# Data & Information Management Framework

Guide

New Zealand Government

# Document Control

| | |
|---|---|
| **Project ID/Name** | Data & Information Management Framework |
| **Author** | Regine Deleu – Strategic Enterprise Architect – Data Governance – Digital Transformation<br>Know-MAT member agencies[1] |
| **Title** | Data & Information Management Framework - Guide |

## Document Classification: UNCLASSIFIED

## Purpose

Information is increasingly being recognised as a key economic resource and as one of the organisation's most important assets. Despite gaining recognition as an asset in its own right, information has so far resisted quantitative measurement. While it consumes vast and ever increasing quantities of organisational resources in terms of data capture, storage, processing and maintenance, it typically receives no financial recognition.

There currently exists no consensus on how to measure the value of information[2], although a lot of techniques have been developed. In practice, information has a notional value only: people think it is valuable but they can't put a number on it. Almost all the literature on the financial valuation of information systems has focused on the technology rather than the information content.

In this document, there has been considerable interest in measuring of the quality of information. This document serves as a guide for ensuring an organisation's quality information for decision making. It describes the components needed. In particular, these guidelines can be used by organisations as part of the education and communication process for improving data and information quality management in their organisation.

[1] Appendix B contains a list of Know-MAT member agencies.
[2] Appendix C contains Information Valuation Models.

# Revision history

| Version | Date | Description of changes | Author | Approved by |
|---|---|---|---|---|
| 0.1 | March 2015 | Initial draft | Regine Deleu | |
| 0.2 | September 2017 | Added comments received during a Know-MAT work session. | Regine Deleu | |
| 0.3 | September 2017 | Added the explanation of the eight dimensions of GEA-NZ and the relationships between them. | Regine Deleu | |
| 0.4 | October 2017 | Added the explanation of the focus areas, and the diagrams to give a visual overview of the components needed. | Regine Deleu<br>John Fisher | |
| 0.5 | October 2017 | Added comments received during the Know-MAT work session around Business. | Regine Deleu | |
| 0.6 | December 2017 | Added comments received during the Know-MAT work session around Strategy, Investment, and Policy & Governance and Performance. | Regine Deleu | |
| 0.7 | December 2017 | Expanded the Introduction with the reasoning behind recognising information as an asset and the characteristics of information.<br>Also added Appendix C containing Information Valuation Models | Regine Deleu | |
| 0.8 | January 2018 | Added comments received during the Know-MAT work session around Data and Information, Application and Software Services, and Infrastructure. | Regine Deleu | |
| 0.9 | February 2018 | Added the “Information Value for a Purpose” In Appendix C | Regine Deleu | |
| 0.10 | February 2018 | Added comments received during the Know-MAT work session around Identity, Privacy, and Security, and Standards. | Regine Deleu | |
| 0.11 | February 2018 | Added comments received from the GCPO team. | Regine Deleu | |
| 1.0 | March 2018 | First final version | Regine Deleu | Know-MAT |
| 2.0 | June 2018 | Changed the title from ‘Data and Information Quality Management’ to ‘Data & Information Management Framework’<br>Changed the title of the valuation formula in Appendix C from “Information Value for a Purpose“ to “How to Value the Quality of Your Information Asset”<br>Added more question to identity and weight the criteria of your information asset. | Regine Deleu | |

# Table of Contents

# Introduction

***"Quality of data is one of the key fundamentals to the success of the business. High quality information is the foundation for good decision making and effective collaboration."***

Information is increasingly being recognised as a key economic resource and as one of the organisation's most important assets. Despite gaining recognition as an asset in its own right, information has so far resisted quantitative measurement. While it consumes vast and ever increasing quantities of organisational resources in terms of data capture, storage, processing and maintenance, it typically receives no financial recognition on the balance sheet. While hardware and software assets are capitalised, the valuation of information has been largely ignored, even though this is a much more valuable asset from a business viewpoint.

Hardware and software are merely mechanisms used to create and maintain information -information is the underlying business asset that is produced and maintained by this technology. Information provides the capability to deliver services, make better decisions, improve performance, achieve competitive advantage and can also be sold directly as a product in its own right. Using a manufacturing analogy:

- Data is the raw material
- Software and hardware are the plant and equipment
- Information is the end product that is delivered to the customer.

The overwhelming component of both the cost and value of an information system resides in the information stored rather than the hardware and software used to store it. To take an example, an information system in an organisation requires $500,000 worth of hardware to operate (calculated as a proportion of usage). The software cost $2 million to develop. However every year, over $10 million are spent entering information and keeping it up to date— these costs are hidden in salary budgets.

To be most effective, the technology strategies should be focused on enhancing and sustaining the value of information (the product) rather than on systems and technology (the production equipment). Business strategies are generally evaluated in terms of how they contribute to the value or profitability of the organisation. Technology strategies should be evaluated in terms of how they contribute to the value of information they deliver. To do this, we need some way of measuring the value of information.

There currently exists no consensus on how to measure the value of information[3], although a lot of techniques have been discussed and developed. In practice, information has a notional value only: people think it is valuable but they can't put a number on it. Almost all the literature on the financial valuation of information systems has focused on the technology rather than the information content. In this document, we place considerable interest in the quality of information and where we need to focus on within the organisation.

[3] Appendix C contains Information Valuation Models.

# Information as an Asset

Before we can put a value on information assets, we need to know if information really is an organisational asset. What are the essential characteristics of an asset[4]?

An organisational asset:

- has a service potential or economic benefit: something is only an asset from an accounting viewpoint if it is expected to provide future services or economic benefits. The benefits may arise from either the use or sale of the assets. Information satisfies this requirement, because it provides the capability to deliver services and to make effective decisions.
- is controlled by the organisation: "control" in this sense means the capacity of the organisation to benefit from the asset and to deny or regulate the access of others to that benefit. Information also satisfies this requirement -if an organisation has information, it alone has access to it unless it sells or gives access to another party.
- is the result of past transactions: this means that control over the asset has already been obtained as a result of past transactions such as purchases, internal development or discovery. Information also satisfies this requirement. Information is usually collected as the by-product of transactions which have occurred (internal development), or may be the result of a purchase (e.g. a proprietary mailing database) or discovery (e.g. through analysis of data).

Information satisfies the definition of an asset much better than employees or customers, which are also commonly referred to in the literature as assets. Employees and customers result in service potential and future economic benefits, but are not owned by the organisation -if employees were to resign or customers to change suppliers, the company would lose the benefits without compensation, Information is a non-physical or intangible asset. However it is the service potential and economic benefits, not the physical form of an object, which is relevant in assessing whether an asset exists.

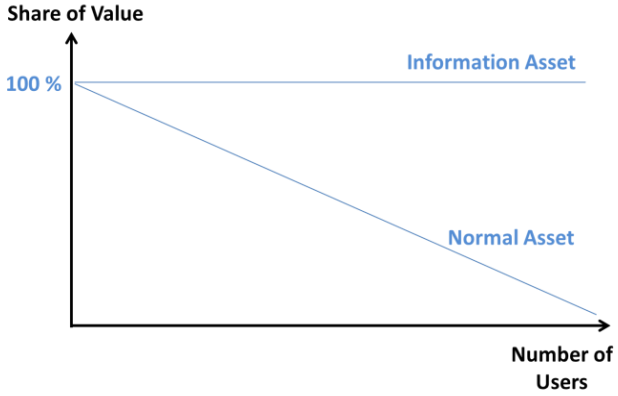
Of all the corporate resources (people, finances, assets, information), information is probably the least well managed. If most organisations managed their finances as badly as their information, they would probably be out of business. The amount of duplication, lack of standardisation and lack of attention to quality of information would probably not be tolerated for other assets. However one explanation for why information is so poorly managed is that it is not well understood. For this reason, defining "characteristics of information" may provide the basis for improving the management of information. Those characteristics need to be understood in order to manage information effectively, in the same way that it is necessary to understand characteristics of human behaviour to manage people effectively, or the characteristics of economics to manage finances effectively.

[4] Godfrey et al, 1997; Henderson and Peirson, 1998

# The Seven Characteristics of an Information Asset[5]

Like other organisational assets, information has a cost -how much it costs to acquire, store, and maintain it- and a value -how much it is worth to the organisation. However this is where the similarity ends. Information does not obey the same characteristics of economics that other assets do -it has some unique properties which must be understood in order to be able to measure its value. We have attempted to define the nature of information as an asset by identifying a number of general characteristics which govern its behaviour as an economic asset.

## Characteristic 1: Information is Shareable




Perhaps the most unique characteristic of information as an asset is that it can be shared between any number of people, business areas and organisations without consequent loss of value to each party.

The Net provides the perfect example of how the same information can be shared by a virtually unlimited number of people. This is quite different to how other assets behave. Most assets are *appropriable* - either you have it or I have it. In the case of information, we can both have it.

For example, sharing finances, equipment or staff between business units results in each business unit receiving some proportion of the total value of the assets. On the other hand, information can be shared by multiple business units while having the same value to each unit as if they had exclusive use of the information. From the organisation's point of view, value is therefore *cumulative* rather than apportioned across different users.

Another example, if one business unit maintains a currency rate table, this information can be shared with other business units without increasing the cost or reducing the value of the information. The alternative to this would be making decisions without the required information -with consequent loss of business effectiveness- or the other business units maintaining their own currency rate table -with consequent increase in costs.

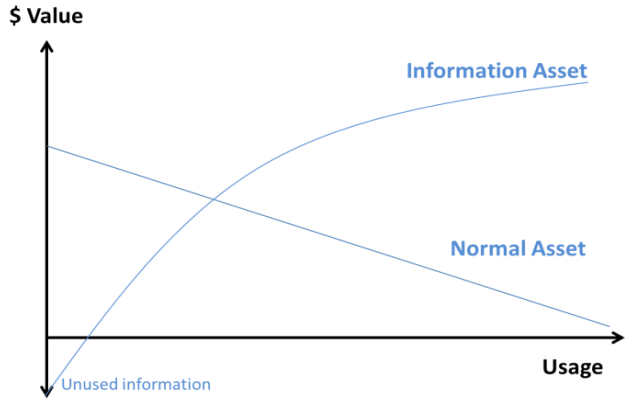
In general, sharing of information tends to *multiply* its value— the more people who use it, the more benefits can be extracted from it.

A major problem in practice is that there are barriers, both institutional and personal, to sharing of information. "Knowledge is power", and as a result, people do not share information easily. *Information hoarding* -where people deny others access to information- represents a loss of business opportunity, because it prevents the potential value of information being realised.

Unfortunately, not only can information be shared, but it can also be infinitely *replicated* -this is the result of not sharing information. Duplicating information does not double its value -two copies have the same value as a single copy because no "new" information is created. Duplication leads to no additional value, only additional costs. Costs of redundant data include: costs of re-keying data into multiple systems, storage costs, additional systems development effort, interfaces to keep data consistent and manual reconciliation effort. The cost of maintaining such levels of redundancy can be enormous. The fact that it is allowed to happen in an uncontrolled manner reflects the lack of financial accountability in information management activities.

[5] Moody and Walsh, 1999

# Characteristic 2: The Value of Information Increases with Use




Most resources exhibit *decreasing returns to use* —that is, they decrease in value the more they are used. For example, vehicles depreciate based on kilometres travelled, aircraft based on flight hours, and equipment based on hours in operation. However information actually increases in value the more it is used -that is, it exhibits *increasing returns to use*.

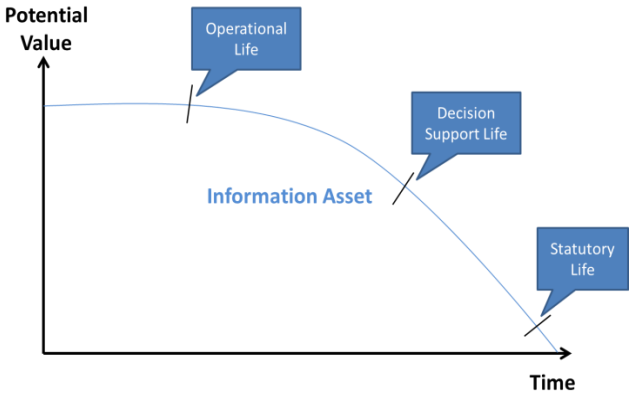
The cost of information is in its capture, storage and maintenance— the marginal costs of using it are almost negligible. Information has no real value on its own —it only becomes valuable when people *use* it. From an accounting point of view, something can only be an asset if it provides services or economic benefits. If information is not used, it cannot possibly result in economic benefits and is therefore not an asset. Unused information is really a *liability*, because no value is extracted from it, and the organisation incurs future costs of storage and maintenance. In many organisations, there is a large amount of information that is collected and stored but never used— this represents waste.

The prerequisites for using information effectively are:

- knowing it exists
- knowing where it is located
- having access to it
- knowing how to use it

Information is at its highest "potential" when everyone in the organisation knows where it is, has access to it and knows how to use it. Information is at its lowest "potential" when people don't even know it is there. In most organisations there is a huge amount of computer based information that could be used for business advantage. However the opportunities for using information are often not realised because people don't know it exists. As obvious as it seems, few organisations have a catalogue of their information assets and where they are located -an information asset register. Such a situation would be intolerable for physical or financial assets. However information is not subject to the same audit requirements as other assets. Another important issue is that of *information literacy*. It is often assumed that if information is provided to people that decision-making will automatically improve. However the quality of decision making depends on both the quality of information provided and the ability of decision-makers to interpret the information and use it to take the appropriate action -information literacy. There is little point in improving the accuracy and timeliness of data if people don't know how to use it effectively. Equal emphasis therefore needs to be placed on improving people's information literacy skills as improving the quality of information itself.

# Characteristic 3: Information is Perishable

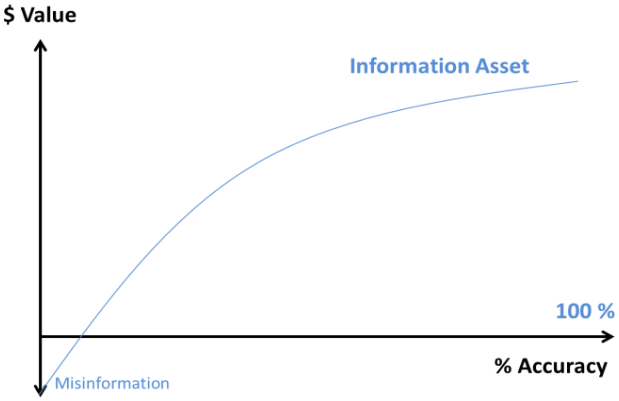



Like most other assets, the value of information tends to depreciate over time. The speed at which it loses value depends on the type of information. For example, once a customer has changed their address, the old address may be of little or no importance. On the other hand, product sales figures may be relevant for years into the future.

Information has three "lives": an operational life, a decision support life and a statutory life. For example, airline tickets must be kept for a year for operational purposes because tickets are valid for one year after purchase (operational life). However for decision-making purposes, ticket sales for the last five years may be relevant to help spot trends and patterns (decision support life). Beyond this, there are legal requirements to keep records for ten years (statutory life).

Information has a relatively short useful lifetime at the operational level. Usually, the only information of relevance is very recent information— a customer's current address or their last bill. It has a much longer lifetime for decision support purposes. In practice, operational systems often discard information once it has exceeded its operational life, making it unavailable for subsequent decision-making purposes. Data warehousing provides a mechanism for storing historical information which has exceeded its operational life, and making it available for decision support and analysis.

# Characteristic 4: The Value of Information Increases with Accuracy

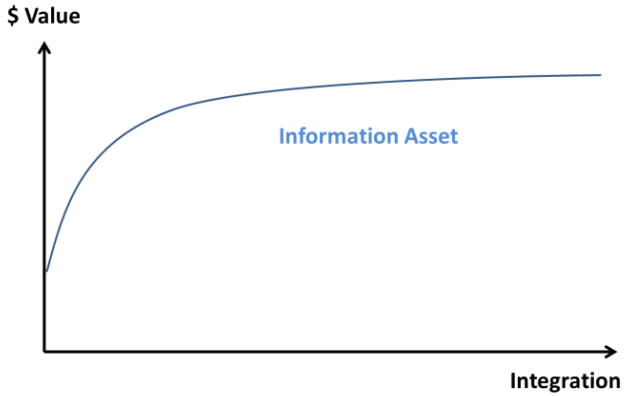



In general, the more accurate information is, the more useful and therefore valuable it is. Inaccurate information can be very costly to an organisation in terms of both operational errors and incorrect decision making. The level of accuracy required is highly dependent on the type of information and how it is used. For some information, 100% accuracy may be required (e.g. aircraft maintenance data or banking records), while for other information 80% may be good enough for practical purposes (e.g. employee home phone numbers).

There is a point of diminishing marginal returns, where increasing the accuracy further provides little additional benefit -100% accurate information is rarely required in a business context. Once the accuracy of information falls below a certain level, it becomes a liability rather than an asset. At this point, it becomes "misinformation" and people will stop using it.

For decision making purposes, often just knowing the accuracy of information is as important as having accurate information. If decision-makers know how accurate (or inaccurate) the information they are working with is, they can incorporate a margin for error into their decisions. However in practice, the accuracy of data is rarely measured -people rely instead on subjective opinions and anecdotal evidence.

# Characteristic 5: The Value of Information Increases when Combined with other Information

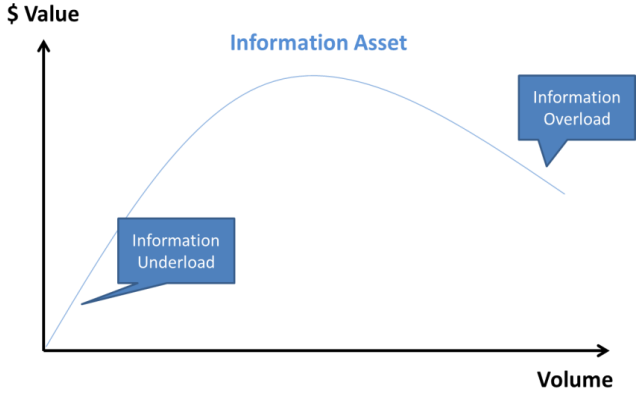



Information generally becomes more valuable when it can be compared and combined with other information. For example, customer information and sales information are each valuable information sources in their own right. However being able to relate the two sets of information together is infinitely more valuable from a business viewpoint. Being able to relate customer characteristics with buying patterns can help to target marketing efforts so that the right products are promoted to the right people at the right time.

Producing decision support information generally requires consolidating information from a wide range of different operational systems. In most organisations, the lack of integration of information in operational systems is a major impediment to producing decision support information. Data from different systems can often only be merged and consolidated with significant manual intervention, translation and discrepancy resolution. It is estimated that 80% of the effort in building information systems is in extracting and reconciling data from different sources and converting it to a common format. Lack of data integration also causes problems at the operational level. For example, a customer may notify their local bank branch -where their savings account is held- of a change of address, but their credit card and home loan statements may still be sent to their old address.

Most of the benefits of integration can be achieved by standardising a relatively small percentage of data. The most important data items for integration purposes are *identifiers* —to enable the linking of information from different sources about a single object together- and *coding schemes* —which are used as the basis for aggregating data for management reporting. Following the "80/20 rule", integrating 20% of the data generally leads to 80% of the benefits. Integrating beyond this point may have diminishing returns, and may actually be counterproductive. Total integration is neither realistic nor justified from a business viewpoint.

# Characteristic 6: More Is Not Necessarily Better




In most cases, the more of a certain resource you have (e.g. finances), the better off you are. A common management problem is deciding how to allocate limited resources (e.g. people or finances) among a number of competing causes. However with the increasing use of information technology, information is anything but scarce. In fact, the biggest problem in most organisations today is not the lack of information but the overabundance of information. Psychological evidence shows that humans have a strictly limited capacity for processing information[6]. When the amount of information exceeds these limits, *information overload* ensues and comprehension degrades rapidly. It has been found in practice that decision making performance decreases once the amount of information exceeds a certain optimal point[7].

However an interesting paradox exists here. The law of diminishing marginal utility (from economics) says that the more people have of a given commodity, the lower its value to them. However studies show that the *perceived value of information* to decision makers continues to increase beyond the point of overload. Human decision-makers tend to seek more information than can be optimally processed. Although the excess information leads to reduced performance, it actually leads to increased confidence and satisfaction with the decision by the decision-maker. The explanation for this is that people seek more information than can be efficiently processed in an effort to avoid mistakes and reduce uncertainty. This suggests that people believe that "more information is better" and are not aware of their own information processing limits.

[6] Miller, 1956; Newell and Simon, 1972
[7] O'Reilly, 1980; Driver and Mock, 1975; Jacoby et al, 1974

## Characteristic 7: Information is not Depletable[8]

Most resources are depletable —the more you use, the less you have. However information is self-generating —the more you use it, the more you have. This is because new or *derived* information is often created as a result of summarising, analysing or combining different information sources together. The original information remains and the derived information are added to the existing asset base. Fundamentally, this is why information is not a scarce resource. Techniques like data mining are used specifically to generate new information from existing data.

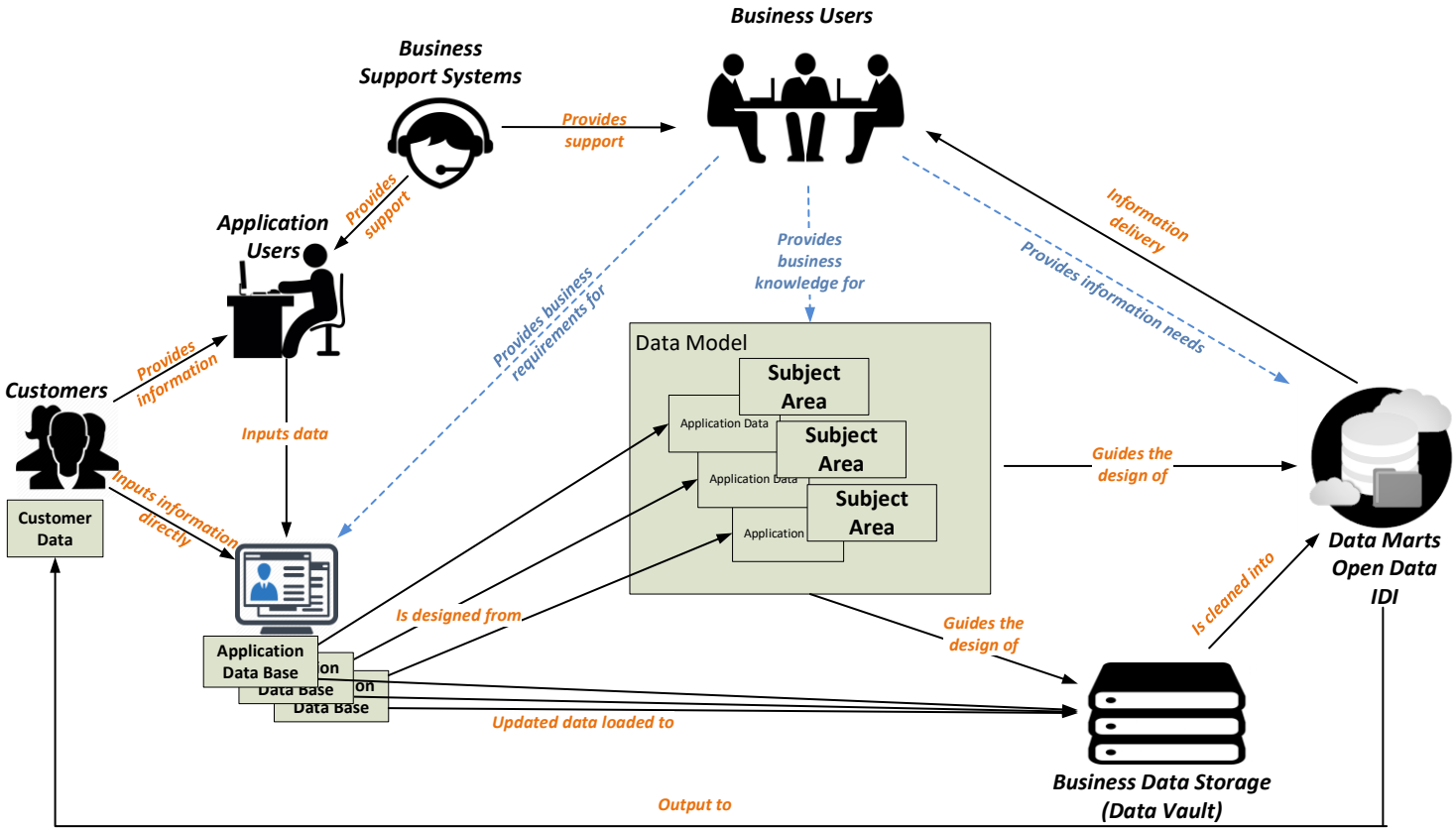
[8] Depletable = to decrease seriously or exhaust the abundance or supply of

# Information Flow

Not all data and information need the same level of quality, depending on the use. Also, not all data and information that is created, received, and used has a high quality level. So, before starting to apply any plans, measurements and controls, you need to have an understanding of the data and information that is handled by the organisation, categorise it and add a value level to each entity.

By improving the quality of data and information throughout its life cycle, organisations will reduce costs, improve productivity and accelerate the delivery of product and services. More accurate information on new and existing product and services will contribute to better utilisation, eliminate the need for multiple measurement of the same service and reduce the number of resources required to do re-work.

Here is a high level view of how data flows through an organisation:



# Principles for High Quality Information

Information Quality is defined as "The fitness for use of the information provided.” Information quality is a relatively new concept to many organisations. With the increase in data collection and storage, and the mining of that data for business uses, the quality of the information produced becomes increasingly important. Bad information can lead an organisation, among other things, to squander resources in ineffective projects, but quality information can identify needs, direct targeted services and create efficiencies in every day work.

"Quality" and “Value” are often perceived as subjective and the quality of information can vary among users and on the use of information. Nevertheless, a high degree of quality increases its objectivity or at least reduces the inter-user subjectivity.

