to the New Zealand Relay Service (NZ Relay)(external link).
    - A link to a General Copyright statement, that indicates it applies to the website, and its contents are protected, listing licensing terms if any.

      The website must indicate the source and copyright status of material either within the General Copyright statement or beside each item of third-party

[37] Web Usability Standard 1.3 | NZ Digital government

copyright material, making mention that material covered by the Flags, Emblems and Names Protection Action 1981 are exempt.

- A link to a General Privacy Statement, which clearly identifies that it applies to the website, the scope, attributes, collection circumstances, uses and sharing, of personal information collected.
  The statement should cover the use cookies, and their purpose.
  The statement should provide users information on their right to correct or update information collected, and how to.
- All links to media must be accompanied by the files format and size.

- The main content of each web page -- excluding thematic headers and footers, navigation and search components -- MUST be printable in its entirety on standard A4 paper, in black text on white background.
- The website should apply the New Zealand Government Open Access and Licensing (NZGOAL) framework when considering the licensing terms that apply to copyright material on the website.

Service Auditability Considerations

- Audit all Operations, whether they change data state or not, whether anonymous or authenticated.

Service Data Considerations

- Make as much as possible of the system's information is Open for public unauthenticated public access.
- Do not permit change of data (comments, records, etc.) by unauthenticated users.
- Make as much as possible the system's Data available for consumption without limit to authenticated users.
- Ensure Media used is granted permission or is copyleft (e.g.: Creative Commons[38]).
- Ensure Māori media is granted documented permission up front, and/or the system has in place a process to accept Applications for Consent/Terms & Conditions Acceptance/Consent Approval[39].

[38] Homepage - Creative Commons

[39] Admittedly, more complex than a blanket copyright law based approval, but it is important for project delivery stakeholders to not confuse Copyright – even Copyleft -- with Consent, and understand *why* it is required.

Appendices

Appendix A - Document Information

Author & Collaborators

Author: Sky Sigal, Solution Architect

Versions

0.1 Initial Draft

0.2 Restructuring

Images

Tables

References

There are no sources in the current document.

Review Distribution

The document was distributed for review as below:

Identity	Notes
Alan Heward, Senior Compliance Advisor	
Sandy Britain, Enterprise Architect	
Amy Orr, Data Domain Architect	

Rodney Snell, Business & Technical Lead

Audience

The document is non-technical in nature.

Diagrams

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

Terms

Acceptance : to assent to the terms of an offer.

Act : an Act is a public, private, local, provincial, or imperial law passed by Parliament. Before it is passed by parliament, it is called a *Bill*.

Adjudicative : the legal process of reviewing evidence and argument presented by parties in dispute to arrive at a decision as to rights and obligations.

Agreement : a meeting of the minds in a common intention, made through *offer* and *acceptance*. Agreement can be shown from words, conduct, and in some cases, silence.

Bill : a proposed Act, introduced by a member of Parliament before the House of Representatives for its consideration, at which point it becomes publicly available.

Consideration : a *promise*, performance, or *forbearance* bargained by a promisor in exchange for their *promise*. It is the main element of a *contract*. Without *consideration* by both parties, *contract*s are unenforceable.

Contract : a contract is legally binding *agreement* between two parties, that can be enforced in court if necessary. To be enforceable, a contract must meet certain requirements: *offer*, *acceptance* and *consideration*.

Dispute : a dis*agreement* that may require *dispute resolution* to progress outcomes.

Dispute Resolution : or dispute settlement, through either avoidance, consensual (facilitation, negotiation, conciliation, mediation), or adjudicative (litigation or arbitration by judge, jury or arbiter) processes.

Forbearance : the intentional action of abstaining from doing something.

House of Representatives : the body made up of individuals, called Members of Parliament (MPs), elected for a term of 3 years.

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

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

Law : the set of rules that are created are enforceable by social or government institutions to regulate behaviour.

Offer : part of *contract negotiations* where a party agrees to do or not do something in exchange for *consideration*.

Promise : a one-sided oral or written commitment statement by one party to another that creates an *obligation*. An assurance that a certain action will be taken, or outcome will be

achieved. To be legally enforceable, a *promise* must meet certain requirements, such as *consideration* and *intention* to create legal relations.

Regulation : law-making actions – including the developing of standards and rules -- made under the delegated authority of an Act.