High quality data and information is achieved when it conforms to all of the following principles:

**Accuracy**

Accuracy refers to the exactness of data and information; it cannot have any erroneous elements and must convey the correct message without being misleading. The need for accuracy has a component that relates to its intended use. Without understanding how the data and information will be consumed, ensuring accuracy could be off-target or more costly than necessary. For example, accuracy in healthcare might be more important than in another industry -which is to say, inaccurate data in healthcare could have more serious consequences- and, therefore, justifiably worth higher levels of investment.

Accuracy is best tackled at source. If data is “entered” inaccurately it will create inaccurate information. Further, it may not be able to be corrected.

The best way to address problems in the areas of Accuracy and Consistency is in the major application of “User” education. Users need to be convinced of the importance of data input quality and its contribution to corporate information quality. Inputting any convenient data which satisfies validation rules should become a thing of the past.

The other place that inaccuracies can be discovered is when data is transferred from the Data Vault to a DataMart for onward delivery. At this point cross checking and cross referencing can be done and data can be cleaned or referred for correction.

**Consistency**

Many systems use and collect the same source data and information. Regardless of what source collected the data or where it resides, it should not contradict a value residing in a different source or collected by a different system. Though this can often not be deleted until it is transferred to a DataMart. There must be a stable and steady mechanism to collect and store data and information without contradiction or unwarranted variance.

The form in which data is passed from one system to another must be as consistent as possible within and across agencies and their business partners.

Data Vaults are, by their nature as a simple recording device, not useful for accuracy or consistency checking. This can only be done when transferring out to Data Marts. Data Marts should not be used as initial storage and their provision should solely to be used for basic reporting

**Relevance**

There must be a valid reason to collect the data to justify the effort required, which also means it has to be collected at the right moment in time. So, make sure the right information is available to the right people at the right time.

Relevance is also a function of how well the DataMart are designed and the relevancy of the outputs from them. This is coupled with mechanisms and availability of access facilities for Users.

**Completeness**

Completeness refers to an indication of whether or not all data and information meet current and future business demands.

Incomplete data and information is as dangerous as inaccurate data. Gaps in collection lead to a partial view of the overall picture to be displayed. Without a complete picture of how operations are running, uninformed actions will occur. It’s important to understand the complete set of requirements that constitute a comprehensive set of data to determine whether or not the requirements are being fulfilled.

Relevance and completeness can only be achieved through comprehensive data modelling. Data models do not have to be implemented in their entirety but a complete data model will ensure that there are no unknowns or surprises in the information area.

**Timeliness**

Timeliness refers to the time expectation for the accessibility of data. Data collected too soon or too late could misrepresent a situation and drive inaccurate decisions.

Timeliness is a function of how efficient Operations are at processing data through the system. It is also a function of the mechanisms and availability of the access facilities for Users.

Timeliness can be measured as the time between when data is expected and when it is readily available for use.

Due to the increasing demand for real-time data-driven decisions, timeliness is the most important dimension of quality.

**Provenance**

Provenance refers to the sources of information, such as entities and processes, involved in producing or delivering an artefact. The provenance of information is crucial to making determinations about whether information is trusted, how to integrate diverse information sources, and how to give credit to originators when reusing information.

The basic source of provenance information is the Data Vault which, by its nature, stores information on the source and time of the data that it holds.

The other mechanism for maintaining provenance is the judicious use of Block Chains.

**Value**

Value of information is the amount a decision maker would be willing to pay for information prior to making a decision.

We can collect a lot of information, but it needs to be valuable for the organisation to keep, store, and maintain that information.

In addition to the above principles, there are two guiding principles for achieving high quality data and information: **usefulness** and **trust**. Most executives have two main questions on their mind when evaluating the information they have in front of them: *How useful is my data? Do I trust it?* The more data is seen as being useful and trustworthy, the more its value increases in the eyes of executives and their teams, and this is important for fostering a data-oriented environment.

**Use**

The use of data is defined by its intended purpose. It is dependent on the source data model, goals and objectives of the organisation and the effectiveness of the Data Mart design. Its Value depends on how well it is used.

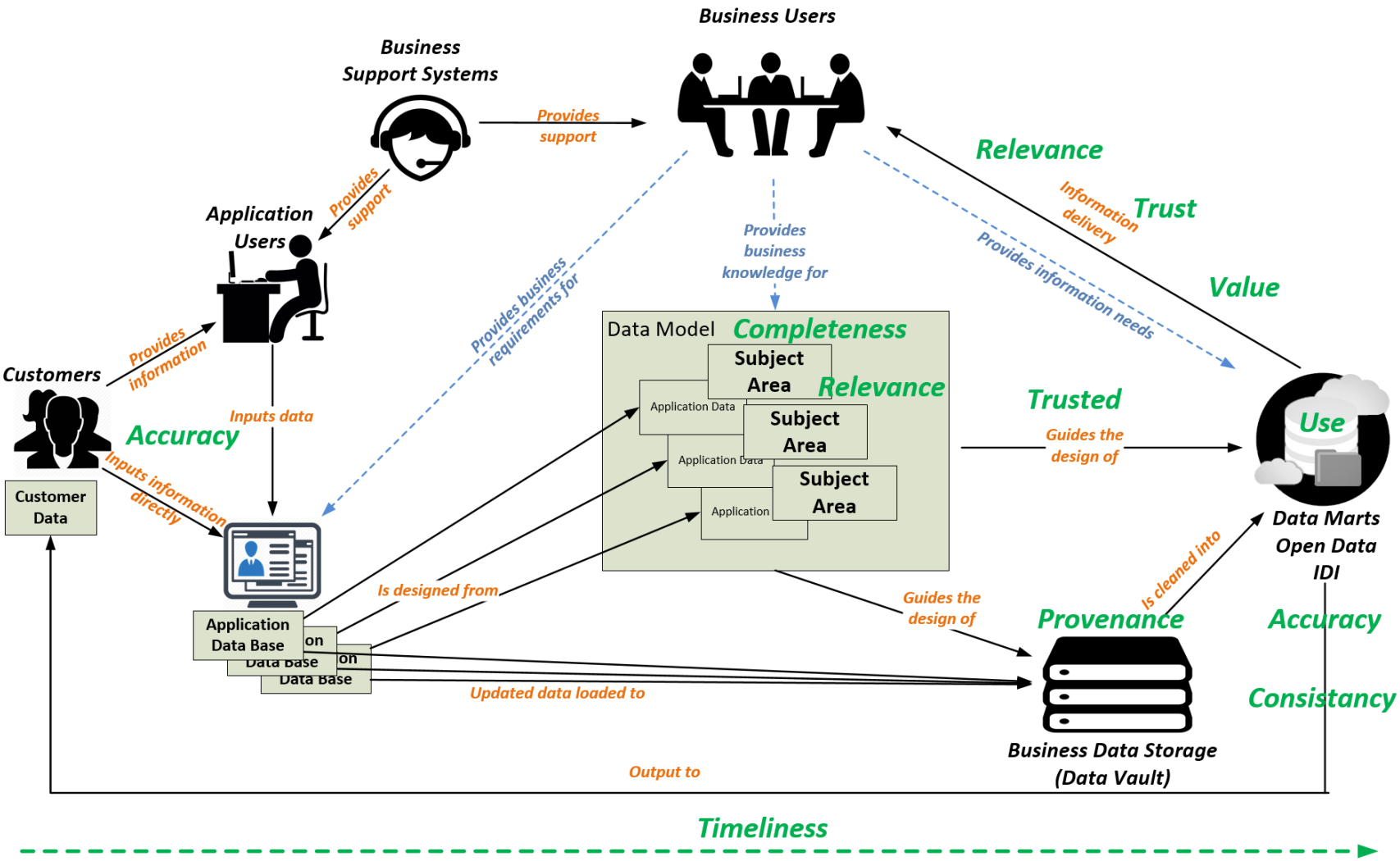
Data needs to be able to answer questions to make decisions. If data is supposed to help measure and optimise performance, it's imperative that the implementation is aligned with business goals and strategy.

Some organisations request much more information than is needed, thinking that it could be useful in the future. The Privacy Act states that 'Personal information must not be collected unless it is necessary to collect the information for that purpose.' and 'Personal information obtained in connection with one purpose must not be used for another.'

**Trusted**

Trust is essential because no manager will act upon data they don't trust. The degree of trust given to the data and information is dependent on the outcomes of the accuracy and consistency reporting from the checks on the data held in the Data Vault.

Here is a visual overview of the principles where they apply the most:



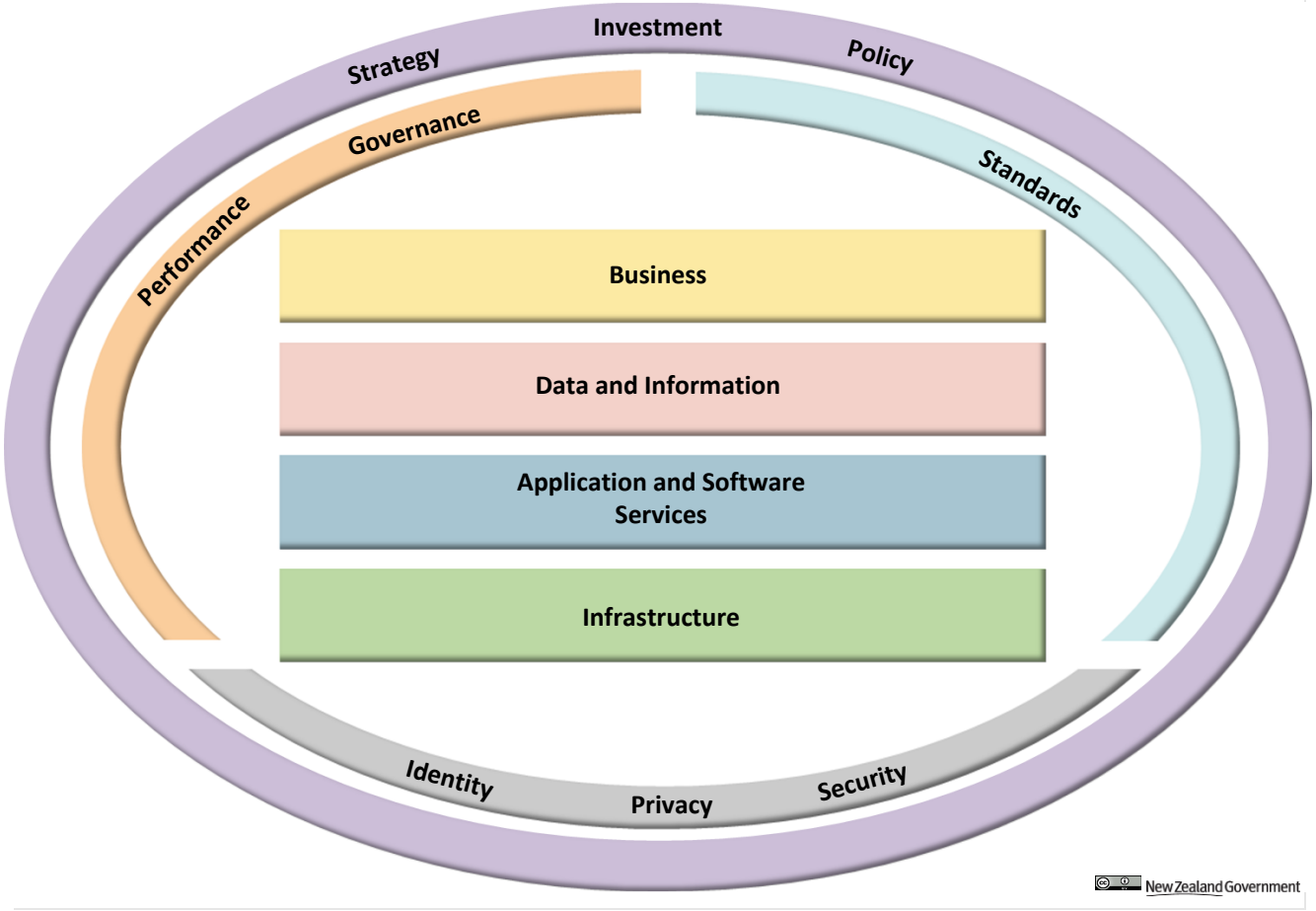
# Government Enterprise Architecture for New Zealand (GEA-NZ)

GEA-NZ architects the structure of a government enterprise. Any major changes alter that structure to achieve goals that are beyond what is already possible.

An enterprise architect needs to understand and be able to:

- Articulate what the existing structure can achieve;
- Assess the structural impact of the changes needed for the future;
- Initiate and design structural changes;
- Make sure investments deliver the structure that is needed for the future.

The Enterprise Architecture will define and design the artefacts needed within the eight dimensions of an organisation.



*There are four governing dimensions:*

- Strategy, Investment, and Policy where you will have the strategic plans, portfolios, capability road maps, etc.
- Governance and Performance where you will find the benchmarks and measurements, maturity assessments and targets.
- Standards with national, international and industry standards that will be used in the organisation.
- Identity, Privacy, and Security with all the laws and regulations, guidelines, possible threats and vulnerabilities and the mitigation plans.

*And four core dimensions:*

- Business which contains a catalogue and strategy around Customers, Channels, Product & Services, People and Organisation, Processes.
- Data and Information which contains the Information Taxonomies, Information Asset Catalogue, Information Quality Framework, and Information Governance Framework.
- Applications & Software Services which contains Application Taxonomy, the Application Asset Catalogue, and the API catalogue.
- Infrastructure which contains Infrastructure Taxonomy and Asset Catalogue.

Each dimension is described in their own section of this document together with the relationship towards the other dimensions and the components needed to insure quality data and information throughout the organisation. Each component contains a description (What), why an organisation needs to have it in place (Why), Who is leading this or is responsible for it (Whom[9]), some examples if needed, and questions an organisation can ask themselves to find out if they already have it in place (can be under another title or within a process).

| GEA-NZ Dimension | Description |
|---|---|
| **Strategy, Investment, and Policy** | Provides linkage between the data and information quality management and strategic goals, policies and investments. |
| **Governance and Performance** | Sets the governance structure and performance measures that needs to be applied across the organisation the ensure quality data and information. |
| **Business** | Represents the business processes, products and services that deliver the outputs of the organisation. |
| **Data and Information** | Here we look at the discovery, describing, managing, sharing and reusing data and information within and across the organisation. |
| **Application and Software Services** | The applications, including 'Software as a Service', that support the business processes of the enterprise. It includes core business applications, COTS corporate applications, and end user computing applications. |
| **Infrastructure** | The technology infrastructures that support the application and business processes of the enterprise. It may include insourced, outsourced or cloud capabilities. |
| **Identity, Privacy, and Security** | Gives a context to the relevant accessibility, security, and privacy around data and information for the organisation. |
| **Standards** | Standards categorises the business, information, and technology standards base for the NZ government. |

[9] See Data and Information Management – Roles and Responsibilities guidelines

# Data and Information Quality Management (DIQM) - Matrix

All the above focus areas and components can be grouped in the eight dimensions of GEA-NZ. The following matrix provides an overview of the components. Each component is hyper-linked to the relevant section in this document where it is described.

| Dimension / Focus Area | Strategy, Investment, and Policy | Governance and Performance | Business | Data & Information | Application and Software Service | Infrastructure | Privacy, Security, and Identity | Standard |
|---|---|---|---|---|---|---|---|---|
| **Plan** | Executive Sponsorship<br>Goals & Objectives<br>Plans & Roadmaps<br>Roles & Responsibilities<br>Terms of Reference | Guiding Principles<br>Success Measures<br>Improvement Plans | Staff Roles & Skills<br>Product & Service Life-cycle<br>Revision & Change | Data Stewards<br>Data & Information Quality Improvement Plan | Application Ownership Model<br>Application Portfolio<br>User Interfaces | Infrastructure Ownership Model<br>External Publication<br>Internal Publication | Privacy & Security Management | Standard Management |
| | | | Initial Data Entry & Setup<br>Ongoing Data Maintenance | | Unified Data Repository<br>Data & Information Interoperability | | | |
| | | | | Architecture & Design | | | | |
| **Document / Record** | Goals & Objectives<br>Plans & Roadmaps<br>Roles & Responsibilities<br>Data & Information Quality Assurance<br>Data & Information Change Management | Data & Information Governance Model<br>Success & Quality Measures<br>Performance Metrics<br>Assessment Procedures<br>Assessment Results<br>Improvement Plans<br>Audit Procedures | Customer Criteria<br>Channel Strategy<br>Product & Service Documentation<br>Governance Organisational Structure<br>Delivery Methodology<br>Customer Feedback & Follow-up<br>Personal Objectives | Information Asset Catalogue<br>Data & Information Taxonomy<br>Data & Information Quality Management | Application Asset Catalogue<br>Application & software Service Taxonomy<br>API Catalogue<br>Application Manuals, Guides, & Instructions | Infrastructure Asset Catalogue<br>Infrastructure Taxonomy<br>Operating Procedures | Security & Privacy Policy, Regulations & Laws<br>Threat & Vulnerability Model<br>Risk Management Procedures | National & International Standards |
| **Execute** | Education & Awareness<br>Data & Information Change Management | Education & Awareness<br>Performance Management | Education & Awareness<br>Customer Feedback Resolution<br>Product & Service Management | Education & Awareness<br>Data Cleansing<br>Data Profiling<br>Data Validation | Education & Awareness<br>Application & software Service Change Management | Education & Awareness<br>Infrastructure Change Management | Education & Awareness<br>Privacy & Security Management<br>Risk Management | Education & Awareness<br>Standard Management |
| **Control / Monitor / Evaluate** | Organisational Capability Review | Performance Controls<br>Service Level Controls<br>Data & Information Audits | Internal & External Feedback Controls<br>Review of Personal Objectives<br>Product & Service Controls<br>Workflow Controls | Data & Information Quality Controls<br>Monitor Impact of Inadequate, Missing, or Wrong Data | Application & software Service Validations<br>Application Service Level Controls<br>Compliance Audits | Infrastructure Issue Management<br>Infrastructure Service Levels Control<br>Compliance Audits | Privacy & Security Validations<br>Compliance Audits | Standard Validations<br>Compliance Audits |

# Focus Areas

In this document, if we talk about Focus Area[10], we mean a point upon which attention, activity, etc., is directed or concentrated. The four focus areas are: Plan, Document / Record, Execute, and Control / Monitor / Evaluate.

## Plan

To *Plan* is typically to create a list of steps with timing and resources, used to achieve an objective to do something. It is commonly understood as a temporal set of intended actions through which one expects to achieve a goal. Plans can be formal or informal.

This icon will be used to indicate a planning component on a diagram. 

The most popular ways to describe plans are by their breadth, time frame, and specificity; however, these planning classifications are not independent of one another. For instance, there is a close relationship between the short- and long-term categories and the strategic and operational categories. There are several Plan activities that need to be considered to make sure the data and information an organisation uses for decision making is of high quality.

## Document / Record

To *Document* / *Record* is to write, photograph, or capture information in any form (structured or unstructured) that provides evidence or serves as an official record[11].

This icon will be used to indicate a document / record component on a diagram. 

To make sure that all employees know the guidelines, processes, workflows, they need to be documented. These documents are also used to evaluate monitor, and control the processes.

## Execute

To *Execute* is to put a plan or course of actions into effect.

This icon will be used to indicate an execute component on a diagram. 

There are actions that need to be executed to achieve high quality data and information which are described in this document.

## Control / Monitor / Evaluate

To *Control* / *Monitor* / *Evaluate* is to exercise restraining or directing influence over the execution of an action, to regularly check something or watch someone in order to find out what is happening, and to determine the significance, worth, or quality of the results.

This icon will be used to indicate a control / monitor / evaluate component on a diagram. 

Besides planning, documenting, and executing tasks there needs to be mechanisms to ensure that we know the data and information is of high quality. Additionally to be able to continuously improve the handling of data and information so there is a high trust in the integrity and liability of information assets.

---

[10] Diagrams for each focus area with the components can be found in Appendix A.

[11] An official record or original copy is an original document that is legally recognized and thus ensuring the quality of a fact when it is established.

# Strategy, Investment, and Policy

## Description

The *Strategy, Investment, and Policy* dimension provides linkage between the data and information quality management and strategic goals, policies and investments.

At an AoG level, it sets out government goals, objectives and roadmaps to achieve the AoG vision. By creating a consolidated view of government transformation, we identify new opportunities to improve and share government services across agencies and drive efficiency, effectiveness, and system transformation across government.

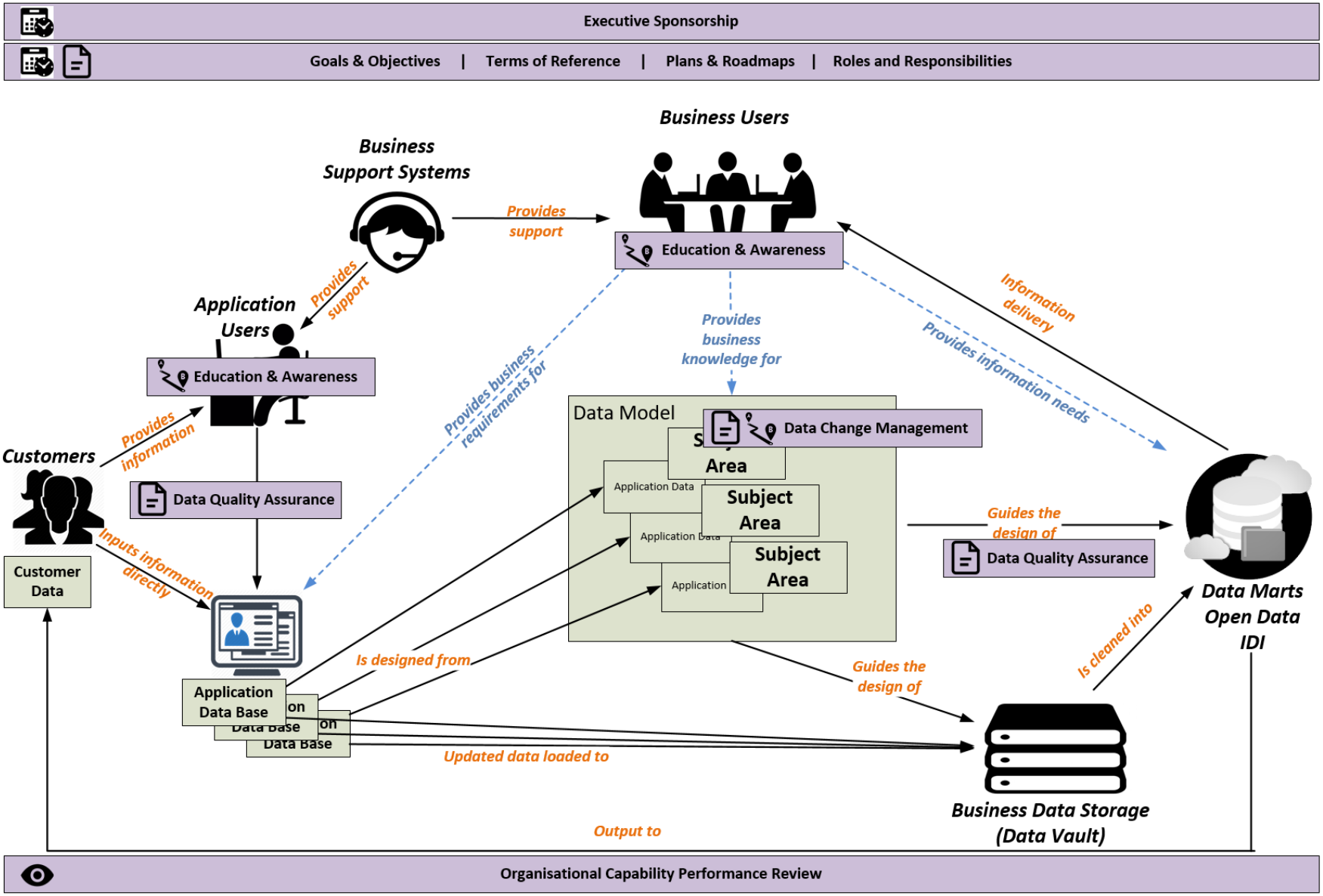
At an agency level, it sets out the agency's goals and objectives defined in the agency's *Four Year Plan, Information Systems Strategy Plan,* and *Statement of Intent*. These will drive the change initiatives within the agency. Agencies should map their programmes directly against the AoG Strategy and the Better Public Services Results to identify where they can adopt common capabilities, share services and collaborate with other agencies to improve the overall customer experience, the services and reduce costs.

## Context and Relationships

| | | |
|---|---|---|
| **Strategy, Investment, and Policy** | sets the strategic goals, objectives, values, and ethics that drives the governance models and performance frameworks | **Governance and Performance** |
| | sets the objectives and roadmaps for business improvement and transformation | **Business** |
| | sets goals for data and information quality, governance and sharing. Defines the guidelines for information asset management | **Data and Information** |
| | sets strategic context for the evolution of the business application portfolio, including efficiencies through sharing, reuse and the adoption of common capabilities. Defines the guidelines for application asset management, and APIs | **Application and Software Services** |
| | defines the guidelines for infrastructure asset management and efficiency through sharing, reuse and the adoption of common capabilities | **Infrastructure** |
| | sets the expectations for identity, ethnicity, privacy, and security | **Identity, Privacy, and Security** |
| | sets the expectations for the use and adoption of standards across government | **Standards** |

# Components Overview

This diagram gives you a visual overview of the different components within the *Strategy, Investment, and Policy* dimension.



# Components

## Plan

### *Executive Sponsorship*

**What** - Secure endorsement from executive for active management of data and information quality in the organisation.

**Why** – Meaningful action around data and information quality will require the organisation to commit to make the necessary resource investments and cultural changes. Without direct and clear executive sponsorship it will be very difficult to create the required conditions.

**Whom –** Executive Leadership Team, Executive Sponsor are responsible for setting up the organisation to ensure quality information.

**Examples:**

- Create and deliver a presentation for executives to articulate the value proposition of action on data and information quality.
- Show how managing data and information quality can directly support the mission and vision of the organisation; communicate the importance and impact of data and information quality within and across agencies and their business partners. Think operationally as well as analytically.

**Questions to ask:**

- Does the executives talk about quality of data and information? Is that part of their strategy?
- Do the executives know about the risks associated with poor data quality?

### *Goals & Objectives*

**What** - Develop and/or update strategic goals and objectives, but also the value and ethics, around appropriate quality data and information.

**Why** - A desired state needs to be articulated or the people within the organisation will not be headed towards the same place.

**Whom:**

- Executive Leadership Team responsible for defining the organisation's goals and objectives.
- Communication group is responsible for making people aware of the goals and objectives.

**Questions to ask:**

- Do the goals & objectives defined conform to the SMART (specific, measurable, attainable, relevant, and time-bound) criteria?
- Are the goals around data and information quality included in the executive's performance objectives?
- Does the DIQM documentation include manual, objectives and targets?

### *Plans & Roadmaps*

**What** - Define strategic plans and roadmaps at government, sector and agency level.

**Why** - Formal documented roadmaps are essential to allow the organisation to follow the same direction at government, sector and agency level.

**Whom:**

- Executive Leadership Team, Executive Sponsor are responsible for defines the strategic plans and roadmaps
- Communication group are responsible to ensure everyone is aware of those plans and roadmaps
- Line managers and project managers are responsible for the implementation of those plans.

**Example** – Information System Strategy Plan (ISSP).

**Questions to ask:**

- Does the 4 year plan include the implementation of a DIQM?
- Are these artefacts stored in a repository that can be accessed by anyone within the organisation?

***Roles & Responsibilities***

**What** - Define clear roles and responsibilities and ensure they are understood and known within the organisation.

**Why** - Clarity is needed to realise value from information. Clear accountabilities and responsibilities need to be established.

**Whom:**

- Executive Leadership Team are responsible for defining roles and responsibilities
- HR is responsible for creating job descriptions and hiring or uplifting skills to align with those roles and responsibilities
- Chief Privacy Officer, Chief Security Officer, and line managers contribute to defining responsibilities and skills needed.

**Example –** See the roles and responsibilities guideline[12]

**Questions to ask:**

- Do the managers who are appointed have the responsibility and authority to ensure that processes needed for the DIQM are established, implemented and maintained?
- Are the quality responsibilities for data and information of the leaders balanced with their reach within the organisation and that support exists for them across multiple levels?
- Are the roles and responsibilities been recorded and communicated throughout the organisation through policies, performance development, etc.?
- Are there KPIs for all key players?

***Terms of Reference***

**What** - Define the terms of reference for data governance that support and guide the DIQM to appropriately use and reuse data.

**Why** - In order to maintain, agree, and take ownership of continuous improvements, it is important to ensure that the guiding principles and policies of the DIQM can evolve along with the organisation; for that purpose, it is necessary to manage and continuously update those elements.

**Whom –** Data stewards / Executive Leadership Team / Governance group to support the development of governance.

**Questions to ask:**

- Is data and information quality part of the organisation's policy?
- How does the organisation communicate the policies to all staff, vendors, and customers?
- Is there a clear internal responsibility for the different elements that need to be maintained?
- Is everyone within the organisation aware of the importance of adopting all policy changes to achieve appropriate quality data and information?

[12] "Data and Information Management - Roles and Responsibilities" – this guide is available on PSI.

## Document / Record

### *Goals & Objectives*

**What** - Record of all strategic and guiding goals and objectives, but also the values, ethics, and principles at government, sector and agency level.

**Why** - Formal documented goals, objectives, values, ethics, and principles are essential to allow the organisation to refer back to the original vision and motivators in order to remain on scope.

**Whom –** Executive Leadership Team

**Questions to ask:**

- Does the DIQM documentation include goals and principles?
- To what extent are the objectives on DIQM measurable?
- Can this information be accessed by anyone within the organisation?

### *Plans & Roadmaps*

**What** - Record of all strategic plans and roadmaps at government, sector and agency level.

**Why** - Formal documented roadmaps are essential to allow the organisation to follow the same direction, and to control and audit appropriate role-based access.

**Whom –** Executive Leadership Team

**Example** – Information System Strategy Plan (ISSP), including cloud, ECM roadmap, BI / Analytics roadmap.

**Questions to ask:**

- Does the organisation's roadmap include the implementation of a DIQM?
- Are these plans stored in a repository that can be accessed by anyone within the organisation?

### *Roles & Responsibilities*

**What** – Record the roles and responsibilities and ensure they are understood and known within the organisation.

**Why** - Clarity is needed in case controversies arise or decisions need to be taken.

**Whom:**

- HR is responsible for describing and recording job descriptions and hiring or uplifting skills to align with those roles and responsibilities
- Chief Privacy Officer, Chief Security Officer, and line managers contribute to defining responsibilities and skills needed.

**Example -** Description of DIQM responsibilities.

| *R – Responsible*<br>*A – Accountable*<br>*S – Support*<br>*C – Consult*<br>*I - Inform* | Stakeholders | Data Custodian | Data Steward | ICT Management | Development | Communications |
|---|---|---|---|---|---|---|
| Activity A | C | R | | | | |
| Activity B | CS | R | S | S | | S |
| Activity C | SI | CA | R | S | C | C |

**Questions to ask:**

- Do the managers who are appointed have the responsibility and authority to ensure that processes needed for the DIQM are established, implemented and maintained?
- Are the quality responsibilities for data and information of the leaders balanced with their reach within the organisation and that support exists for them across multiple levels?
- Has the division of responsibilities been recorded and communicated throughout the organisation?

### *Data & Information Quality Assurance (DIQA)*

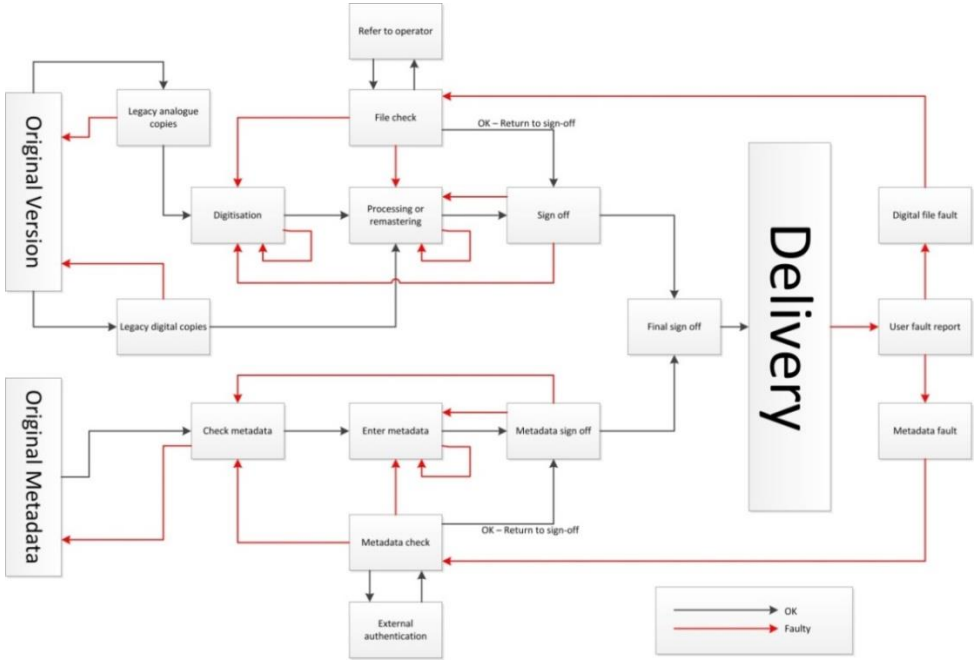
**What** - Record of all processes for profiling data to discover inconsistencies and other anomalies in the data, as well as performing data cleansing activities, and ensuring efficiency and effectiveness of the data and information.

**Why** - Formal documented DQA processes are essential to periodically look at the organisation's data processes to ensure that they are still up-to-date and that the data and information used and produced is still fit for purpose.

**Whom:**

- Data custodians are responsible for describing and recording all quality assurance processes
- Standard experts and auditors contribute to defining those processes.
- Executive Leadership team is responsible for the correctness of those processes.

**Example –** One of the artefacts within the DQA could be the DQA workflow.




**Questions to ask:**

- How often does the organisation prepare for a DQA Audit?
- Who reviews and approves the DQA processes?
- What criteria does the organisation utilize to do DQA?
- Is the DQA communicated throughout the organisation and accessible by anyone within the organisation?

### *Data & Information Change Management*

**What** - Record of all processes to manage changes to data and information as part of the overall system change process.

**Why** - Formal documented data and information change management processes contributes to quicker and better adoption of new procedures within the organisation to achieve high quality data and information.

**Whom:**

- Architects are responsible for the design of the changes needed
- Change managers are responsible for defining the processes and managing changes

**Example –** Documentation on the different phases of data and information change management and impact assessments:

- Phase 1 – Preparing for data and information change: Preparation, assessment and strategy development
- Phase 2 – Managing data and information change: Detailed planning and data change management implementation
- Phase 3 – Reinforcing data and information change: Data gathering, corrective action and recognition.

**Questions to ask:**

- Does the organisation's overall change management process include data and information?
- Include section for data and information into generic project templates.
- Does the organisation know where, when and how data changes throughout their organisation?

## Execute

### *Education & Awareness*

**What** - Conduct the necessary education programmes needed to ensure people understand what data and information quality is, what the impact and importance is to the organisation, that it contributes to the good outcomes for the public, etc. Engage in communications across the organisation to show how these initiatives support the main organisational objectives, mission and vision to improve data and information quality. Should be part of information as an asset training.

**Why** - There must be clear understanding of the concept and role that data and information quality has in supporting good results, good decision making, good customer outcomes, etc.

**Whom:**

- SLT/ELT to fund the training and awareness.
- CDIO, HR, people managers, business unit leads, data stewards to define what training is needed.
- Separate business units will need to take responsibility for identifying educational needs and ensuring relevant staff gets trained as needed.
- Data stewards establish the requirements:
    - For 'fit for purpose'
    - To connect those to capability requirements
    - Identify where quality can be improved / delivered
    - System design and functionalities
    - Individual capabilities.
- Communication manager to be responsible for the awareness and communications.
- Architects to define the changes.
- Staff to attend training and to give feedback.

**Questions to ask:**

- Is data and information quality linked to daily activities?
- Is there an ongoing internal communication process on any aspect of data and information quality, to create awareness within the organisation on the importance of providing highly accurate data and information?
- Is there a process in place to keep the organisation up-to-date regarding the requirements to achieve high quality data and information?
- To what extent does the organisation maintain appropriate records of education, training, skills, and experience?
- Are the results of audits shared within the organisation?
- Are the results on performance indicators communicated within the organisation and if applicable to other organisations and business partners?

### *Data & Information Change Management*

**What** - Establish a process to manage data and information changes as part of the organisation's change management process.

**Why** - Having a good process for data and information changes contributes to quicker and better adoption of new procedures within the organisation to achieve high quality data and information.

**Whom:**

- Architects are responsible for the design of the changes needed
- Change managers are responsible for defining the processes and managing changes

**Example –** The different phases in data and information change management have these processes:

- Phase 1 – Preparing for data and information changes:
  - Develop a Request for Change (RfC) specifically focussed on data changes.
  - Do an impact assessment
  - Obtain strategic acceptance
- Phase 2 – Managing data and information changes:
  - Create a detailed plan and activities to implement the changes
  - Apply the data change management
- Phase 3 – Reinforcing data and information changes:
  - Gather data and report the result of the changes
  - Execute periodic audits
  - Apply corrective actions and recognition

**Questions to ask:**

- Does the organisation have a procedure implemented to facilitate changes to the DIQM?

## Control / Monitor / Evaluate

### *Organisational Capability Review*

**What** - Conduct periodical reviews of the documentation of the data and information governance structure, process flow, roles and responsibilities and ongoing training programmes to evaluate the effectiveness and/or to define improvements.

**Why** - Continuous improvement is fundamental to good process. The data and information governance structure and ToR needs to be updated periodically to catch up with changes and variations that may appear naturally through the years.

**Whom:**

- Executive Leadership Team responsible for defining the organisational capabilities.
- Risk and assurance group and auditors are responsible conducting reviews

**Example** – Yearly holistic review of objectives and performance; auditing compliance of the process to policies/goals.

**Questions to ask:**

- Who is responsible for periodically reviewing documentation and processes?
- Does the organisation periodically audit the DIQM structure? And are results of audits actioned?
- Are the results of these audits shared within the organisation?
- Is there risk and assurance oversight?
- Are the review period balanced so they do not become irrelevant or obsolete?
- Is the ownership of the data within the organisation defined, documented, implemented and/or regularly reviewed?
- To what extent do the people who manage data and information quality have the right talents and skills set?
- To what extent are people working with master data part of an ongoing training program?
- To what extent does the organisation maintain records of education, training, skills, and experience?
- To what extent does the organisation evaluate the effectiveness of data handling practices to increase the competencies of personnel regarding data quality?
- Are audit results reported to the business and are the used for decision making?
- Based on the analysis of performance indicators, are the necessary follow-up actions executed regarding individual staff, business units, processes, governance arrangements, etc.?

# Governance and Performance

## Description

The *Governance and Performance* dimension sets the governance structure and performance measures that needs to be applied across the organisation the ensure quality data and information.

At an AoG level, it provides targets and performance measures that quantify the intended action plan and BPS benefits. It also includes the capability maturity models that are provided for agencies to measure and improve their performance.

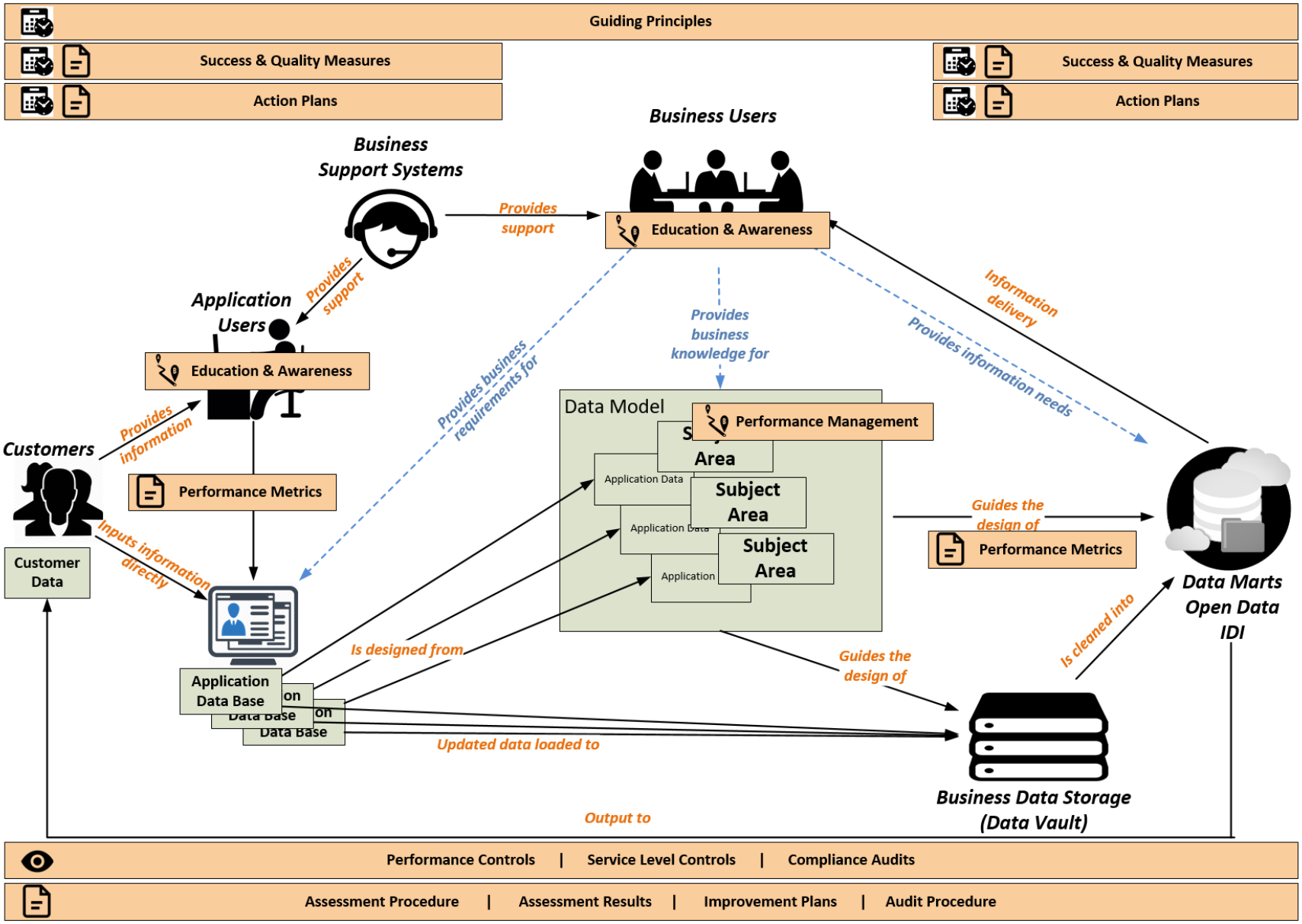
At an agency level, it sets out the improvement plan and Governance and Performance measurements to optimise their services towards internal and external customers, to improve their collaboration with other agencies and 3rd parties, and to improve their information and technology assets.

## Context and Relationships

| | | |
|---|---|---|
| **Governance and Performance** | describes the governance structure, performance measures, risk and assurance, and compliance to achieve the strategic goals and the benefit realisation | **Strategy, Investment, and Policy** |
| | provides measurements and controls for business services, processes, people capabilities and performance, and business capabilities | **Business** |
| | provides measurements and controls for data and information quality, governance and sharing | **Data and Information** |
| | provides measurements and controls for application and software services' cost benefits, sharing, reuse and effectiveness | **Application and Software Services** |
| | provides measurements and controls for infrastructure cost benefits, sharing, reuse and effectiveness | **Infrastructure** |
| | provides measurement, controls, risk and assurance, and compliance to determine effectiveness of identity, privacy, and security | **Identity, Privacy, and Security** |
| | provides measurements for compliance of standards | **Standards** |

# Components Overview

This diagram gives you a visual overview of the different components within the *Governance and Performance* dimension.



# Components

## Plan

### *Guiding Principles*

**What** – Develop, plan and establish the guiding principles that will direct the execution of the DIQM.

**Why** – Guiding principles will help the organisation stay on course, keep going, and make better and faster decisions.

**Whom –** Governance group is responsible for the development and planning of the principles.

**Example** - A list of core guiding principles linked to overarching principles.

**Questions to ask:**

- Does the organisation have a data and information quality as part of their policy?
- Is there an ongoing internal communication process on any aspect of data and information quality, to create awareness within the organisation on the importance of providing highly accurate data and information?

### *Success Measures*

**What** – Define the criteria, for the different dimensions, that establish what is considered successful performance within the measurable objectives.

**Why** – Having a measure of what represents satisfactory performance will not only give more depth to the monitoring of goals and KPI's but it will also allow the organisation to define when certain maturity has been achieved in the roadmap allowing it to progress to the next stages.

**Whom –** Governance group and auditors are responsible for identifying success measures.

**Example** – Undertake an information audit and provide a benchmark.

**Questions to ask:**

- To what extent are the objectives on DIQM measurable? Are they fit for purpose?
- Are the successful performance measures realistic but ambitious enough so they represent a leap forward for the organisation?
- Are they acted on?

### *Improvement Plans*

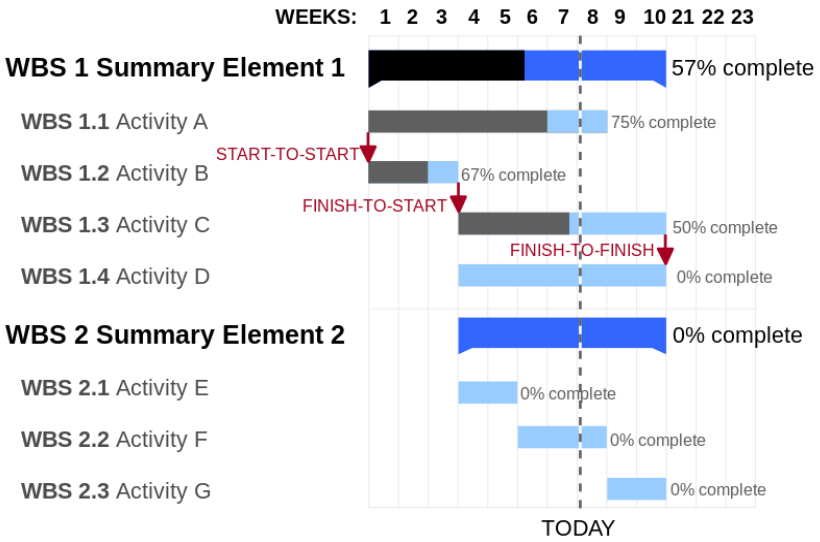
**What** - Develop plans for the implementation of improvement measures and programmes.

**Why** - Formalised planning is necessary for the successful execution of any improvement actions.

**Whom:**

- Executive Leadership Team responsible for defining action plans.
- Governance group contributes to the definition and is responsible for the implementation of action plans

**Example -** A Gantt chart can be used scheduling tasks. This Gantt chart shows three kinds of schedule dependencies (in red) and percent complete indications (Source: Wikipedia).




**Questions to ask:**

- Is there a standardised approach to the development of actions plans; consider that the same planning criteria may be used for anything from new training programmes to system implementations?
- To what extent does the documentation of this DIQM structure contain the DIQM action plans?
- Do the audits result in documented, communicated and implemented action plans?

## Document / Record

***Data & Information Governance Model***

**What** - Create formal documentation of the data and information governance structure and roles and responsibilities within the DIQM.

**Why** - Having a clear charter for the data and information governance structure will make the operation easier and will give legitimacy to all actions within the process.

**Whom:**

- Business and technology leaders are responsible for defining a governance model.
- Governance group contributes to the definition and is responsible for the implementation of a governance model.

**Example –** Data and Information Governance Framework[13]

**Questions to ask:**

- Is the Data and Information governance structure available to everyone and is it adjusted as needed depending of the feedback of the process?
- Is the ownership of the data and information within the organisation defined, documented, implemented and/or regularly reviewed?

[13] See the Data and Information Governance Framework developed by the GCIO's Government Enterprise Architect team.

- Does the organisation periodically audit the DIQM? Are the results of these audits shared within the organisation?
- Are the data and information classified?

***Success & Quality Measures***

**What** – Record all success and quality measures needed to achieve high quality data and information within and across organisations.

**Why** - Formal documented measurements allows the organisation to refer back to the original vision and objectives in order to remain on scope.

**Whom –** Governance group and auditors are responsible for recording, storing, and the accessibility of the measures.

**Example** – Data and information quality measurements.

**Questions to ask:**
- Are the success and quality measure available to everyone within the organisation?
- Does the documentation include DIQM manual, objectives and targets?
- Are there different success measures for the privacy and security of data and information?
- To what extent is the DIQM measurable?

***Performance Metrics***

**What** – Document the specific KPI's and metrics that are to be used to measure the performance of DIQM activities.

**Why** - Having clear performance expectations and measurements will provide a context for people and will allow the organisation to always maintain a consistent level of performance across processes.

**Whom –** Governance group and auditors are responsible for recording, storing, and the accessibility of the metrics.

**Example** – Performance targets for new product and services.

**Questions to ask:**
- Does the organisation have any operational processes in place to audit, monitor and improve the accuracy of qualitative (non-dimension) attributes, such as descriptions, names, target groups, etc..?
- Does the organisation make use of standardised monitoring and measuring processes?
- Has the organisation got operational processes in place for data and information generation?
- Are the results of audits shared with the people in the organisation as a means to involve them more in the process; people committed to a goal will certainly strive for better results?

***Assessment Procedures***

**What** – Assessment procedures are a methodology used to assess and compare data and information performance, quality and success measures within an organisation.

**Why** - Provide accurate and reliable assessments of data and information performances, quality and success that are needed to underpin data and information quality initiatives.

**Whom –** Governance group and auditors are responsible for defining, recording, storing, and the accessibility of assessment procedures.

**Example** – Flowchart of assessment modules by product and service phases.

**Questions to ask:**
- Does the organisation has any operational assessment processes in place and documented to assess and compare measurements?
- Is the assessment procedure available to everyone within the organisation?

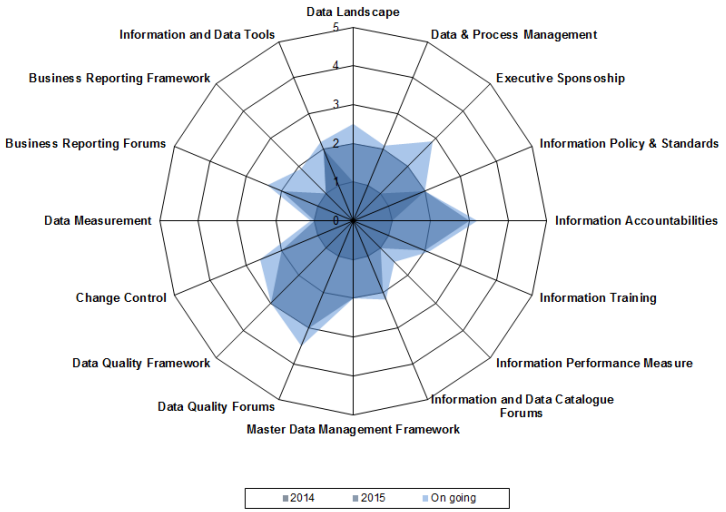
### *Assessment Results*

**What** – Results of the assessment procedures on data and information performance, quality and success measures within an organisation.

**Why** – Having a history of the results available will help the organisation to see the impact of certain initiatives to improve the quality of data and information and to plan the next stage to achieve high quality data and information within and across organisations. It also aids in the continuation of having high quality data and information.

**Whom –** Auditors are responsible for producing and documenting assessment results.

**Example –** Web chart which shows the progress and where improvement is still needed.




**Questions to ask:**

- Does the organisation keep a history of the assessments?
- Are the impacts of data and information change management included and identifiable in the assessments?
- Are those results used to plan initiatives to improve the quality of data and information within and across the organisation?

### *Improvement Plans*

**What** – Document a set of techniques and tools to improve the data and information quality of process outputs by identifying and removing the causes of errors and minimizing variability in business processes.

**Why** – Formal documented improvement plans allows the organisation to refer back to the original vision and objectives in order to remain on scope to achieve high quality data and information.

**Whom:**

- Business and technology leaders are responsible for defining a improvement plans.
- Governance group contributes to identifying improvements
- Change managers and line managers are responsible for the implementation of improvement plans.

**Example** – Strategic outline for improvement: Goals -> Strategy -> Areas for Improvement -> Projects.

**Questions to ask:**

- Does the improvement plan align with the strategic vision of the organisation?
- Are the improvement plans available to everyone within the organisation?

### *Audit Procedures*

**What** – Define and document a standardised protocol for the execution of internal audits of the performance of the DIQM and its data and information output.

**Why** – Formal rules and procedures to conduct evaluations and audits ensure reliable and objective results.

**Whom** – Auditors and the governance group are responsible for defining audit procedures.

**Example** – Product inspection procedure of the Data and Information Quality Framework.

**Questions to ask:**

- Do the audits result in documented, communicated and implemented action plans?
- Is there a process for determining the criteria, scope, frequency and methods for executing internal audits of the DIQM system?
- Are these audit guidelines in line with the audit criteria used for other areas of the organisation?
- Is the audit methodology repeatable?

## Execute

### *Education & Awareness*

**What** - Conduct the necessary education programmes needed to ensure people understand what data and information performance, quality and success measurements are, where they are measured and what their responsibilities are to achieve high quality data and information within and across organisations. Engage in communications across the organisation to show how the data and information performance, quality and success measurements support the main organisational objectives, mission and vision to improve data and information quality.

**Why** - There must be clear understanding of why the organisation must have high quality data and information and how it is measured in order to promote higher acceptance.

**Whom:**

- SLT/ELT to fund the training and awareness.
- CDIO, HR, people managers, business unit leads, data stewards to define what training is needed.
- Separate business units will need to take responsibility for identifying educational needs and ensuring relevant staff gets trained as needed.
- Data stewards establish the requirements:
    - For ‘fit for purpose’
    - To connect those to capability requirements
    - Identify where quality can be improved / delivered
    - System design and functionalities
    - Individual capabilities.
- Communication manager to be responsible for the awareness and communications.
- Architects to define the changes.
- Staff to attend training and to give feedback.

**Questions to ask:**

- How do the measurements impact the daily activities?
- Is there an ongoing internal communication process on any aspect of data and information measurements, to create awareness within the organisation on the importance of providing

highly accurate information?
- Is there a process in place to keep the organisation up-to-date regarding the requirements to achieve high quality data and information?
- To what extent does the organisation maintain appropriate records of education, training, skills, and experience?
- Are the results of audits shared within the organisation?
- Are the results on performance indicators communicated within the organisation and if applicable to other organisations and business partners?

***Performance Management***

**What** - Carry out activities to measure and manage performance of the DIQM; the focus of this performance management should be to continuously evaluate the performance metrics and conduct improvements/corrective actions whenever necessary to achieve the desired performance levels.

**Why** - Formalising and externalising performance management will provide the organisation with an objective and effective way to monitor and improve the performance of the DIQM.

**Whom:**
- CDIO, HR, people managers, business unit leads, data stewards to define performance management.
- Separate business units will need to take responsibility for executing performance management
- Data stewards establish the requirements:
    - For 'fit for purpose'
    - To connect those to capability requirements
    - Identify where quality can be improved / delivered
    - System design and functionalities
    - Individual capabilities.
- Communication manager to be responsible for the awareness and communications.
- Architects to define changes.

**Example** – Protocol for periodical performance metrics revisions.

**Questions to ask:**
- To what extent is the policy management applied within the organisation?
- Does the organisation have approved processes and procedures for data input?
- Does the organisation periodically review the DIQM and performance on data?

## Control / Monitor / Evaluate

***Performance Controls***

**What** - Monitor effectiveness of the process and its data and information to the expected performance criteria across the DIQM in order to measure the degree in which the organisation adheres to the defined policies and standards.

**Why** - Successful execution of a DIQM system depends on ensuring that the different checks that have been built into the workflows and processes are applied and that data and information are controlled and monitored to ensure the output conforms to the defined performance requirements.

**Whom –** Governance group and auditors are responsible for monitoring and auditing performance.

**Example** – Implementing consistency checks for data and information.

**Questions to ask:**

- Are the checks for the data and information performance pragmatic and are they based on the performance metrics defined so that a successful monitoring depends on having KPI's that can be tracked and measured in an efficient way?
- Is there a process in place to identify and communicate changes/corrections to the data and information?
- Does the organisation have approved processes and procedures for data input?
- Has the organisation established, maintained, and documented the operational processes needed for internal data publishing?
- Have critical success factors (key elements that ensure a satisfactory performance) been established in the processes for external data publishing?
- Are any changes in data relayed to any other parties who may have received it?

***Service Level Controls***

**What** - Track the performance on the agreed KPI's of service levels offered to other organisations and business partners and vendors.

**Why** - While service level agreements (SLA's) may not specifically cover data and information quality, the performance on service level goals is a valuable insight into the impact that poor quality data is having on the organisation's performance.

**Whom –** Contractors, contract management are responsible for SLAs.

**Example** – Controlling late metrics for deliveries, order processing, etc.

**Questions to ask:**

- Are the key data asset identified that support SLA objectives and goals; that gives the organisation visibility into the information whose improvement can result in direct benefits for the customers, value purpose and impacted outcomes?
- Does the organisation make use of standardised monitoring and measuring processes?
- Which monitoring methods on master data management are used within the organisation to evaluate and track the DIQM processes and procedures?
- Are performance indicators defined for each process in the DIQM system?
- To what extent are these performance indicators tracked and communicated?
- To what extent are all corrections suitable, made in both the product master data and the published data?
- Based on the results of the analysis of performance indicators, are the necessary follow-up actions executed?

***Data & Information Audits***

**What** - Conducting periodical audits to verify that procedures are followed as defined within the DIQM.

**Why** - A process is only as effective as the people executing it want to make it: if the established protocols and procedures are not consistently applied and followed the DIQM system may fail to achieve its goals. Conducting periodical audits is key to guarantee that results are met.

**Whom –** Governance group and auditors are responsible for conducting audits.

**Example** – Audit on application of defined policies, processes and roles across the organisation.

**Questions to ask:**

- Does the organisation periodically audit the DIQM structure?
- To what extent is the data quality policy applied within the organisation?
- Does the organisation review the procedures for data input and creation for adequacy?
- Which monitoring methods on master data management are used within the organisation to evaluate and track the DIQM processes and procedures?
- Based on the results of the analysis of performance indicators, are the necessary follow-up actions executed?
- Is there a process for determining the criteria, scope, frequency and methods for executing internal audits of the DIQM system?

- Does the review input include process performance?
- Does the review input include status of preventative and corrective actions?
- Does the review input include follow-up actions from previous management reviews?
- Does the review input include changes that could affect the DIQM structure?
- Does the review output include decisions and action related to improvement of the effectiveness of the DIQM structure?
- Does the review output include decisions and action related to improvement of the effectiveness of the DIQM processes to ensure data and information quality and accuracy?
- Does the review output include decisions and action related to improvement of customer related requirements with respect to DIQM?

# Business

## Description

The *Business* dimension is a generic representation of the business processes, products and services that deliver the outputs of the organisation. It emphasises aspects of customer centricity and channel shift that are objectives of the AoG Strategy.

At an AoG level, it describes the customers and different channels used to interact with government; common products and services provided by the government; and the different roles, skills and processes needed to support all of the above. The government business capabilities promote cross-government collaboration and enables business and technology leaders to discover opportunities for cost savings and new business capabilities that help to achieve strategic objectives.

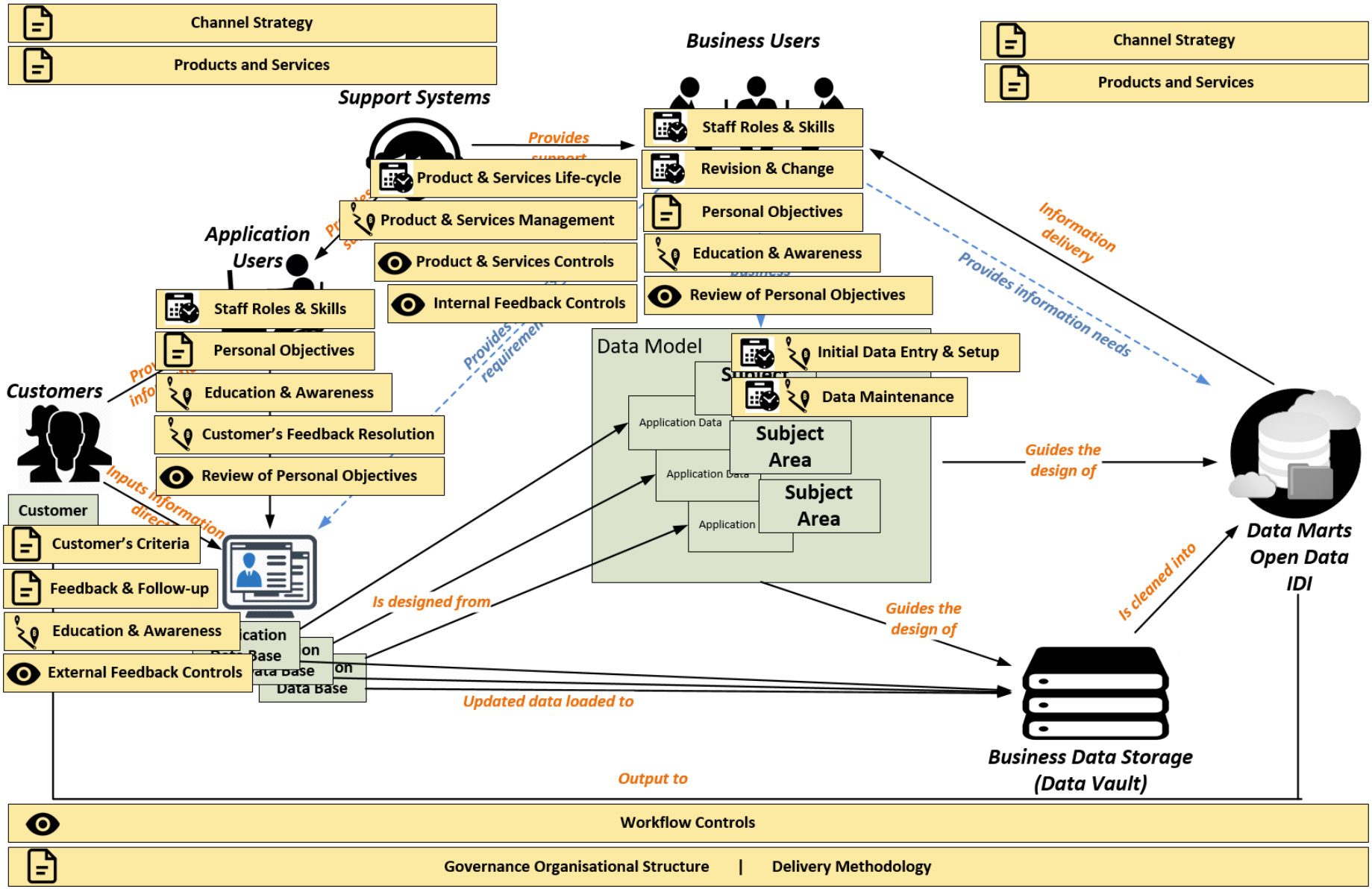
At an agency level, it describes the agency's customer personas and experiences as they interact with the agency, and the products and services that the agency provides.

## Context and Relationships

| | | |
|---|---|---|
| **Business** | describes the business services, processes, and capabilities to support the strategic goals and objectives | **Strategy, Investment, and Policy** |
| | sets out the business capabilities required to support governance models and effective business performance management | **Governance and Performance** |
| | sets the business requirements for data and information, and identifies redundancy, duplication and gaps | **Data and Information** |
| | sets the business requirements for application and software services, and identify redundancies and opportunities for reuse and sharing | **Application and Software Services** |
| | sets the business requirements for infrastructure, and identify redundancies and opportunities for reuse and sharing | **Infrastructure** |
| | identifies the business elements that require security and privacy protection, and the business requirements for identity and access management | **Identity, Privacy, and Security** |
| | sets the business requirements that drive development and scope of corresponding standards | **Standards** |

# Components Overview

This diagram gives a visual overview of the different components within the *Business* dimension.



# Components

## Plan

### *Staff Roles & Skills*

**What** – Define and clarify the exact profile of each one of the roles[14] that are needed to successfully manage a DIQM system within the organisation and plan the resources needed to support these roles. Other aspects that need to consider in the planning are the behaviours, expectations, the tasks those roles must, but also should do. Establish a customer representative role to reduce customer burden.

**Why** – It is essential to have a reference regarding the performance expected from people executing activities around DIQM. It will also help to ensure that people receive the training needed for their tasks.

**Whom:**

- The Chief Digital and Information Officer[15] is accountable for the planning.
- HR and Functional managers are responsible to identify the people for the specific roles and skills.
- HR is responsible for the planning of education and training.
- Communication business unit is responsible for the awareness within the organisation.
- Other roles that should be involved in the planning are:
    - Knowledge and Information managers
    - Enterprise, Business, Data, and System architects
    - Customer representatives
    - Testing designers and testers

**Example:**

- Job descriptions checked by HR & Quality Management.
- Data and Information Management - Roles and Responsibilities guidelines.

**Questions to ask:**

- Has the organisation defined the DIQM roles and responsibilities?
- To what extent has the organisation identified what skills are required to manage data and information?
- Does the project leadership and business owners define the best set of skill needed for each part of the process?
- Are these profiles aligned with the different organisational areas?[16]
- Is there an ongoing internal communication process in place on any aspect of data and information quality, to create awareness within the organisation on the importance of providing highly accurate data and information?

[14] See the Data and Information Management - Roles and Responsibilities guidelines developed by the Know-MAT in 2017 and approved June 2017. This guideline is available on PSI.

[15] Chief Digital and Information Officer or similar role.

[16] Should not influence profile design

### *Product & Service Life-cycle*

**What** – Develop a general strategy for managing information, according to the value[17] of the information asset, that reflects the business, customer, and staff needs for each of the phases in the product and service's life-cycle. Also to take in consideration is the Memorandum of Understanding (MoU) or any other agreements with 3th parties. At the End-of-Life, there are some aspects that needs to be defined and planned: destruction, retention, and any archiving issues.

**Why** – Product & service life-cycle plays a critical role in the organisation's strategy. Depending on the stage, the strategy can be refined accordingly to ensure optimal performance and results in each stage.

The four stages of a Product & Service Life-cycle are:

- Research & Development
- Growth - general increase in demand
- Maturity - conduct research to determine trends, adapt product or services to meet the trends
- Discontinuation – or introduce new product or services

Master data is an integral part of product and services the organisation provide to their customers. This information should evolve in the same way as the products and services' life-cycle, from research & development and launch all the way to the eventual discontinuation.

**Whom:**

- The Product and Service owners are responsible for setting up the strategy for the products and services, together with the planning on managing the information around those product and services.
- Enterprise, Data, and Solution architects are responsible to identify the impact of any changes in the data and information, the DIQM structure is reviewed, and to make sure those changes are reflected in the different layers of architecture and development.

**Example -** Planned product and service audits at specific phases of the life-cycle.

**Questions to ask:**

- Are the types of changes that will most likely occur in each phase of the life-cycle analysed?
- Does the organisation periodically audit the DIQM structure so it still reflects all the products and services an organisation provide?
- Do the audits result in documented, communicated and implemented action plans?
- Are the results of these audits shared within the organisation?
- Do metrics reflect user experience?

### *Revision & Change*

**What** – Plan the steps to ensure changes in the product and services' information is reflected to any future use, change, or access to that information. Establish the value of the organisation's information assets, the security controls, the reason for change, and the requirements for tracking, auditing, recording, storing, and access control according to the value and the cost.

**Why** – This enables the organisation to be able to track changes on the data and information to the source which is crucial for the resolution of discrepancies and to have visibility into the data along its life-cycle.

[17] There are several techniques to determine the value of an information asset. Four key areas to look at are: the risk when lost or not have, the cost for maintaining, the usage, and the knowledge that can be gained from that asset.

**Whom:**

- Data Owner with strong leadership with mandate to guide the requirements for tracking, access control, auditing of changes.
- Data Change manager to make sure the requirements are executed and met.
- Data Custodian to store based on the Data Owner's details

**Example** - Log all changes on data.

**Questions to ask:**

- Are the changes and revisions recorded? Including when, why, how, and by whom the changes were made?
- Does the organisation have a structure and controls in place to ensure the security of data from unauthorised access and change?
- To what extent does the database structure ensure traceability of amendments?

## Document / Record

### *Customer Criteria*

**What** - Create formal documentation of the customer's[18] criteria they need to have to interact with the organisation, what product and services they need and which customers need additional assistance. Define what is expected from the customer, the impact on then, and what is seen as success when resolving issues. Communicate this to the customers.

**Why** - Having a clear view of the customers, the organisation can improve their services towards groups of customers, add additional information to decrease calls to customer service, initiate new services to resolve gaps, etc. Having a clear view of the customers also helps in better communication, discover opportunities, and decrease costs.

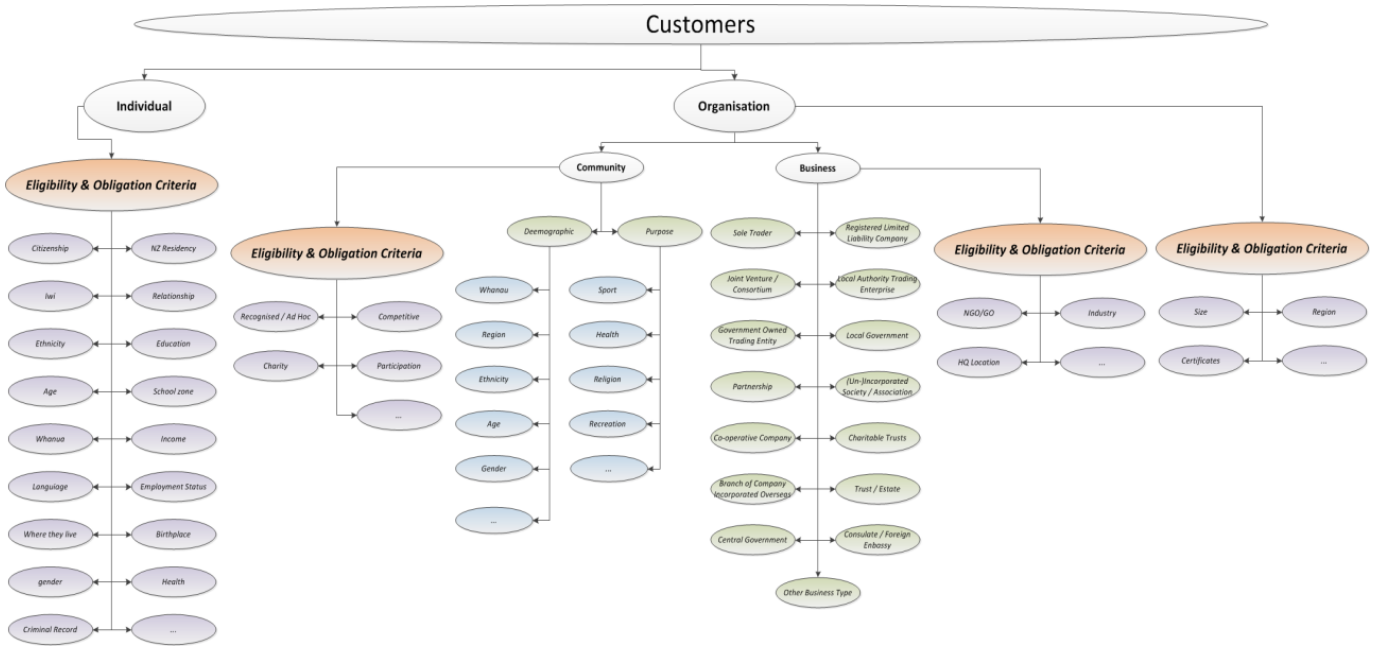
**Whom:**

- Service delivery managers
- Customer strategists
- Marketing managers
- Bi Mangers
- Sales

**Example** – Customer, service, and staff criteria.

**Questions to ask:**

- Has the organisation a view on the different types of customers who interact with the organisation?
- Can the organisation classify its customers into different groups?
- Does the organisation know which customer groups apply for which product and services?
- Is the customer interaction with the organisation tracked and stored from day one?




[18] Current and desired, but not yet engaged.

### *Channel Strategy*

**What** – A formal high-level plan for the Government's online activities and interaction with all citizens, this to ensure that the Government and all its customers interact effectively and productively online.

**Why** - Organisations are more and more engaged in using digital technologies to improve their service delivery to customers. This Channel Strategy provides coordination, direction and encouragement to the current and new digital activities of the organisation. When implemented the channel strategy will improve customer service and the customer experience, fulfilling the service value, whilst reducing costs and improving customer compliance.

**Whom:**

- Communication manager
- Web manager

**Example** – Channel strategy roadmaps.

**Questions to ask:**

- Has the organisation a view on the different types of channels customers interact with the organisation?
- Does the organisation know the impact of channels of the different types of customers?
- Has the organisation identified customer capabilities to use government channels? E.g. cell phone, internet, ability to travel, money for courier, etc.
- Does the organisation know which channels are used for which product and services? And why or why not?

### *Product & Service Documentation*

**What** – Documentation that accompanies product and services, outlining the business rules, purpose, development, design, technical configuration, terms, etc.. Use of standardised terminology is highly recommended. Make sure all areas of the organisation know what is what and where it is.

**Why** – Good product and service documentation enhances the communication about the product and services offered by the organisation. It can indicate how to evolve product and services, the channels to use (see Channel Strategy), and other avenues to access information.

**Whom:**

- SLT is accountable for the completeness.
- Product owners are responsible for the completeness of their product and services
- Architects are responsible for describing the products and services
- Delivery leads are responsible for the correct delivery of the products and services.

**Example** – Online documentation about products and services offered by the organisation.

**Questions to ask:**

- Does the organisation make use of a single source of the truth for product and service master data[19] to manage and share data with other organisations and business partners?
- Does the data publishing process include all necessary provisions to ensure that product and service changes published are based upon the most relevant version?
- Does publishing systems ensure changes are reflected in a timely manner? And are those changes indicated to the 'reader'?
- Does the documentation include compliance requirements? Including data sharing?
- Does the documentation include requirements to retain and / or destroy?
- Does the organisation have a clear view on what product and services and data sets it is responsible for?

---

[19] Master data represents the business objects which are agreed on and shared across the organisation.

***Governance Organisational Structure***

**What** – Ensure that the governance model defined for the organisation during the planning phase is properly documented and made available to everyone within the organisation. Clearly state the accountability throughout? the organisation.

**Why** – Documenting the governance structure is required to formalise its existence in the organisation; it is also necessary when evaluating its performance or to further improve it.

**Whom –** Information Leadership team / Governance group.

**Example** – Documented elements of the governance model of the process such as: Responsibility Assignment Matrix, internal and external policies for the process.

**Questions to ask:**

- Is there a governance entity or group within the organisation?
- Does the organisation have a documented DIQM structure in place?
- Does the documentation of this DIQM structure include manual, objectives and targets?
- Is the data and information ownership within the organisation defined, documented, implemented and/or regularly reviewed?
- Has the division of responsibilities been recorded and communicated throughout the organisation?
- To what extent does the review include assessing opportunities for improvement and the need for changes to the DIQM structure, including the DIQM policy and objectives?
- Does the review input include changes that could affect the DIQM structure?

***Delivery Methodology***

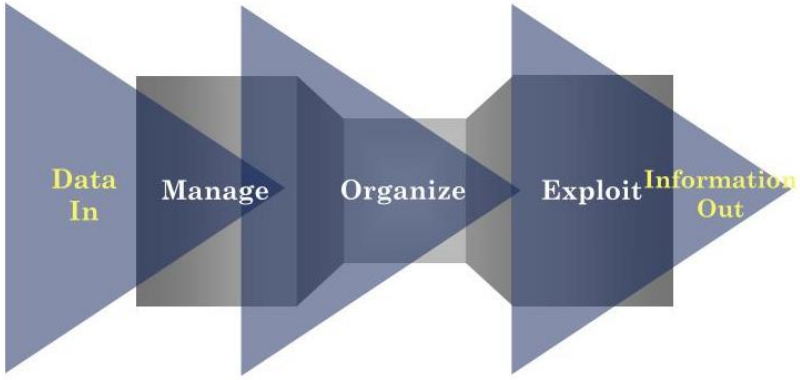
**What** – Formally document the delivery methodology for information management best practices. Its scope covers the complete information supply chain[20] within an organisation: from how it is created, accessed, presented and used in decision-making to how it is kept secure, stored and destroyed.

**Why –** Having a clear description of the delivery methodology will make the operation easier and will give legitimacy to all actions within the process:

- How it is created: collected from individuals or organisations.
- Disclosure: provided to individuals or organisations

**Whom -** Business owners / Information managers

**Example** – Information delivery process




[20] The scope here is very wide; we recommend the agency split this up into areas and or data sets.

**Questions to ask:**

- Does the organisation have a documented DIQM structure in place?
- Does the DIQM documentation include a delivery methodology?
- Is the delivery methodology regularly reviewed?

### *Customer Feedback & Follow-up*

**What** – Establish direct access for queries, complaints, requests, follow-ups, etc. and formally document, management and process those.

**Why** – A customer feedback process will allow everyone within the organisation to process customer feedback correctly improving the response given by the organisation to its customers.

**Whom:**

- Data owner should provide the resources
- Compliance manager
- Internal and external customer insight specialists / customer representatives
- Service delivery
- Customer service staff / operations

**Example** – Guidelines for the timeframe in which customer complaints/requests should and must be answered.

**Questions to ask:**

- Is a documented procedure in place for handling customer complaints concerning data and information quality?
- Are improvement actions initiated based on the analysis of customer feedback and are they distributed throughout the organisation?
- Is there a mechanism to store and document customers' feedback into a system, to be used for improvements and to avoid reoccurrence?
- Are formal responses issued to customers in regards to their data and information quality complaints?
- Are the customer feedback procedures known not only to those directly involved with customers, but to all that contribute to the process so they are aware of the organisation's commitments to their customers?

### *Personal Objectives*

**What** – Integrate DIQM KPIs into staff objectives[21] according to their roles and responsibilities.

**Why** – It will provide not only formality to the relevance of data and information quality for the organisation but also additional motivation for people to excel at the data quality-related tasks.

**Whom:**

- Information manager and HR manger to define the organisational DIQM KPIs
- Line managers to measure and track all staff compliances and competencies with IDQM KPIs

**Example** – Required competencies for the functions on the process.

**Questions to ask:**

- To what extent has the organisation identified what skills and talents are required in managing data and information quality?
- To what extent does the organisation evaluate the effectiveness of the actions taken to increase the competencies of staff regarding data and information quality?
- Are the people defined goals realistic and valuable for each one of their roles?

---

[21] Job description, Code of Conduct, organisational objectives, etc.

## Execute

### *Education & Awareness*

**What** – Run a compulsory information management module for all staff. Conduct the necessary education programmes needed to ensure people understand their role and responsibility in DIQM. Engage in communications across the organisation to educate people in the policy, procedures, and guidelines in place they need to follow to help the organisation achieve high quality data and information.

**Why -** There must be clear understanding of:

- The roles and responsibilities
- The importance of value to staff
- The reasoning behind the DIQM

**Whom:**

- SLT/ELT to fund the training and awareness.
- CDIO, HR, people managers, business unit leads, data stewards to define what training is needed.
- Separate business units will need to take responsibility for identifying educational needs and ensuring relevant staff gets trained as needed.
- Data stewards establish the requirements:
    - For 'fit for purpose'
    - To connect those to capability requirements
    - Identify where quality can be improved / delivered
    - System design and functionalities
    - Individual capabilities.
- Communication manager to be responsible for the awareness and communications.
- Architects to define the changes.
- Staff to attend training and to give feedback.

**Example** – Internal newsletters, announcements, meetings and sessions to inform people on their role and responsibility in the quality of data and information.

**Questions to ask:**

- Is data and information quality linked to daily activities?
- Is there an ongoing internal communication process in place to create awareness within the organisation on the importance of providing highly accurate data and information?
- Is there an external communication process in place to communicate any change and to identify the source of information in engagement with other organisations and 3rd parties?
- Is there a process in place to keep the organisation up-to-date regarding the requirements to achieve high quality data and information?
- To what extent does the organisation maintain appropriate records of education, training, skills, and experience?
- Are the results of audits shared within the organisation?
- Are the results on performance indicators communicated within the organisation and if applicable to 3rd party service providers?
- Are learnings fed back into ongoing improvements in process and in trainings?
- Are the training efficiency verified?

### *Customer Feedback Resolution*

**What** - Implement or update procedures to process and resolve customer feedback. This includes testing and checking identified issues 'Are they what they seem to be'.

**Why** - Customer feedback should be used as input for further improvement of the DIQM system.

**Whom:** Both internal and external:

- Stakeholders
- Customers
- Clients
- Citizens
- Staff
- Etc.

**Example** – Key-account management policies, service level agreements (SLA's).

**Questions to ask:**

- Are improvement actions initiated based on the analysis of customer feedback?
- Are formal responses issued to customers in regards their data and information quality complaints?
- Does the customer feedback resolution process tie-in correctly to the data and information issue resolution procedure?
- Is the customer interface accessible, readily useable, broad-reaching, and understandable?
- Are customers being provided with tools:
    - To improve their experience
    - Provide better feedback
    - Be part of the process for improvement, not just the recipient.

***Product & Service Management***

**What** - Carry out activities to measure and manage products and services to continuously evaluate the metrics and conduct improvements/corrective actions whenever necessary to achieve the desired quality of information around the products and services. Define appropriate and meaningful metrics (not just numbers, also identify of the value of information asset[22]) Execute periodic reviews of what is the customer experience of the service.[23]

**Why** - Formalising and externalising product and service management will provide the organisation with an objective and effective way to monitor and improve their services.

**Whom:**

- Product managers
- IT Service delivery leads

**Example** – Protocol for periodical metrics revisions.

**Questions to ask:**

- To what extent is the product and service management applied within the organisation?
- Does the organisation have approved processes and procedures for product and service data input?
- Do metrics reflect user experience?
- Do the measures feedback through testing and reporting?
- Are the training efficiency verified?

[22] See Product & Service Life-cycle.

[23] See Product & Service Controls.

## Control / Monitor / Evaluate

### *Internal & External Feedback Controls*

**What** - Monitor compliance level of process, data and information to the expected performance criteria across the DIQM in order to measure the degree in which the organisation adheres to the defined policies and standards. Use legislative requirements to articulate and track process procedures.

**Why** - Successful execution of a DIQM system depends on ensuring that the different checks that have been built into the workflows and processes are applied and that data and information are controlled and monitored to ensure the output conforms to the defined performance requirements.

**Whom:** Both internal and external:

- Stakeholders
- Customers
- Clients
- Citizens
- Staff
- Etc.

**Example** – Implementing consistency checks for data and information.

**Questions to ask:**

- Are the checks for the data and information performance pragmatic?
- Are they based on the performance KPIs defined so that they can be successfully monitored?
- Are there KPIs defined and tracked?
- Is there a process in place to identify and communicate changes/corrections to the data and information?
- Does the organisation have approved processes and procedures for data input?
- Has the organisation established, maintained, and documented the operational processes needed for internal data publishing?
- Have critical success factors (key elements that ensure a satisfactory performance) been established in the processes for external data publishing?

### *Review of Personal Objectives*

**What** – Together with the person, review the degree of progress that they made in regards to their personal objectives towards data and information quality.

**Why** - Evaluation of results is needed to re-calibrate actions that may need corrections or to update the goals that people have.

**Whom:**

- Information manager and HR manger to define the organisational DIQM KPIs
- Line managers to measure and track all staff compliances and competencies with IDQM KPIs
- Staff

**Example** – Compare performance and competencies of staff to the documented target descriptions and goals.

**Questions to ask:**

- To what extent has the organisation identified what skills and talents are required in managing data and information quality?
- To what extent do the people who manage data and information quality have the right talents and skills set?
- Does the review output include decisions and action related to improvement of customer related requirements with respect to DIQM?

***Product & Service Controls***

**What** - Ensure that the methodology for conducting product and service inspection is always followed when executing product and service measurements, either within a monitoring audit, a first measurement of new product and service or as part of the maintenance process of data. Execute periodic reviews of what is the customer experience, the process, etc. of the service.

**Why** - The ultimate proof of the effectiveness of the DIQM system lies in ensuring that data will successfully match when inspected at any given time.

**Whom:**

- SLT is accountable for the completeness.
- Auditors
- Quality Assurance
- Legal counsel
- Product managers
- IT Service delivery leads

**Example** – Monthly random inspections on existing product and services.

**Questions to ask:**

- Does the organisation make use of standardised monitoring and measuring processes within the organisation and across the industry?
- Are the tools that require calibration being calibrated within the organisation (either by internal or external certified service providers), according to requirements?
- Does the organisation compare the right product and service to the data that will be published. Compare the results of internal audits to the levels of quality reported by customers and identify any potential mismatch that could be caused by external factors?
- To what extend are these controls applied?

***Workflow Controls***

**What** - Monitor compliance level of the process and its data output to the expected performance criteria across the DIQM system in order to measure the degree in which the organisation adheres to the defined policies and standards.

**Why** - Successful execution of a DIQM system depends on ensuring that the different checks that have been built into the workflow are applied and that processes, data and information are controlled and monitored to ensure the input and output conforms to the defined minimum requirements.

**Whom:**

- Auditors
- Quality Assurance
- People managers
- HR
- Business unit leads

**Example** – Implementing consistency checks for information.

**Questions to ask:**

- Is there a process in place to identify and communicate changes/corrections to data and information? Is this process documented and clearly communicated?
- Is there a process in place for customers to review / amend data provided?
- Are there controls in place within the organisation to track the use of the information?
- Does the organisation have approved processes and procedures for data input and output?
- Has the organisation established, maintained, and documented the operational processes needed for internal information publishing?
- Have critical success factors (key elements that ensure a satisfactory performance) been established in the processes for external information publishing?

- Has the organisation established and maintained procedures to control the process of publishing product and service information?
- Does the information publishing process include all necessary provisions to ensure that product and service changes published are based upon the most relevant version of the product or service?
- To what extent does the information publishing process include all necessary provisions to ensure that product and service attributes published can be traced back to its origin?

# Data and Information

## Description

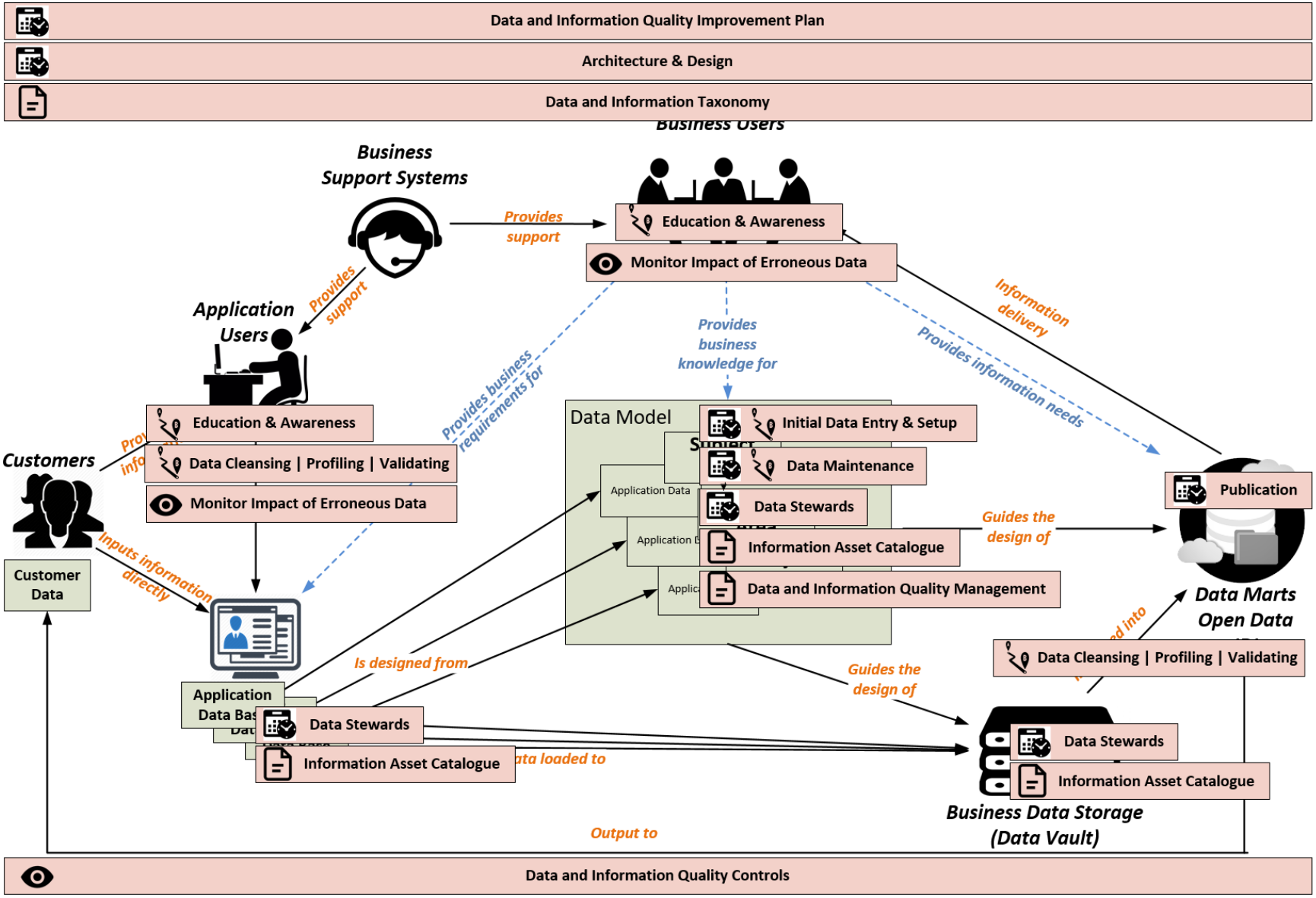
The *Data and Information* dimension primary purpose is to discover, describe, manage, protect, share and reuse information within and across organisations and their business partners. It provides a standard means by which data may be described, categorised, analysed, valued, and shared, and it facilitates discovery and exchange of core information across organisational boundaries. And it also provides means of tracing distribution, identifying, and relaying provenance of original data and any cha nges.

## Context and Relationships

| | | |
|---|---|---|
| **Data and Information** | provides a framework for trusted data and information that can be used for strategic decision making | **Strategy, Investment, and Policy** |
| | provides a framework for trusted data and information that can be used to improve governance models and business performance management | **Governance and Performance** |
| | provides the data and information structures that support business services, processes, capabilities, information sharing, and reuse | **Business** |
| | provides the authoritative data and information structures to be used by application and software services | **Application and Software Services** |
| | provides the data and information requirements for technology and infrastructure services | **Infrastructure** |
| | provides the data and information requirements and models needed for identity, privacy, and security | **Identity, Privacy, and Security** |
| | sets the data and information requirements that drive development and scope of corresponding standards | **Standards** |

# Components Overview

This diagram gives you a visual overview of the different components within the *Data and Information* dimension.



# Components

## Plan

### *Data Stewards*

**What** – Identify and appoint data stewardship and responsibilities across the organisation and make sure that the relationship between them and other staff is clear and is consistent with the overall structure of the DIQM. A data steward is a person responsible for the management of data assets (also known as critical data assets) - both the content and metadata.

**Why** - Clear data stewardship is fundamental for reliable governance of the process. Data stewards have a specialist role that incorporates processes, policies, guidelines and responsibilities for administering organizations' data sets in compliance with policy and/or regulatory obligations.

Data stewards[24] ensure that each assigned data set:

- Has clear and unambiguous data asset definition.
- Does not conflict with other data sets (removes duplicates, overlap etc.)
- Have clear enumerated value definitions.
- Is still being used? Remove (or move to an archive database) unused data sets)
- Is being used consistently in various computer systems
- Has adequate documentation on appropriate usage and notes
- Documents the origin and sources of authority on each metadata
- Is protected against unauthorized access or change

**Whom:**

- Executive Leadership Team is responsible for identifying the need for a data steward.
- HR is responsible for creating job descriptions and hiring or uplifting skills to align with a data steward role.
- Chief Privacy Officer, Chief Security Officer, and line managers contribute to defining responsibilities and skills needed.

**Questions to ask:**

- Is the data steward role defined, documented, implemented and/or regularly reviewed?
- Has the division of responsibilities been recorded and communicated throughout the organisation?

### *Data & Information Quality Improvement Plan*

**What** – Plan the steps to improve the quality of the data and information within the organisation: data profiling, data cleansing, data defect prevention, etc.

**Why** - Improved data and information quality supports good strategic decision making and provides accurate management reporting such as for Key Performance Indicators.

[24] For the specific responsibilities check the related Data and Information Management Roles and Responsibilities guidelines.

**Whom:**

- Data Owner with strong leadership with mandate to guide the requirements for tracking, access control, auditing of changes.
- Data Change manager to make sure the requirements are executed and met.
- Data Custodian to track based on the Data Owner's details

**Example** – Planning of the following steps to improve the data and information quality: data profiling, data cleansing, and data defect prevention.

**Questions to ask:**

- Has the organisation set out and planned the different tasks needed to achieve high quality data and information?
- How are datasets prioritised? Based on Value? And how are they valuated?

***Initial Data Entry & Setup***

**What** – Define a process for the initial set up of product, service, and process information in the organisation's back-end systems so that all data entered is only entered when verified to be reliable. Tracking provenance and verifying authenticity.

**Why** - Ensuring that only reliable data is ultimately added to the internal systems is fundamental for supply chain efficiency. Controlling the process and audit trail for creating, amending, changing, or deleting of data into the back-end systems is the first step to guarantee that the data and its subsequent evolution are based on quality foundations.

**Whom:**

- Product Owner with strong leadership with mandate to guide the requirements for tracking, access control, auditing of changes.
- Change manager to make sure the requirements are executed and met.

**Example** - Centralised product and service set up for the organisation. Initiative based data and information impact assessment.

**Questions to ask:**

- Does the organisation have a specific process for generating and checking the data for new products and services, prior to first distribution and development of new product or service?
- Does the organisation review the procedures for data input and creation for adequacy and accuracy?
- Is all data being verified and provenance, data of generation and collection recorded, before being entered and set up in internal systems?
- Is there monitoring of data in place that conforms to any internal policies that the organisation may have? Including data access, role based restrictions, etc.
- Is the data entry process protected against access, modification, and deletion by unauthorised parties?

***Ongoing Data Maintenance***

**What** – Define a process for the continuous update and maintenance of data that has been set up so that it is always relevant and up to date with the latest changes in the product and services.

**Why** - As the information of a product or service changes and evolves through time, its consistency has to be guaranteed along the life-cycle to ensure it is always reliable; for that purpose a process must be in place to prevent changes from affecting the quality of the information and need to account for changes in the 'product'. It also needs to incorporate valid changes in the data.

**Whom:**

- Data Owner with strong leadership with mandate to guide the requirements for tracking, access control, auditing of changes.
- Change manager to make sure the requirements are executed and met.
- Data Custodian to track based on the Data Owner's details

**Example** - Cross-functional product and service development teams that ensure that changes that affect the product and services are shared across all areas; locking certain 'key' attributes so they cannot be edited without proper consultation.

**Questions to ask:**

- Does the organisation make use of a single source of the truth for product and service master data to manage, change, and share data with other organisations or business partners?

- Is there a process in place to identify and communicate changes/corrections to data and information?
- Does the organisation have a process in place for checking product and service information during the product or service life-cycle?
- Are there clear guidelines for product and service changes?

***Architecture & Design***

**What** – Set up a data architecture design for the organisation that supports not only the DIQM but also is aligned with the system and infrastructure architecture.

**Why** - This will provide the organisation with a clear vision and plan for the interaction between the supporting systems the organisation makes use of, which results in effective deployment of the systems.

**Whom:**
- Enterprise, Data, and Solution architects are responsible to identify the impact of any changes and design the architecture, the DIQM structure is reviewed, and to make sure those changes are reflected in the different layers of architecture and development.
- The Product and Service owners are responsible for setting up the strategy for the products and services.
- Operations and development are responsible for the implementation.

**Example** - Cross-functional product and service development teams that ensure that changes that affect the product and services are shared across all areas; locking certain 'key' attributes so they cannot be edited without proper consultation.

**Questions to ask:**
- To what extent does the data structure ensure traceability of amendments (change history)?
- Are the requirements for the solution architecture drawn from the organisation's priorities identified in the vision and planning?

## Document / Record

***Information Asset Catalogue***

**What** - A systematically categorized, organized and descriptive collection, list or aggregation of the information assets that can either be electronic or hardcopy in nature and that makes it clear where to find, retrieve and store these items, as necessary.

**Why** - One of the primary purposes for the collection of the information asset catalogue is to further the government and organisation information sharing strategy by ensuring a government-wide understanding of data assets. The information asset catalogue is used to allow discovery of the data and information across the organisation, ultimately resulting in reuse and increased sharing with other organisations and business partners.

**Whom:**
- SLT is accountable for the completeness.
- Product owners are responsible for the completeness of the information around their product and services
- Data architects are responsible for identifying the metadata
- Everyone is responsible for identifying information assets and adding it to the catalogue.

**Example** – Information asset catalogue.

**Questions to ask:**
- Has the organisation a view on their data and information assets, incoming and outgoing, and the processes that modify the assets, and where each asset is stored and who has the stewardship?

***Data & Information Taxonomy***

**What** - The GEA-NZ Data and Information Reference Taxonomy categorise and describe the New Zealand Government Information consistently in three pillars of Information: motivators, entities, and activities.

**Why** - The primary purpose is to discover, describe, manage, protect, share and reuse information within and across the organisation and their business partners.

**Whom:**

- SLT is accountable for the completeness.
- Enterprise architects are responsible for identifying the data and information categories
- Everyone is responsible for identifying information assets and describing and categorising it in the taxonomy.

**Example** – GEA-NZ Data and Information Reference Taxonomy

**Questions to ask:**

- Does the organisation use the GEA-NZ Data and Information Reference Taxonomy to categorise their data and information assets?

***Data and Information Quality Management***

**What** – This document. DIQM is an administration type that incorporates the role establishment, role deployment, policies, responsibilities and processes with regard to the acquisition, maintenance, disposition and distribution of data and information.

**Why** – The DIQM establishes the governance, identification of the roles and responsibilities, quality expectations as well as the supporting business strategies.

**Whom –** Everyone is responsible for following the data and information quality management policies and procedures.

**Example** – This document.

**Questions to ask:**

- Does the organisation use this document to organise their DIQM processes and governance?

## Execute

***Education & Awareness***

**What** - Conduct the necessary education programmes needed to ensure all needed steps are in place to improve high quality data and information, and that all data and information assets and processes are defined and processed in a consistent way.

**Why** - There must be clear understanding of the steps needed and the accountabilities of those involved, to achieve high quality data and information.

**Whom:**

- SLT/ELT to fund the training and awareness.
- CDIO, HR, people managers, business unit leads, data stewards to define what training is needed.
- Separate business units will need to take responsibility for identifying educational needs and ensuring relevant staff gets trained as needed.
- Data stewards establish the requirements:
    - For ‘fit for purpose’
    - To connect those to capability requirements
    - Identify where quality can be improved / delivered
    - System design and functionalities

    - Individual capabilities.
- Communication manager to be responsible for the awareness and communications.
- Architects to define the changes.
- Staff to attend training and to give feedback.

**Example** – Internal newsletters, announcements, communication campaigns, meetings and sessions to inform people on steps needed to achieve high quality data and information.

**Questions to ask:**
- Is data and information quality linked to daily activities, to the impact if quality is not met, etc.?
- Is there an ongoing internal communication process on any aspect of data and information quality, to create awareness within the organisation on the importance of providing, generating, and recording of highly accurate data and information?
- Is there a process in place to keep the organisation up-to-date regarding the requirements to achieve high quality data and information?
- To what extent does the organisation maintain appropriate records of education, training, skills, and experience?
- Does the organisation ensures that eduction and training is sufficient and appropriate across different roles?
- Are the results of audits shared within the organisation?
- Are the results on performance indicators communicated within the organisation and if applicable to 3rd party service providers?

***Data Cleansing***

**What** - Data cleansing, data cleaning or data scrubbing is the process of detecting and correcting (or removing) corrupt or inaccurate, out of date, or irrelevant records from a record set, table, or database. It may involve removing typographical errors or validating and correcting values against a known list of entities.

**Why** - There are key purposes data cleaning should serve in delivering fit for purpose data:

- Eliminate Errors
- Eliminate Redundancy
- Increase Data Reliability
- Deliver Accuracy – opportunities to confirm accuracy with originators e.g. customers, personnel, external parties, etc.
- Ensure Consistency
- Assure Completeness
- Provide Feedback for Improvements

**Whom:**
- Business units responsible for identifying which data sets need cleansing.
- Data stewards establish the requirements
- Data architects to do the cleansing.

**Example** – Cleaning up data in a database that is incorrect, incomplete, or duplicated.

**Questions to ask:**
- Does the organisation stores their data as original as possible?
- Is there a process to ensure that data is as accurate, up to date, and relevant as possible?
- Does the data repository contain duplicated data items?
- Is there a process in place to ensure stored data and information is still needed for original purpose of collection or generation? Or have changes in systems or processes moved into secondary use? Is this still consistent with authorisations?

### *Data Profiling*

**What** - Data profiling is the process of examining the data available in an existing data source (e.g. a database or a file) and collecting statistics and information about that data.

**Why -** The purpose of these statistics may be to:

- Find out whether existing data can easily be used for other purposes.
- Improve the ability to search the data by tagging it with keywords, descriptions, or assigning it to a category.
- Give metrics on data quality including whether the data conforms to particular standards or patterns.
- Assess the risk involved in integrating data for new applications or combining data sets.
- Assess whether metadata accurately describes the actual values in the source database.
- Understanding data challenges early in any data intensive project, so that late project surprises are avoided. Finding data problems late in the project can lead to delays and cost overruns.
- Have an enterprise view of all data, for uses such as master data management where key data is needed, or data governance for improving data quality.

**Whom:**

- Data stewards establish the requirements
- Data architects to do the data profiling.

**Example** – Different analyses are performed for different structural levels.

**Questions to ask:**

- Does the organisation perform data profiling several times and with varying intensity throughout the data warehouse developing process?
- Is the purpose clear, does it clarify at an early stage if the right data is available at the right detail level and that anomalies can be handled subsequently?

### *Data Validation*

**What** - Data validation is the process of ensuring that a program operates on clean, correct and useful data. It uses routines, often called "validation rules" "validation constraints" or "check routines", that check for correctness, meaningfulness, and security of data that are input to the system. The rules may be implemented through the automated facilities of a data dictionary, or by the inclusion of explicit application program validation logic.

**Why -** The purpose of data validation depend on the type of validation, and vice versa:

- Data type validation: Verifies that the individual characters provided through user input are consistent with the expected characters of one or more known primitive data types.
- Range and constraint validation: Examines user input for consistency with a minimum/maximum range, or consistency with a test for evaluating a sequence of characters, such as one or more tests against regular expressions.
- Code and Cross-reference validation: Verifies that the user-supplied data is consistent with one or more external rules, requirements, or validity constraints relevant to a particular organization, context or set of underlying assumptions.

**Whom:**

- Data stewards establish the validation requirements
- Data architects to do the data validation.

**Example** – Data type validation.

**Questions to ask:**

- Does the organisation perform data validation at all levels of data entry and modification?

## Control / Monitor / Evaluate

### *Data & Information Quality Controls*

**What** - Execute activities for the identification, analysis, processing and resolution of issues and disruptions that may impact the quality of the data and information. Identifying data and information quality issues is the first step in solving them. Data and information quality investigations are designed to surface problems with data and information. The issues need to drive changes that will improve the quality of data and information within and across organisations.

**Why** – It is important to have a formal process in place for moving issues from information to action. It is also important to track the process of issues as they go through this process. The disposition of issues and the results obtained from implementing changes will give the organisation the best value for achieving high quality data and information.

**Whom –** Governance group and auditors

**Example** – Formally document and track issue activity.

**Questions to ask:**

- Are the issue-escalation and resolution rules clearly communicated as part of the education programmes conducted by the organisation?
- After a known failure, are steps taken to prevent them recurring?
- Based on the results of the analysis, are the necessary follow-up actions executed, documented, and build back into the processes and requirements?
- Does the review input include status of preventative and corrective actions?
- Does the review input include recommendations for improvement and accountabilities for actions?
- Does the review input include the evaluation of the KPI results?
- Does the review output include decisions and actions to improvement of the effectiveness of the DIQM?

### *Monitor Impact of Inadequate, Missing, or Wrong Data*

**What** - Monitor and record the known issues that result from poor data and information quality in order to create a clear map of the repercussions that erroneous data and information causes.

**Why** – Clearly identifying and monitoring these issues will help to position the real-life consequences of bad data and information for the organisation.

**Whom –** Governance group and auditors

**Example** – Metrics on bad service results caused by erroneous content information.

**Questions to ask:**

- Does the review input include status of preventative and corrective actions?
- Does the organisation quantify the costs of data and information issues and the effect on people, products and services?

# Application an Software Services

## Description

The *Application and Software Services* dimension describes the business applications, including 'Software as a Service', that support the business processes of the organisation. It includes core business applications, COTS corporate applications, software components (websites, databases, email, and other supporting software) and end user computing applications.

At an AoG level, it facilitates a common understanding of application assets and software services, identifying opportunities for sharing, reuse, and consolidation or renegotiation of licenses. It also assists the GCDO assurance function by identifying application assets that will require maintenance or renewal within the business planning horizon.

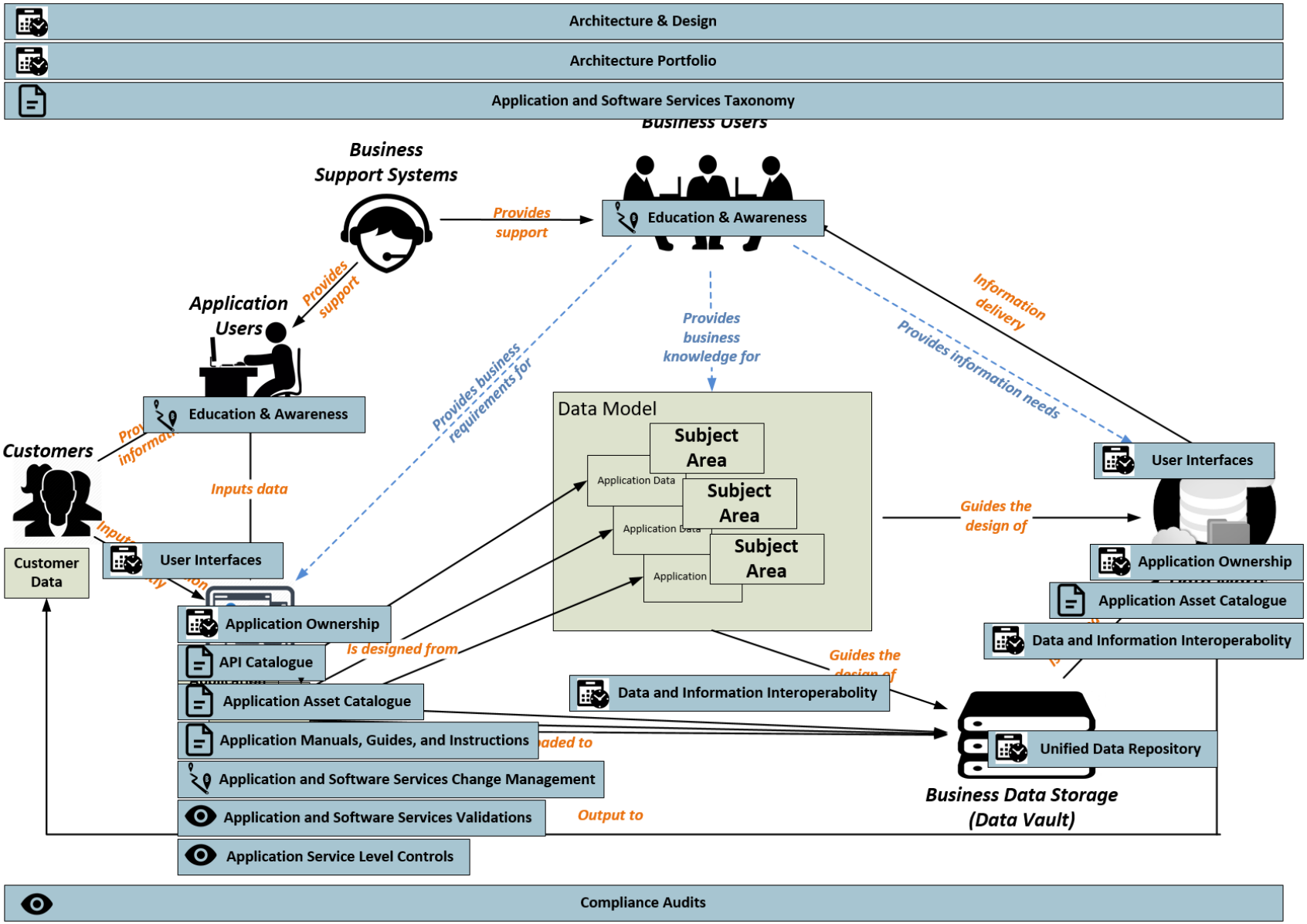
At an agency level, it describes the application assets and software services of the agency, and helps application portfolio management. Mapping their current and planned Information Systems to the Application and Software Services Reference Taxonomy categories should help agencies and sectors identify opportunities for sharing, reuse, and consolidation or renegotiation of licenses.

## Context and Relationships

| | | |
|---|---|---|
| **Application and Software Services** | represents a key mechanism for realising strategic goals, through adoption of agile core business applications and industry standard corporate support functions | **Strategy, Investment, and Policy** |
| | provides the application and software services that enables governance and performance measurement and control, and offers opportunities to improve business efficiency through sharing and reuse | **Governance and Performance** |
| | provides the application and software services that support business services, processes, capabilities, information sharing, and reuse | **Business** |
| | sets requirements and provides the tools to manage, model, structure, share, and exchange data and information | **Data and Information** |
| | provides the application and software service requirements for technology and infrastructure services, and supporting applications for infrastructure management (e.g. CMDB) | **Infrastructure** |
| | provides the application and software service controls needed to support identity, privacy, and security requirements | **Identity, Privacy, and Security** |
| | sets the application and software service requirements that drive development and scope of corresponding standards | **Standards** |

# Components Overview

This diagram gives you a visual overview of the different components within the *Application and Software Services* dimension.



# Components

## Plan

### *Application Ownership Model*

**What** – Define clear roles and responsibilities for all applications and software services that the organisation owns, uses, or interacts with.

**Why** - Clear application ownership is fundamental for reliable governance of applications and interoperability.

**Whom:**

- Executive Leadership Team is responsible for identifying the need for an application ownership model.
- HR is responsible for creating job descriptions and hiring or uplifting skills to align with an application owner role.
- Chief Privacy Officer, Chief Security Officer, and line managers contribute to defining responsibilities and skills needed.

**Questions to ask:**

- Do the people who are appointed have the responsibility and authority to ensure that applications and software services needed are procured, installed correctly, implemented and maintained?
- Are the responsibilities balanced within their reach within the organisation and that support exists for them across multiple levels in the organisation?
- Has the division of responsibilities been recorded and communicated throughout the organisation?

### *Application Portfolio*

**What** – Application portfolio is used to gather information about each application in use in the organisation, including the cost to build and maintain the application, the business value produced, the quality of the application, and the expected lifespan.

**Why** – This information is used to provide detailed reports on the performance of the IT infrastructure in relation to the cost to own and the business value delivered.

**Whom:**

- Executive Leadership Team is responsible for identifying the need for a application portfolio.
- Technology managers contribute to identifying and grouping the applications.
- Portfolio managers responsible for managing the portfolios.

**Questions to ask:**

- Does the organisation have an application portfolio and do the application owners have the authority to initiate changes to applications to improve the performance and interoperability?

### *User Interfaces*

**What** – When applicable and possible, establish definitions and requirements for the interface used to facilitate the utilisation of internal and external systems by the users.

**Why** - Ensuring the functionality and practical applicability of the organisation's systems is an important measure that simplifies the execution of the process.

**Whom:**

- Architects responsible for designing the user interfaces
- Developers responsible for implementing the interfaces
- Change and project managers responsible for managing the development of the interfaces

**Example** – User-friendly systems interfaces, on-screen help, etc.

**Questions to ask:**

- Does the organisation review the match between roles and system complexity to ensure there is balance between both factors?
- Does the organisation uses customer testing to ensure the customer- friendliness if the interfaces?
- Has the division of responsibilities been recorded and communicated throughout the organisation?

***Unified Data Repository***

**What** – Establish a central data repository for the organisation that consolidates all final data for external publication, including sharing and dissemination.

**Why** - A central data repository for all 'final' product and service data and information is essential to support the organisation's vision for one single source of the truth for product and services.

**Whom:**

- Executive Leadership Team is responsible for identifying the need for a unified data repository.
- Data architects responsible for designing the repository
- Developers responsible for the implementation
- Change and project managers responsible for managing the development

**Example** – Product and Service Information Management system.

**Questions to ask:**

- Does the organisation make use of a single source of the truth for product and service master data to manage and share data with customers, other organisations and business partners?
- Does the data publishing process include all necessary provisions to ensure that product and service changes published are based upon the most relevant version of the product or service?
- Has the organisation done a study on the needs and long term aspirations and risks before choosing the type of central repository that will be used (e.g. "in-house" development vs. Solution provider, etc.)?

***Data & Information Interoperability***

**What** – Interoperability is the ability of making systems and organisations work together. There are two types of interoperability:

- Syntactic interoperability: If two or more systems are capable of communicating and exchanging data, they are exhibiting syntactic interoperability. Specified data formats, communication protocols and the like are fundamental. XML or SQL standards are among the tools of syntactic interoperability. This is also true for lower-level data formats, such as ensuring alphabetical characters are stored in a same variation of ASCII or a Unicode format in all the communicating systems.
- Semantic interoperability: Beyond the ability of two or more systems to exchange information, semantic interoperability is the ability to automatically interpret the information exchanged meaningfully and accurately in order to produce useful results as defined by the end users of both systems. To achieve semantic interoperability, both sides must refer to a common information exchange reference model. The content of the information exchange requests are unambiguously defined: what is sent is the same as what is understood.

**Why** - Interoperability ensures that information flows seamlessly. In other words, the information follows the product and service regardless of geographic, organisational, or vendor boundaries. Specifically, Interoperability refers to the architecture or standards that make it possible for diverse electronic record systems to work compatibly in a true information network.

**Whom:**

- Data architects responsible for designing the interoperability
- Developers responsible for the implementation
- Change and project managers responsible for managing the development

**Example** – Syntactic interoperability.

**Questions to ask:**

- How do the applications interact with internal and external systems?
- How do systems communicate with each other?
- How is data and information processed and managed?
- How does the organisation integrate with systems and applications from their business partners?

**Note** – Interoperability must be distinguished from open standards. Although the goal of each is to provide effective and efficient exchange between systems, the mechanisms for accomplishing that goal differ. Open standards imply interoperability ab-initio, i.e. by definition, while interoperability does not, by itself, imply wider exchange between a range of products, or similar products from several different vendors, or even between past and future revisions of the same product. Interoperability may be developed post-facto, as a special measure between two products, while excluding the rest, or when a vendor is forced to adapt its system to make it interoperable with a dominant system.

## Document / Record

### *Application Asset Catalogue*

**What** - A systematically categorized, organized and descriptive collection, list or aggregation of the application and software services and a clear view where these applications and software services are installed and used for.

**Why** - One of the primary purposes for the collection of application asset catalogue is to further the government and organisation information sharing strategy by ensuring a government-wide understanding of application assets and their interoperability. The application asset catalogue is used to allow discovery of the data and information exchange across organisations, ultimately resulting in reuse and increased sharing with other organisations and business partners.

**Whom:**

- SLT is accountable for the completeness.
- Product owners are responsible for the completeness around their product and services
- Application architects are responsible for identifying the metadata
- Everyone is responsible for identifying and adding application assets to the catalogue.

**Example** – Application asset catalogue

**Questions to ask:**

- Has the organisation a view on their applications and software services, their interoperability and the information that is exchanged between the organisation and other organisations and business partners?

### *Application & Software Service Taxonomy*

**What** - The GEA-NZ Application and Software Service Reference Taxonomy categorise and describe the New Zealand Government applications and software services consistently into application domains, which are divided into application areas, which have categories.

**Why** - The primary purpose is to discover, describe, manage, protect, share and reuse applications and software services within and across organisations and their business partners.

**Whom:**

- SLT is accountable for the completeness.
- Enterprise architects are responsible for identifying the application and software services categories
- Everyone is responsible for identifying application assets and describing and categorising it in the taxonomy.

**Example** – GEA-NZ Application and Software Service Reference Taxonomy

**Questions to ask:**

- Does the organisation use the GEA-NZ Application and Software Service Reference Taxonomy to categorise their applications and software services?
- To what extent is the GEA-NZ Application and software service Reference Taxonomy applied internally?

### *API Catalogue*

**What** - Provides complete API lifecycle, including definition, creation, security, monitoring, and management of APIs.

**Why - The purpose is to:**

- Gain comprehensive, enterprise-wide visibility into APIs
- Minimizes redundancy and optimizes reuse of APIs
- Provides a single-source for visibility to internal and external APIs

**Whom:**

- SLT is accountable for the completeness.
- Product owners are responsible for the identification of APIs around their product and services
- Application and solution architects are responsible for identifying the APIs
- Developers responsible for developing and adding APIs to the catalogue.

**Example** – API catalogue.

**Questions to ask:**

- Does the organisation use the API Standard and Guidelines available on ict.govt.nz?
- Has the organisation a view on their own internal and external APIs?

### *Application Manuals, Guides, & Instructions*

**What** – Reference documents which provide detailed information about each application and or software service.

**Why** – Detailed information about applications improves the configurations of those applications and the correct use, especially for interoperability between other systems.

**Whom:**

- SLT is accountable for the completeness.
- Product owners are responsible for the distribution of the manuals and guides around their product and services
- Application and solution architects are responsible for creating manuals

**Example** – Solution architecture or detailed design documents.

**Questions to ask:**

- Has the organisation manuals, guides and or instructions for every application and software services they use or interact with?

## Execute

### *Education & Awareness*

**What** - Conduct the necessary education programmes needed to ensure all steps are in place to improve high quality data and information across applications and other systems, and that all data and information exchanged are defined and processes in a consistent way.

**Why** - There must be clear understanding of the steps needed and the responsibilities of those using, accessing, disclosing data and information.

**Whom:**

- SLT/ELT to fund the training and awareness.
- CDIO, HR, people managers, business unit leads, data stewards to define what training is needed.
- Separate business units will need to take responsibility for identifying educational needs and ensuring relevant staff gets trained as needed.
- Data stewards establish the requirements:
    - For 'fit for purpose'
    - To connect those to capability requirements
    - Identify where quality can be improved / delivered
    - System design and functionalities
    - Individual capabilities.
- Communication manager to be responsible for the awareness and communications.
- Architects to define the changes.
- Staff to attend training and to give feedback.

**Example** – Internal newsletters, announcements, meetings and sessions to inform people on data and information interoperability.

**Questions to ask:**

- Is data and information quality linked to daily activities and audited through KPIs?
- Is there an ongoing internal communication process on any aspect of data and information quality, to create awareness within the organisation on the importance of providing highly accurate data and information?
- Is there a process in place to keep the organisation up-to-date regarding the requirements and responsibilities to achieve high quality data and information?
- To what extent does the organisation maintain appropriate records of education, training, skills, and experience?
- Are the results of audits shared within the organisation?
- Are the results on performance indicators communicated within the organisation and if applicable to other organisations and business partners?

### *Application & Software Service Change Management*

**What** - Establish a process to manage application and software service changes within the organisation. Each application and software service change that has an impact on data or information needs to be aligned with the overall DIQM.

**Why** - Having a good process for application and software service changes and the linkage with the DIQM, contributes to quicker and better adoption of new procedures within the organisation to achieve high quality data and information.

**Whom:**

- Architects are responsible for the design of the changes needed
- Change managers are responsible for defining the processes and managing changes

**Example –** The different phases in application and software service change management have these processes:

- Phase 1 – Preparing for application and software service changes:
  - Develop a Request for Change (RfC) specifically focussed on application and software service changes and the impact in data and information.
  - Do an impact assessment
  - Obtain strategic acceptance
- Phase 2 – Managing application and software service changes:
  - Create a detailed planning and activities to implement the changes
  - Apply the application and software service change management
- Phase 3 – Reinforcing application and software service changes:
  - Gather data and report the result of the changes
  - Execute periodic audits
  - Apply corrective actions and recognition

**Questions to ask:**

- Does the organisation have a procedure implemented to facilitate application and software service changes to the DIQM?

## Control / Monitor / Evaluate

***Application & Software Service Validations***

**What** - Monitor the results of the application and software service automated validations in order to track down frequent errors and issues.

**Why** – This activity will allow the identification of commonly recurring errors, which helps the organisation focus in areas that need specific attention.

**Whom –** Governance group and auditors

**Example** – Statistics on most common reasons why applications and software services fail a validation.

**Questions to ask:**

- Does the organisation have a specific process for generating and checking the information of new product and services, prior to first the release?
- Is the output data and information in compliance with standards and accepted measures?
- To what extent does the data and information publishing process include all necessary provisions to ensure that product and service information published can be traced back to its origin?
- Does the review output include decisions and actions to improvement of the effectiveness of the DIQM?

***Application Service Level Controls***

**What** - Track the performance on the agreed KPI's of service levels around applications and software services offered to other organisations and business partners.

**Why** - While service level agreements (SLA's) may not specifically cover data and information quality, the performance on service level goals is a valuable insight into the impact that bad data is having on the organisation's performance.

**Whom –** Governance group and auditors

**Example** – Controlling late metrics for deliveries, order processing, etc.

**Questions to ask:**

- Are the key data identifies that supports the different SLA objectives and goals; that gives the organisation visibility into the information whose improvement can result in direct benefits for the customers?
- Does the organisation make use of standardised monitoring and measuring processes?
- Which monitoring methods on master data management are used within the organisation to evaluate and track the DIQM processes and procedures?
- Are performance indicators defined for each process in the DIQM system?
- To what extent are these performance indicators tracked and communicated?
- To what extent are all corrections suitable, made in both the product master data and the published data?
- Based on the results of the analysis of performance indicators, are the necessary follow-up actions executed?

***Compliance Audits***

**What** - Conducting periodical audits, reports, monitoring of applications and software services to verify that procedures are followed as defined within the DIQM.

**Why** - A process is only as effective as the people executing it want to make it: if the established protocols and procedures are not consistently applied and followed the DIQM system may fail to achieve its goals. Conducting periodical audits is key to guarantee that results are met.

**Whom –** Governance group and auditors

**Example** – Audit on application of defined policies, processes and roles across the organisation.

**Questions to ask:**

- Does the organisation periodically audit the DIQM structure?
- To what extent is the data and information quality policy applied within the organisation?
- Does the organisation review the procedures for data input and creation for adequacy?
- Which monitoring methods on master data management are used within the organisation to evaluate and track the DIQM processes and procedures?
- Based on the results of the analysis of performance indicators, are the necessary follow-up actions executed?
- Is there a process for determining the criteria, scope, frequency and methods for executing internal audits of the DIQM system?
- Does the review input include process performance?
- Does the review input include status of preventative and corrective actions?
- Does the review input include follow-up actions from previous management reviews?
- Does the review input include changes that could affect the DIQM structure?
- Does the review output include decisions and action related to improvement of the effectiveness of the DIQM structure?
- Does the review output include decisions and action related to improvement of the effectiveness of the data quality processes to ensure data quality and accuracy?
- Does the review output include decisions and action related to improvement of customer related requirements with respect to DIQM?

# Infrastructure

## Description

The *Infrastructure* dimension describes the technology infrastructures that support the application and business processes of the organisation. It may include insourced, outsourced or cloud capabilities. The reference model includes sub-dimensions for facilities, platforms, networks, and end user devices.

At an AoG level, it guides the development and maintenance of common capabilities and the sharing and reuse of infrastructure to reduce costs, increase interoperability across organisations, support efficient acquisition and deployment, and enable greater access to information across organisations.

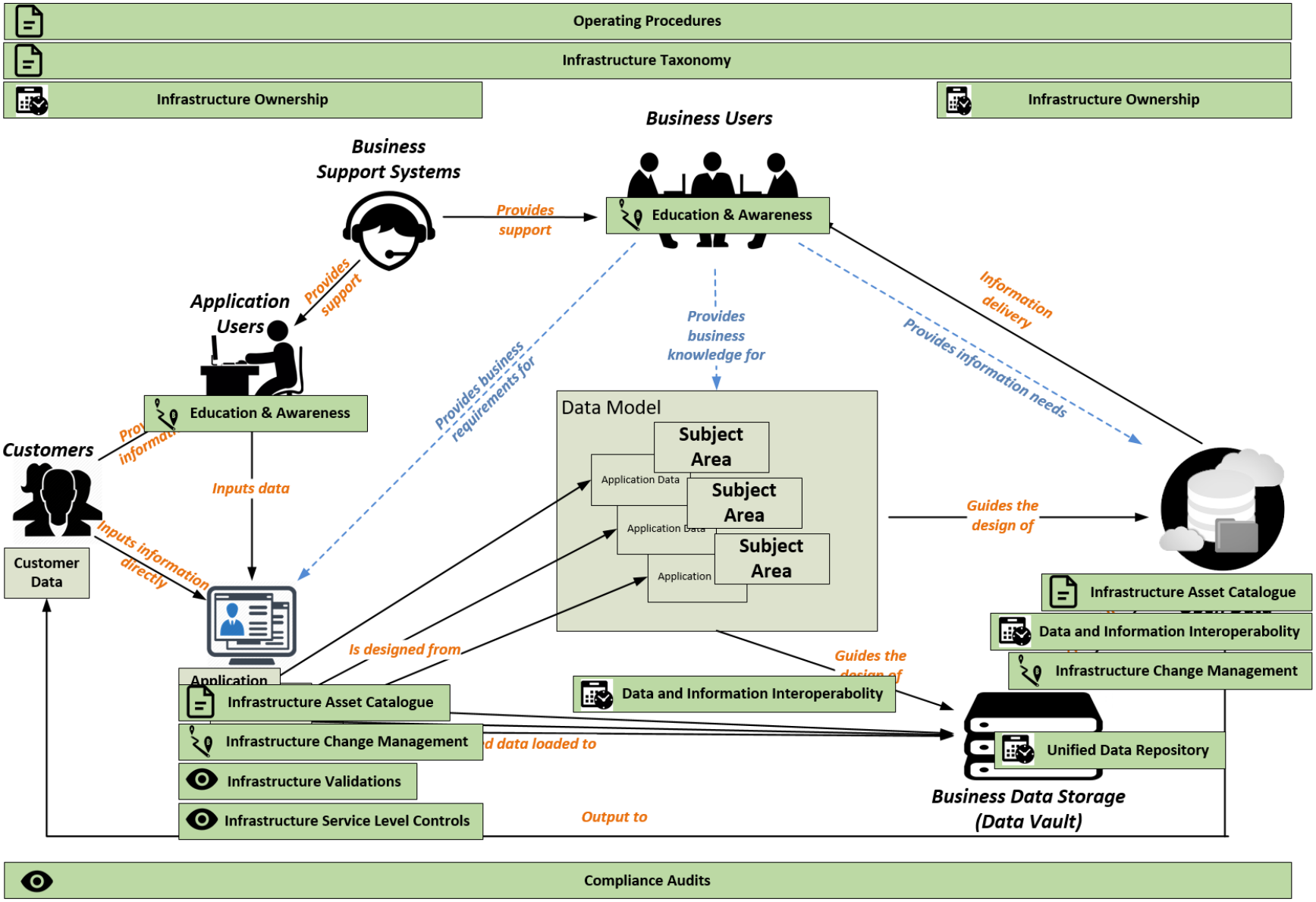
At an agency level, it describes the infrastructure assets of the agency, and helps asset management. It also helps organisations plan their migrations away from internally owned and managed infrastructure to cloud and common capability of offerings as required in the Government ICT Strategy.

## Context and Relationships

| | | |
|---|---|---|
| **Infrastructure** | helps policy compliance through the adoption of common capabilities | **Strategy, Investment, and Policy** |
| | provides the infrastructure that enables Governance and Performance measurement and control, and offers opportunities to improve business efficiency through sharing and reuse | **Governance and Performance** |
| | provides the infrastructure that support business services, processes, capabilities, information sharing, and reuse | **Business** |
| | provides the infrastructure to support storage and exchange of data | **Data and Information** |
| | provides the internal or external infrastructure for hosting applications and software services | **Application and Software Services** |
| | provides the infrastructure controls needed to support identity, privacy, and security requirements | **Identity, Privacy, and Security** |
| | sets the infrastructure requirements that drive development and scope of corresponding standards | **Standards** |

# Components Overview

This diagram gives you a visual overview of the different components within the *Infrastructure* dimension.



# Components

## Plan

### *Infrastructure Ownership Model*

**What** – Define clear roles and responsibilities for all infrastructure assets that the organisation owns, uses, or interacts with.

**Why** - Clear infrastructure ownership is fundamental for reliable governance of infrastructure and interoperability.

**Whom:**

- Executive Leadership Team is responsible for identifying the need for an infrastructure ownership model.
- HR is responsible for creating job descriptions and hiring or uplifting skills to align with an infrastructure owner role.
- Chief Privacy Officer, Chief Security Officer, and line managers contribute to defining responsibilities and skills needed.

**Questions to ask:**

- Do the people who are appointed have the responsibility and authority to ensure that infrastructure needed are procured, installed correctly, implemented and maintained?
- Are the responsibilities balanced within their reach within the organisation and that support exists for them across multiple levels in the organisation?
- Has the division of responsibilities been recorded and communicated throughout the organisation?

### *External Publication*

**What** – Define system requirements for the tools that will be used to publish data and information externally (i.e. beyond the organisation's firewall, such as to other organisations or business partners, etc.). 'Publish' includes distribution, dissemination, and sharing of information.

**Why** - Internal and external definitions for data and information may be in some cases different and therefore all systems to be used for external publication must help verify that the data and information conforms to the right specifications of the intended external audience.

**Whom –** Communication group

**Example** - Limiting the types of changes to data and information once it has been logged in for external publication.

**Questions to ask:**

- Is there a process in place to identify and communicate changes/corrections to data and information?
- Have critical success factors (key elements that ensure a satisfactory performance) been established in the processes for external data and information publishing?
- Has the organisation established and maintained procedures to control the process of publishing product and service information?
- Does the data and information publishing process include all necessary provisions to ensure that product and service changes published are based upon the most relevant version of the product or service?
- Has the division of responsibilities been recorded and communicated throughout the organisation?

### *Internal Publication*

**What** – Define system requirements for the tools that will be used to publish data and information internally (i.e. within the organisation's firewall, such as to other business units within the organisation, etc.). 'Publish' includes distribution, dissemination, and sharing of information.

**Why** - Internal and external definitions for data and information may be in some cases different and therefore all systems to be used for internal publication must help verify that the data and information conforms to the right specifications of the intended internal audience.

**Whom –** Communication group

**Example** - Quality requirements for data and information that is communicated between different business units.

**Questions to ask:**

- Has the organisation established, maintained, and documented the operational processes needed for internal data and information publishing?
- Has the division of responsibilities been recorded and communicated throughout the organisation?

## Document / Record

***Infrastructure Asset Catalogue***

**What** - A systematically categorized, organized and descriptive collection, list or aggregation of the infrastructure assets and a clear view of where these infrastructure assets are installed and used.

**Why** - One of the primary purposes for the collection of infrastructure asset catalogues is to further the government and organisation information sharing strategy by ensuring a government-wide understanding of infrastructure assets and their interoperability. The infrastructure asset catalogue is used to allow discovery of the data and information exchange across organisations, ultimately resulting in reuse and increased sharing with other organisations and business partners.

**Whom:**

- SLT is accountable for the completeness.
- Product owners are responsible for the completeness around their product and services
- Solution architects are responsible for identifying the metadata
- Everyone is responsible for identifying and adding infrastructure assets to the catalogue.

**Example** – Infrastructure asset catalogue.

**Questions to ask:**

- Has the organisation a view on their infrastructure assets, their interoperability and the information that is exchanged between the organisation and other organisations and business partners?
- Where is the asset catalogue stored?

***Infrastructure Taxonomy***

**What** - The GEA-NZ Infrastructure Reference Taxonomy categorises and describe the New Zealand Government infrastructure assets consistently into domains, which are divided into areas, which have categories.

**Why** - The primary purpose is to discover, describe, manage, protect, share and reuse infrastructure within and across organisations and their business partners.

**Whom:**

- SLT is accountable for the completeness.
- Enterprise architects are responsible for identifying the infrastructure categories
- Everyone is responsible for identifying infrastructure assets and describing and categorising it in the taxonomy.

**Example** – GEA-NZ Infrastructure Reference Taxonomy.

**Questions to ask:**

- Does the organisation use the GEA-NZ Infrastructure Reference Taxonomy to categorise their infrastructure?
- To what extent is the GEA-NZ Infrastructure Reference Taxonomy applied internally?

***Operating Procedures***

**What** – Document the workflows and procedures to operate the infrastructure that support the DIQM system.

**Why** – This will help ensure that infrastructure are utilised correctly and that the infrastructure supports the main objectives set for the DIQM system.

**Whom –** Line managers

**Example** – Integrated workflows that show the interaction with the roles and tasks of the DIQM system.

**Questions to ask:**

- Are these operation procedures integrated with the main workflow of the DIQM system to simplify the workflow definitions?
- Does the organisation make use of standardised monitoring and measuring processes?
- Is there a process in place to identify and communicate changes/corrections to data and information?
- To what extent does the data and information publishing process include all necessary provisions to ensure that product and service information published can be traced back to its origin?

## Execute

***Education & Awareness***

**What** - Conduct the necessary education programmes needed to ensure all infrastructure is in place to improve high quality data and information across systems, and that all data and information exchanged are defined and processes in a consistent way.

**Why** - There must be clear understanding of the infrastructure needed to achieve high quality data and information.

**Whom:**

- SLT/ELT to fund the training and awareness.
- CDIO, HR, people managers, business unit leads, data stewards to define what training is needed.
- Separate business units will need to take responsibility for identifying educational needs and ensuring relevant staff gets trained as needed.
- Data stewards establish the requirements:
    - For 'fit for purpose'
    - To connect those to capability requirements
    - Identify where quality can be improved / delivered
    - System design and functionalities
    - Individual capabilities.
- Communication manager to be responsible for the awareness and communications.
- Architects to define the changes.
- Staff to attend training and to give feedback.

**Example** – Sessions to with specific audience responsible for infrastructure.

**Questions to ask:**

- Is data and information quality linked to daily activities?
- Is there an ongoing internal communication process on any aspect of data and information quality, to create awareness within the organisation on the importance of providing highly accurate data and information?
- Is there a process in place to keep the organisation up-to-date regarding the requirements to achieve high quality data and information?
- To what extent does the organisation maintain appropriate records of education, training, skills, and experience?

- Are the results of audits shared within the organisation?
- Are the results on performance indicators communicated within the organisation and if applicable to other organisations and business partners?

***Infrastructure Change Management***

**What** - Establish a process to manage infrastructure changes within the organisation. Each infrastructure change that has an impact on data or information needs to be aligned with the overall DIQM.

**Why** - Having a good process for infrastructure changes and the linkage with the DIQM, contributes to quicker and better adoption of new procedures within the organisation to achieve high quality data and information.

**Whom:**
- Architects are responsible for the design of the changes needed
- Change managers are responsible for defining the processes and managing changes

**Example –** The different phases in infrastructure change management have these processes:
- Phase 1 – Preparing for infrastructure changes:
    - Develop a Request for Change (RfC) specifically focussed on infrastructure changes and the impact in data and information.
    - Do an impact assessment
    - Obtain strategic acceptance
- Phase 2 – Managing infrastructure changes:
    - Create a detailed planning and activities to implement the changes
    - Apply the infrastructure change management
- Phase 3 – Reinforcing infrastructure changes:
    - Gather data and report the result of the changes
    - Execute periodic audits
    - Apply corrective actions and recognition

**Questions to ask:**
- Does the organisation have a procedure implemented to facilitate infrastructure changes to the DIQM?

## Control / Monitor / Evaluate

***Infrastructure Issue Management***

**What** - Monitor the performance of infrastructure assets in order to track down frequent errors and issues.

**Why** – This activity will allow the identification of commonly recurring errors, which helps the organisation focus in areas that need specific attention.

**Whom –** Governance group and auditors

**Example** – Statistics on infrastructure issues and solutions.

**Questions to ask:**
- Does the organisation have a specific process for generating and checking the information of new product and services, prior to first the release?
- Is the output data and information in compliance with standards and accepted measures?
- To what extent does the data and information publishing process include all necessary provisions to ensure that product and service information published can be traced back to its origin?

- Does the review output include decisions and actions to improvement of the effectiveness of the DIQM?
- If the organisation uses IaaS, does it receive reports on issue management from the provider?

***Infrastructure Service Level Controls***

**What** - Track the performance on the agreed KPI's of service levels around infrastructure offered to other organisations and business partners.

**Why** - While service level agreements (SLA's) may not specifically cover data and information quality, the performance on service level goals is a valuable insight into the impact that bad data is having on the organisation's performance.

**Whom –** Governance group and auditors

**Example** – Controlling late metrics for deliveries, order processing, etc.

**Questions to ask:**
- Are the key data identifies that supports the different SLA objectives and goals; that gives the organisation visibility into the information whose improvement can result in direct benefits for the customers?
- Does the organisation make use of standardised monitoring and measuring processes?
- Which monitoring methods on master data management are used within the organisation to evaluate and track the DIQM processes and procedures?
- Are performance indicators defined for each process in the DIQM system?
- To what extent are these performance indicators tracked and communicated?
- To what extent are all corrections suitable, made in both the product master data and the published data?
- Based on the results of the analysis of performance indicators, are the necessary follow-up actions executed?

***Compliance Audits***

**What** - Conducting periodical audits on infrastructure to verify that procedures are followed as defined within the DIQM.

**Why** - A process is only as effective as the people executing it want to make it: if the established protocols and procedures are not consistently applied and followed the DIQM system may fail to achieve its goals. Conducting periodical audits is key to guarantee that results are met.

**Whom –** Governance group and auditors

**Example** – Audit on infrastructure of defined policies, processes and roles across the organisation.

**Questions to ask:**
- Does the organisation periodically audit the DIQM structure?
- To what extent is the data and information quality policy applied within the organisation?
- Does the organisation review the procedures for data input and creation for adequacy?
- Which monitoring methods on master data management are used within the organisation to evaluate and track the DIQM processes and procedures?
- Based on the results of the analysis of performance indicators, are the necessary follow-up actions executed?
- Is there a process for determining the criteria, scope, frequency and methods for executing internal audits of the DIQM system?
- Does the review input include process performance?
- Does the review input include status of preventative and corrective actions?
- Does the review input include follow-up actions from previous management reviews?
- Does the review input include changes that could affect the DIQM structure?
- Does the review output include decisions and action related to improvement of the effectiveness of the DIQM structure and processes to ensure data quality and accuracy?
- Does the review output include decisions and action related to improvement of customer related requirements with respect to DIQM?

# Identity, Privacy, and Security

## Description

The Identity, Privacy, and Security dimension does not prescribe a "new" approach to comprehensive information management but rather gives the context to system or service Identity, Privacy and Protective Security requirements and other artefacts that guide security and privacy considerations through the information life-cycle. These apply to all Organisations for all dimensions of their architectures, and can be considered as its own eco-system supporting all of business.

The Government Chief Privacy Officer (GCPO) has issued core expectations that represent good practice for privacy management and governance in the State services. A Privacy Maturity Assessment Framework has also been developed to help organisations assess their existing capability and implement appropriate improvements. Technology is an important part of the solution to improving capability in privacy management across government.

Governance and accountability arrangements for security and privacy will vary within organisations, but Architecture has a role to play in ensuring that security and privacy management is applied systematically and comprehensively at all scales, from AoG planning through sector information management down to individual component designs within agency applications.

At all levels and life-cycle phases, there are standards, rules, guidelines and other artefacts which the agency's Enterprise Architecture should reflect. These include security and privacy standards, best practice guidelines, threat and vulnerability taxonomies, security risk management processes, risk registers, and control catalogues,. There are also monitoring, auditing, assurance, reporting (including by and to external third parties) plans and improvement plans.

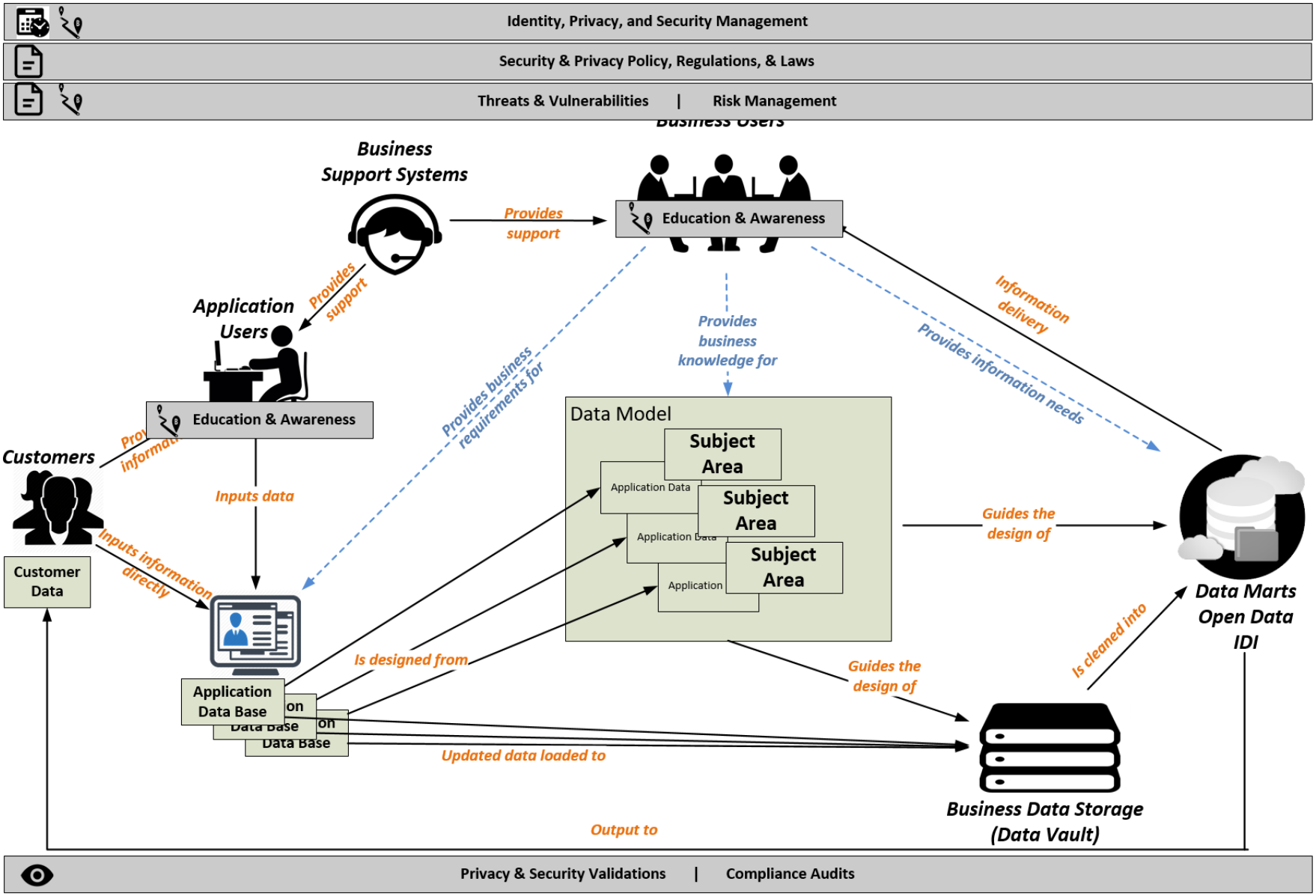
## Context and Relationships

| | | |
|---|---|---|
| **Identity, Security. and Privacy** | identifies access, security, privacy, but also ethical, confidentiality, and the right to be forgotten[25] considerations for strategy, investment, and policy development | **Strategy, Investment, and Policy** |
| | provides access, security, and privacy inputs and constraints for governance and performance measurement and control | **Governance and Performance** |
| | provides access, security, and privacy information, tools and standards that secure customer interests, channels, business services, and processes | **Business** |
| | provides access, security, and privacy input and constraints for collection, storage and exchange of information | **Data and Information** |
| | provides access, security, and privacy information, tools and standards that secure applications and software services | **Application and Software Services** |
| | provides access, security, and privacy information, tools and standards that secure infrastructure | **Infrastructure** |
| | defines access, security, and privacy standards and implementation guidelines | **Standards** |

[25] The *right to be forgotten* is also part of Identity, Privacy, and Security, it is a concept that has been discussed and put into practice in both the European Union (EU), and Argentina since 2006. The issue has arisen from desires of individuals to "determine the development of their life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past.

# Components Overview

This diagram gives you a visual overview of the different components within the *Identity, Privacy, and Security* dimension.



# Components

## Plan

***Privacy & Security Management***

**What** - Define responsibilities and processes for the management and maintenance of all privacy and security aspects that support and guide the DIQM. Define specific policies for the safeguard of the integrity of the data and information, in terms of accessibility, edit-rights, privacy, intellectual property, etc. This is to be defined by data subject and by need to know as well as for actual data manipulation. Policies must cover deletion and disclosure and duplication permissions together with obligations to advise any secondary receivers of information should there be changes to the 'source' data.

**Why** - In order to maintain a cycle of continuous improvements, it is important to ensure that the guiding privacy and security principles and policies of the DIQM can evolve along with the organisation. These principles and policies and their enforcement are necessary to protect the data's integrity.

**Whom:**

- Executive Leadership Team, Chief Privacy Officer, Chief Security Officer, Information owner, and data custodians are responsible for defining the policy around privacy and security.
- Chief Privacy Officer, and Chief Security Officer responsible for managing all aspects of privacy and security within the organisation
- Enterprise, Security, and Data architects contribute to designing the rules around privacy and security
- Development responsible for the implementation of the privacy and security rules.

**Example** – Different access levels (edit, read-only, etc.) given to people depending on their role in the process.

**Questions to ask:**

- Does the organisation have a data and information privacy and security principles and policy suitably documented and audited?
- Does the organisation have rules, controls, and procedures in place around the use of personal information (ethics, human rights, machine decisions, etc.)?
- Is there a clear internal responsibility for the different elements that need to be maintained?
- Is everyone within the organisation aware of the importance of adopting/reviewing/revising all privacy and security processes to achieve high quality data and information ?
- To what extent does the repository have access authorisation procedures?
- Does the organisation have an identity and access management procedure in place?
- Does the organisation have a structure in place to ensure the security of data from unauthorised change Including deletions, destruction, disclosures/transfers?
- Does information publishing[26] procedure include: appropriate authorisation, and procedures for ensuring appropriately cleansed/redacted prior to release/disclosure?
- Are Users are familiar with the requirements that apply to them and where the limits of their access/usage?
- Are the privacy and security principles and policies enforced by the governance model?
- What responsibilities (security, privacy, access) has the organisation around employee information? What happens to the employee information when that person leaves the organisation?
- Does the organisation has archiving and decommissioning procedure in place, and does all privacy, security, ethics, and confidentiality requirements are considered when archiving and decommissioning?
- Does the organisation know where its entire information asset resides physically?
- Does the organisation have rules and procedures in place around cloud (jurisdiction), eDiscovery, and archiving, multi-tenant environment?

[26] See Internal/External Publication

## Document / Record

***Privacy & Security Policies, Regulations & Laws***

**What** - Record of all strategic and guiding policies, regulations and laws around privacy and security at government, sector and agency level.

**Why** - Formal documented policies, regulations and laws are essential to allow the organisation to refer back to the original vision and objectives in order to remain on scope.

**Whom:**

- Executive Leadership Team, Chief Privacy Officer, and Chief Security Officer are responsible for defining the policy around privacy and security.
- Chief Privacy Officer, and Chief Security Officer responsible for managing all aspects of privacy and security within the organisation
- Enterprise, Security, and Data architects contribute to designing the rules around privacy and security
- Development responsible for the implementation of the privacy and security rules.

**Example** – Privacy Act; Public Records Act; NZISM; Protective Security Requirements (PSR); NZ Cyber Security Strategy (DPMC); AS/NZS ISO 31000:2009 Risk Management; ISO 27000-series security and privacy framework standards.

**Questions to ask:**

- Does the DIQM documentation include privacy and security requirements, objectives, targets, and review / revision points?
- Are at least the regulatory and mandated PSR/NZISM controls documented in the DIQM?
- To what extent are the objectives on DIQM measurable?
- Are these documents and records stored in a repository that has a role-based access with appropriate restrictions and routine and triggered (e.g. for high risk areas/personnel/data) audit?

***Threat & Vulnerability Model***

**What** - Threat and vulnerability modeling is an approach for analysing the privacy and security of applications and software services. It is a structured approach that enables the organisation to identify, quantify, and address the privacy and security risks associated with an application or a software service.

**Why -** Threat and vulnerability modeling allows the organisation to systematically identify and rate the threats that are most likely to affect systems or services. By identifying and rating threats based on a solid understanding of the architecture and implementation of applications and software services, the organisation can address threats with appropriate countermeasures in a logical order, starting with the threats that present the greatest risk, including consideration of dependencies (e.g. if A then B so fix A first). Threat and vulnerability modeling has a structured approach that is far more cost efficient and effective than applying security features in a haphazard

**Whom:**

- Chief Privacy Officer and Chief Security Officer responsible for identifying the threats and vulnerabilities within the organisation, also to identify the mitigation plans.
- Enterprise, Security and Data architects responsible for designing the model
- Development responsible for the implementation of the privacy and security rules.

**Example –** Threat and vulnerability modelling process that the organisation can perform:

- **Identify and document assets**: Identify the valuable assets that systems must protect.
- **Create an architecture overview**: Use simple diagrams and tables to document the architecture of applications, including subsystems, cloud services, trust boundaries, and data flow.
- **Decompose the application**: Decompose the architecture of applications, including the underlying network and host infrastructure design, to create a security profile for the application. The aim of the security profile is to uncover vulnerabilities in the design, implementation, or deployment configuration of applications.
- **Identify the threats and vulnerabilities**: Keeping in mind that the main risk to any organisation comes from within – staff (whether malicious, negligent or incompetent), and with knowledge of the architecture and potential vulnerabilities of your application, identify the threats that could affect the application.
- **Document the threats and vulnerabilities**: Document each threat and vulnerability using a common threat and vulnerability template that defines a core set of attributes to capture for

each threat or vulnerability.

- **Rate the threats and vulnerabilities**: Rate the threats and vulnerabilities to prioritize and address the most significant threats first as these present the biggest risk. These threats present the biggest risk. The rating process weighs the probability of the threat against damage that could result should an attack occur as well as the cost of any mitigation actions. It might turn out that certain threats do not warrant any action when compared with the risk posed by the threat with the resulting mitigation costs, the account the non-financial costs, including lost opportunity costs of inaction/action options.
- **Put mitigations in place:** check they work through audit/penetration testing etc.; review and revise as needed (and in time to ensure any issues caught promptly and when able to be most effective in remediation).

**Questions to ask:**

- To what extent does the DIQM documentation contain the threats and vulnerability both to the organisation and staff, and to the individuals/subjects/customers?

***Risk Management Procedures***

**What** - Identify and assess possible risks, and document risk-assessments criteria in order to prioritise/evaluate actions carried out in the DIQM.

**Why** - Clear risk assessment helps an organisation focus on the actions that deliver the greatest value and support to general organisational objectives.

**Whom –** Risk Assurance group

**Example – Risk-assessment matrix and heat map[27].**

| | | | | | |
|---|---|---|---|---|---|
| **5 - Severe** | **15** | **19** | **22** | **24** | **25** |
| **4 - Significant** | **10** | **14** | **18** | **21** | **23** |
| **3 - Moderate** | **6** | **9** | **13** | **17** | **20** |
| **2 - Minor** | **3** | **5** | **8** | **12** | **16** |
| **1 - Minimal** | **1** | **2** | **4** | **7** | **11** |
| | **1 - Almost never** | **2 - Possible but unlikely** | **3 - Possible** | **4 Highly possible** | **5 - Almost certain** |

Key: Inherent risk assessment; Redidual risk assessmnet

| Zone | Escalation path | Escalated to |
|---|---|---|
| **Extreme** | Risk must be escalated to the Deputy Chief Executive via the Executive or Business / System owner at the first possible opportunity. GCIO Assurance Lead updated on the risk. | DCE Business Owner via previous escalations first. |
| **High** | Risk must be escalated to the Business / System Owner | Business / System Owner via the Operational Manager if appropriate. |
| **Medium** | Risk can be managed and monitored by the operational manager (Technical and Business) | Operational Manager (Technical and Business) |
| **Low** | | |

[27] See ICT Assurance Framework

**Questions to ask:**

- To what extent does the documentation of the DIQM structure contains the risk identification, risk assessment, risk control, and risk mitigation actions?
- Are these criteria on the assessment of risks consistent with other risk areas?

## Execute

***Education & Awareness***

**What** - Conduct the necessary education programmes needed to ensure all privacy, security, and ethical measurements are in place and being analysed by staff within the agency to improve high quality data and information across systems, and that all data and information exchange and processes are defined and implemented in a consistent way. Education also includes customer/staff interface – e.g. education of the public about agency processes/practice as well as staff (needs-based-training and verification of learnings).

**Why** - There must be clear understanding of the privacy and security measurements needed to achieve high quality data and information. Need to ensure different needs identified at different points in time and across the organisation. Everyone needs to be aware (and variably accountable – e.g. through HR requirements, KPIs etc.) – collective AND individual responsibilities.

**Whom:**

- SLT/ELT to fund the training and awareness. They also are the recipient of the reporting on a regular bases (should be part of the monthly agenda), so improvement can be agreed upon as soon as possible.
- CDIO, HR, people managers, business unit leads, data stewards to define what training is needed.
- Separate business units will need to take responsibility for identifying educational needs and ensuring relevant staff gets trained as needed.
- Data stewards establish the requirements:
    - For 'fit for purpose'
    - To connect those to capability requirements
    - Identify where quality can be improved / delivered
    - System design and functionalities
    - Individual capabilities.
- Communication manager to be responsible for the awareness and communications to the wider organisation and outside (Public facing, to Ministers/ELT, etc. ) around everyone's responsibilities, e.g. for communication to staff, contractors, 3rd parties, front-line staff direct to 'customers' etc.
- Architects to define the changes.
- Staff to attend training and to give feedback. Uptake/learnings need to be reviewed/monitored.

**Example** – Include data and information security and privacy aspects in internal newsletters, announcements, meetings and staff workshop sessions.

**Questions to ask:**

- Is data and information privacy and security linked to daily activities and KPIs?
- Is there an ongoing internal communication process on any aspect of data and information quality, to create awareness within the organisation on the importance risks, outcomes, and dependencies (including relating to /arising from/for staff, individuals, and organisation)?
- Is there a process in place to keep the organisation up-to-date regarding the requirements to achieve high quality data and information?
- To what extent does the organisation maintain appropriate records of education, training, skills, and experience?
- Are the results of audits shared within the organisation?
- Are the results on performance indicators communicated within the organisation and if applicable to 3rd party service providers?

***Privacy & Security Management***

**What** - Establish a process to manage privacy and security policy changes within the organisation. Each change that has an impact on data or information and need process to identify what will constitute a change and how it will be identified (i.e. iterative/step-wise PIAs etc.) needs to be aligned with the overall DIQM.

**Why** - Having a good process for privacy and security policy changes and the linkage with the DIQM, contributes to quicker and better adoption of new procedures within the organisation to achieve high quality data and information.

**Whom:**

- Executive Leadership Team, Chief Privacy Officer, and Chief Security Officer are responsible for defining the policy around privacy and security.
- Chief Privacy Officer, and Chief Security Officer responsible for managing all aspects of privacy and security within the organisation
- Enterprise, Security, and Data architects contribute to designing the rules around privacy and security
- Development responsible for the implementation of the privacy and security rules.

**Example –** The different phases in privacy and security policy change management may have these processes:

- Phase 0 – identifying the need for a change.
- Phase 1 – Preparing for privacy and security policy changes:
    - Develop a Request for Change (RfC) specifically focussed on privacy and security policy changes and the impact in data and information.
    - Do an impact assessment
    - Obtain strategic acceptance
- Phase 2 – Managing privacy and security policy changes:
    - Create a detailed planning and activities to implement the changes
    - Apply the privacy and security policy change management
- Phase 3 – Reinforcing privacy and security policy changes:
    - Gather data and report the result of the changes
    - Execute periodic audits
    - Apply corrective actions, recognition, and embed – ongoing review/revision/audit programmes etc.

**Questions to ask:**

- Does the organisation have a procedure implemented, documented, disseminated, reviewed etc. to facilitate privacy and security policy changes to the DIQM?

***Risk Management***

**What** - Establish a process to manage risks within the organisation. Each risk that has an impact on data or information needs to be aligned with the overall DIQM. Managing risks is a process that includes risk assessment and a mitigation strategy for those risks. Risk assessment includes both the identification of potential risk and the evaluation of the potential impact of the risk. A risk mitigation plan is designed to eliminate or minimize the impact of the risk events—occurrences that have a negative impact.

**Why** - Having a good process for risk management and the linkage with the DIQM, contributes to quicker and better adoption of new procedures within the organisation to achieve high quality data and information and therefore same for outcomes etc.

**Whom –** Risk Assurance group

**Example –** The different phases in infrastructure change management have these processes:

- Describe the processes for identifying risk.
- Describe the processes for evaluating risk.
- Identify the major elements in managing risk.
- Describe the processes for mitigating risk

**Questions to ask:**

- Does the organisation have a procedure implemented to facilitate risk management to the DIQM?

## Control Monitor / Evaluate

***Privacy & Security Validations***

**What** - Monitor the results of the privacy and security validations in order to track down threats, vulnerabilities, errors and issues, and effect of implementing NZISM/PSR controls.

**Why** – This activity will allow the identification of threats and vulnerabilities, which helps the organisation focus in areas that need specific attention.

**Whom:**

- Executive Leadership Team, Chief Privacy Officer, and Chief Security Officer are responsible for defining the policy around privacy and security.
- The Contract Owner is responsible for privacy and security around cloud services.
- Chief Privacy Officer, and Chief Security Officer responsible for managing all aspects of privacy and security within the organisation
- Governance group and auditors responsible for conducting validations

**Example** – Statistics on threats and vulnerabilities, including changes in threats/vulnerabilities and drivers/impacts.

**Questions to ask:**

- Does the organisation have a specific process for generating and checking the information of new product and services, the impact, dependencies, etc. prior to first the release?
- Is the output data and information in compliance with standards and accepted measures? And have requirements been comprehensively identified?
- To what extent does information publishing[28] process include all necessary provisions to ensure that product and service information published can be traced back to its origin?
- Does the review output include decisions and actions to improvement of the effectiveness of the DIQM?

***Compliance Audits***

**What** - Conducting periodical audits on privacy and security policy implementation to verify that procedures are followed as defined within the DIQM.

**Why** - A process is only as effective as the people executing it want to make it: if the established protocols and procedures are not consistently applied and followed the DIQM system may fail to achieve its goals. Conducting periodical audits, implementation of consequent actions / remediation and checking to assure their ongoing effectiveness / suitability for purpose is key to guarantee that results are met.

**Whom:**

- Executive Leadership Team, Chief Privacy Officer, and Chief Security Officer are responsible for defining the policy around privacy and security.
- Chief Privacy Officer, and Chief Security Officer responsible for managing all aspects of privacy and security within the organisation
- Governance group and auditors responsible for conducting the audits.

**Example** – Audit on privacy and security defined policies, processes, roles, activities and externalities (if these change, or if statutory authorities change etc.) underlying basis for process/procedure/policy may no longer apply/remain unchanged.

**Questions to ask:**

- Does the organisation periodically audit the DIQM structure?
- To what extent is the data and information quality policy applied within the organisation?

---

[28] See Internal/External Publication

- Does the organisation review the procedures for data input and creation for adequacy?
- Which monitoring methods on master data management are used within the organisation to evaluate and track the DIQM processes and procedures?
- Is there “One source of truth”?
- Are there procedures for identifying changes in sub-sets of data? Or for addressing information that has been transferred to a 3rd party?
- Based on the results of the analysis of performance indicators, are the necessary follow-up actions executed?
- Is there a process for determining the criteria, scope, frequency and methods for executing internal audits of the DIQM system?
- Does the review input include process performance?
- Does the review input include status of preventative and corrective actions?
- Does the review input include follow-up actions from previous management reviews?
- Does the review input include changes that could affect the DIQM structure?
- Does the review output include decisions and action related to improvement of the effectiveness of DIQM structure?
- Does the review output include decisions and action related to improvement of the effectiveness of DIQM processes to ensure data quality and accuracy?
- Does the review output include decisions and action related to improvement of customer related requirements, collection, use, disclosure, up-dating with respect to DIQM?

# Standard

## Description

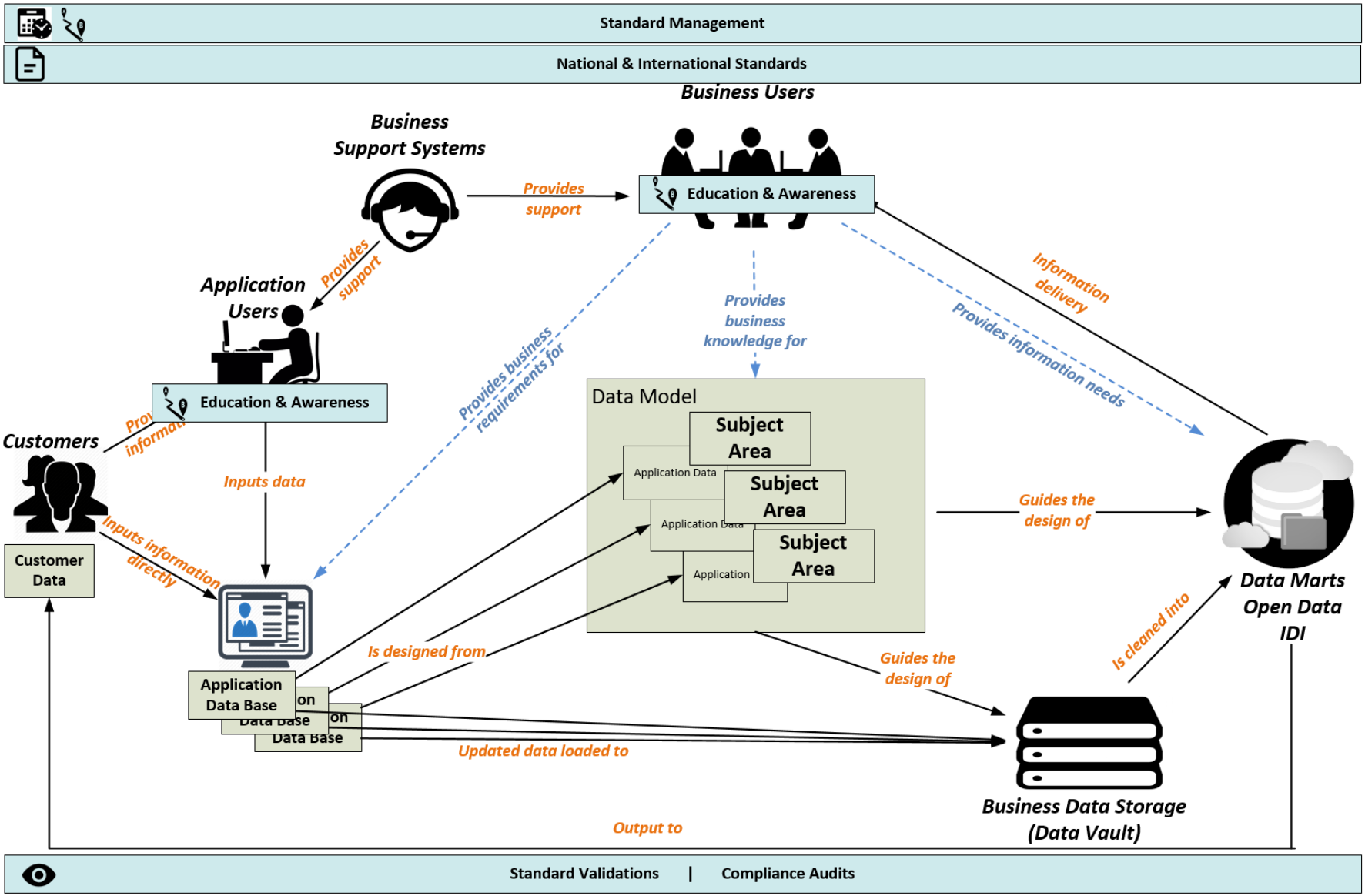
The *Standards* dimension sets out and categorises the information and technology standards base for the NZ government.

## Context and Relationships

| | | |
|---|---|---|
| **Standards** | identifies standards for compliance and improved collaboration | **Strategy, Investment, and Policy** |
| | provides standards inputs for setting governance and performance measurement and control | **Governance and Performance** |
| | provides standards that guide business services, processes, capabilities, information sharing, and reuse | **Business** |
| | provides standards that guide data and information | **Data and Information** |
| | provides standards that guide application and software services | **Application and Software Services** |
| | provides standards that guide infrastructure | **Infrastructure** |
| | defines standards and implementation guidelines | **Identity, Privacy, and Security** |

# Components Overview

This diagram gives you a visual overview of the different components within the *Standard* dimension.



# Components

## Plan

***Standard Management***

**What** - Define responsibilities and processes for the management and maintenance of all national, international, regional, and organisational standards and approved guidelines that support and guide the DIQM.

**Why** - In order to maintain a cycle of continuous improvements, it is important to ensure that the standards and approved guidelines of the DIQM can evolve along with the organisation. These standards and approved guidelines and their enforcement are necessary to ensure high quality data and information.

**Whom:**

- Executive Leadership Team is responsible for defining the policy around standards and approved guidelines.
- Standard experts are responsible for identifying which standards and approved guidelines are needed within the organisation
- Everyone for the implementation of the standards and approved guidelines.

**Example** – Awareness and understanding of Government standards and approved guidelines to maintain standards updated for the organisation.

**Questions to ask:**

- Does the organisation has data and information standards and approved guidelines policy?
- Is there a clear internal responsibility for the different elements that need to be maintained?
- Is everyone within the organisation aware of the importance of adopting standards and approved guidelines to achieve high quality data and information?
- Are the standard principles and policies enforced by the governance model?

## Document / Record

***National & International Standards***

**What** - Record of all national, international, regional, and organisational standards and approved guidelines used by government, sector and agency level.

**Why** - Formal documented standards and approved guidelines are essential to allow the organisation to refer back to the organisational vision and objectives in order to remain on scope.

**Whom:**

- Executive Leadership Team is responsible for defining the policy around standards and approved guidelines.
- Standard experts are responsible for identifying which standards and approved guidelines are needed within the organisation
- Everyone for the implementation of the standards and approved guidelines.

**Example** – GEA-NZ Standards – these are one of the technical interoperability standards.

**Questions to ask:**

- Does the DIQM documentation includes national, international, regional, and organisational standards and approved guidelines?
- Are these documents and records stored in a repository that can be accessed by anyone within the organisation?

## Execute

### *Education & Awareness*

**What** - Conduct the necessary education programmes needed to ensure all applied standards are in place to improve high quality data and information across systems, and that all data and information exchanged are defined and processes in a consistent way.

**Why** - There must be clear understanding of the standards and approved guidelines needed to achieve high quality data and information.

**Whom:**

- SLT/ELT to fund the training and awareness.
- CDIO, HR, people managers, business unit leads, data stewards to define what training is needed.
- Separate business units will need to take responsibility for identifying educational needs and ensuring relevant staff gets trained as needed.
- Data stewards establish the requirements:
    - For 'fit for purpose'
    - To connect those to capability requirements
    - Identify where quality can be improved / delivered
    - System design and functionalities
    - Individual capabilities.
- Communication manager to be responsible for the awareness and communications.
- Architects to define the changes.
- Staff to attend training and to give feedback.

**Example** – Internal newsletters, announcements, meetings and sessions to inform people on standards and approved guidelines.

**Questions to ask:**

- Is data and information quality linked to daily activities?
- Do staff understand their roles and responsibilities? Is it included in the induction pack, etc.?
- Is there an ongoing internal communication process on any aspect of data and information quality, to create awareness within the organisation on the importance of providing highly accurate data and information?
- Is there a process in place to keep the organisation up-to-date regarding the requirements to achieve high quality data and information?
- To what extent does the organisation maintain appropriate records of education, training, skills, and experience?
- Are the results of audits shared within the organisation?
- Are the results on performance indicators communicated within the organisation and if applicable to 3rd party service providers?

### *Standard Management*

**What** - Establish a process to manage standards within the organisation. Each standard that has an impact on data or information needs to be aligned with the overall DIQM.

**Why** - Having a good process for standards and approved guidelines and the linkage with the DIQM, contributes to quicker and better adoption of new procedures within the organisation to achieve high quality data and information.

**Whom:**

- Executive Leadership Team is responsible for defining the policy around standards and approved guidelines.
- Standard experts are responsible for identifying which standards and approved guidelines are needed within the organisation
- Everyone for the implementation of the standards and approved guidelines.

**Example** – Process to internally review and adopt new standards and approved guidelines.

**Questions to ask:**

- Is there a process in place to keep the organisation up-to-date regarding new standards and approved guidelines?
- To what extent does the review include assessing opportunities for improvement and the need for changes to the DIQM structure, including the DIQM policy and objectives?

## Control / Monitor / Evaluate

***Standard Validations***

**What** - Monitor the results of the standards and approved guidelines validations in order to track down inconsistency, errors and issues. Keep a metadata trail from creation, to archiving, to disposal, because authenticity and reliability depends on this. This is key for decision making.

**Why** – This activity will allow the identification of inconsistency, errors and issues, which helps the organisation focus in areas that need specific attention.

**Whom:**

- Executive Leadership Team, Chief Privacy Officer, and Chief Security Officer are responsible for defining the policy around standards and approved guidelines.
- Standards experts are responsible for identifying for the measurements for validation around standards and approved guidelines
- Governance group and auditors responsible for conducting validations

**Example** – Statistics on standards and approved guidelines inconsistencies, errors and issues.

**Questions to ask:**

- Does the organisation have a specific process for generating and checking the information of new product and services, prior to first the release?
- Is the output data and information in compliance with standards and accepted measures?
- To what extent does the data and information publishing[29] process include all necessary provisions to ensure that product and service information published can be traced back to its origin?
- Does the organisation keep a trail of the metadata from creation to archiving to disposal?
- Does the review output include decisions and actions to improvement of the effectiveness of the DIQM?

***Compliance Audits***

**What** - Conducting periodical audits on standards and approved guidelines implementation to verify that procedures are followed as defined within the DIQM.

**Why** - A process is only as effective as the people executing it want to make it: if the established protocols and procedures are not consistently applied and followed the DIQM system may fail to achieve its goals. Conducting periodical audits is key to guarantee that results are met.

[29] See Internal/External Publication

**Whom:**

- Executive Leadership Team, Chief Privacy Officer, and Chief Security Officer are responsible for defining the policy around standards and approved guidelines.
- Standards experts are responsible for identifying for the compliance requirements
- Governance group and auditors responsible for conducting audit

**Example** – Audit on standard defined policies, processes and roles across the organisation.

**Questions to ask:**

- Does the organisation periodically audit the DIQM structure?
- To what extent is the data and information quality policy applied within the organisation?
- Does the organisation review the procedures for data input and creation for adequacy?
- Which monitoring methods on master data management are used within the organisation to evaluate and track the DIQM processes and procedures?
- Based on the results of the analysis of performance indicators, are the necessary follow-up actions executed?
- Is there a process for determining the criteria, scope, frequency and methods for executing internal audits of the DIQM system?
- Does the review input include process performance?
- Does the review input include status of preventative and corrective actions?
- Does the review input include follow-up actions from previous management reviews?
- Does the review input include changes that could affect the DIQM structure?
- Does the review output include decisions and action related to improvement of the effectiveness of the DIQM structure?
- Does the review output include decisions and action related to improvement of the effectiveness of the DIQM processes to ensure data quality and accuracy?
- Does the review output include decisions and action related to improvement of customer related requirements with respect to DIQM?

# Appendix A – Focus Area Diagrams

The four focus areas we use are: Plan, Document / Record, Execute, and Control / Monitor / Evaluate.

## Plan

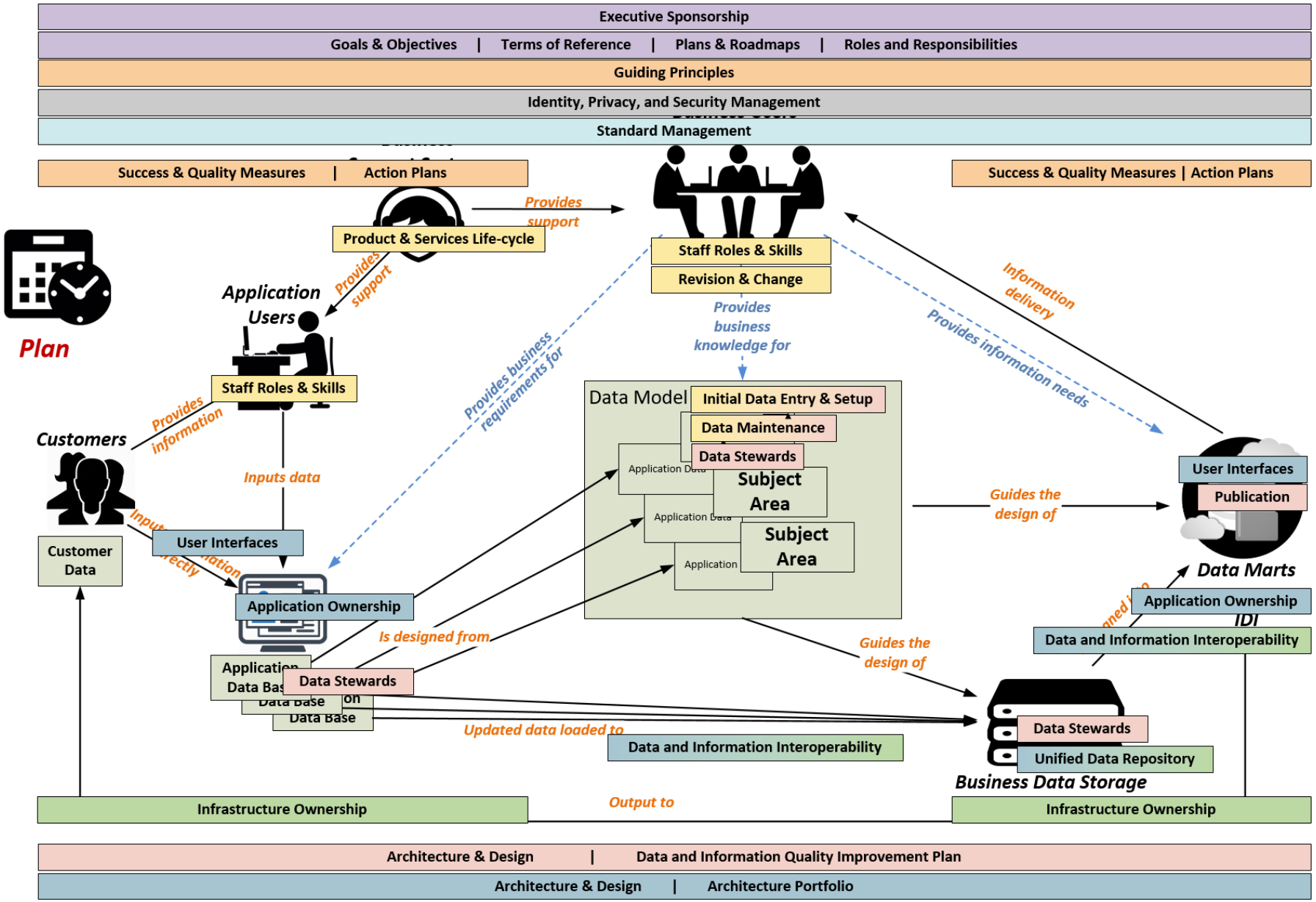
To *Plan* is typically to create a list of steps with timing and resources, used to achieve an objective to do something. It is commonly understood as a temporal set of intended actions through which one expects to achieve a goal. Plans can be formal or informal.

This icon will be used to indicate a planning component on diagrams. 

The most popular ways to describe plans are by their breadth, time frame, and specificity; however, these planning classifications are not independent of one another. For instance, there is a close relationship between the short- and long-term categories and the strategic and operational categories.

It is common for less formal plans to be created as abstract ideas, and remain in that form as they are maintained and put to use. More formal plans are initially created with and as an abstract thought, and are likely to be written down, drawn up or otherwise stored in a form that is accessible to multiple people across time and space. This allows more reliable collaboration in the execution of the plan.

There are several Plan activities that need to be considered to make sure the data and information an organisation uses for decision making is of high quality:

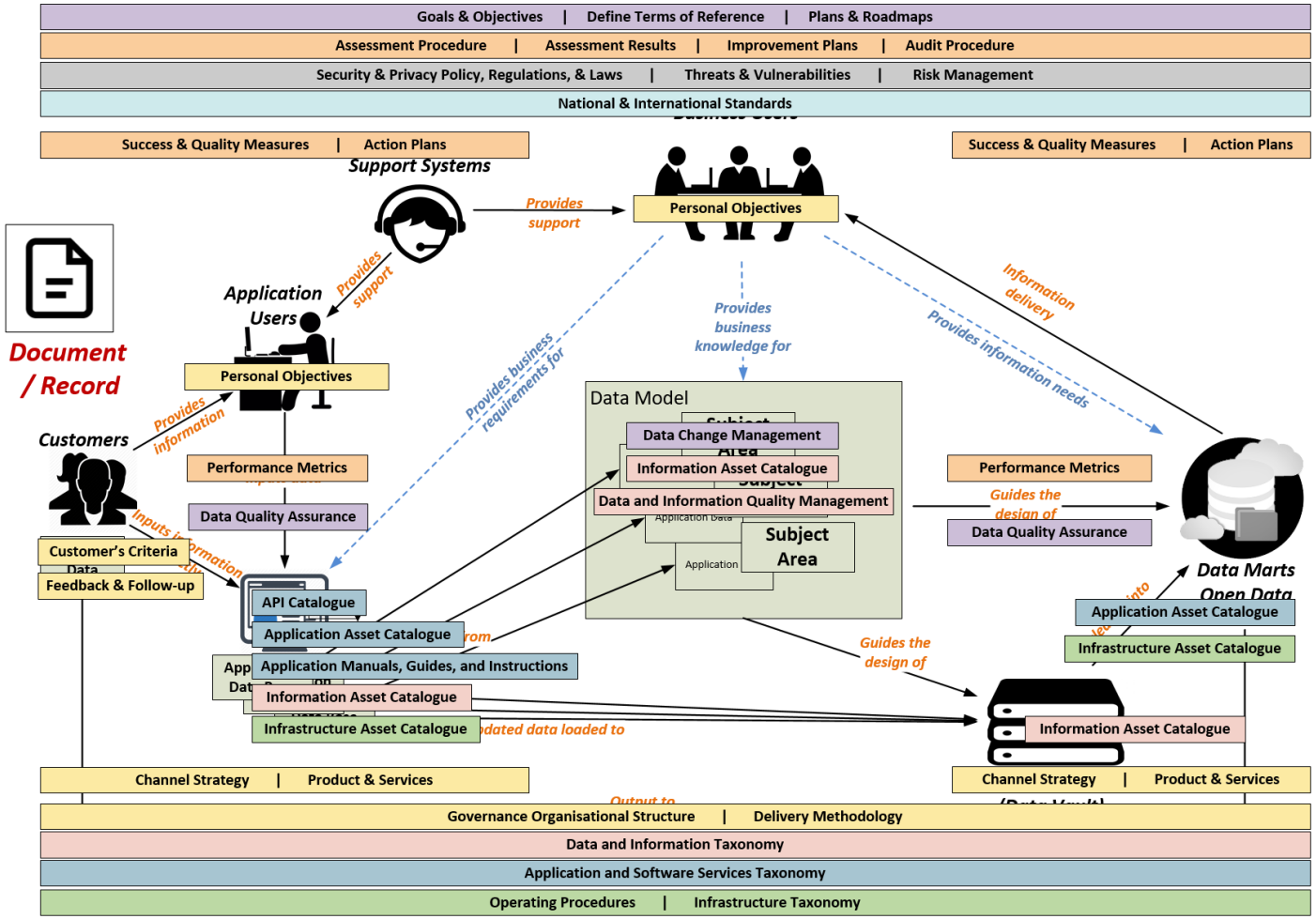


# Document / Record

To *Document / Record* is to write, photograph, or capture information in any form (structured or unstructured) that provides evidence or serves as an official record[30].

This icon will be used to indicate a document / record component on diagrams.

To make sure that all employees know the guidelines, processes, workflows, we need to document those. These documents or records are also used to evaluate monitor, and control the processes to make sure data and information is of high quality:



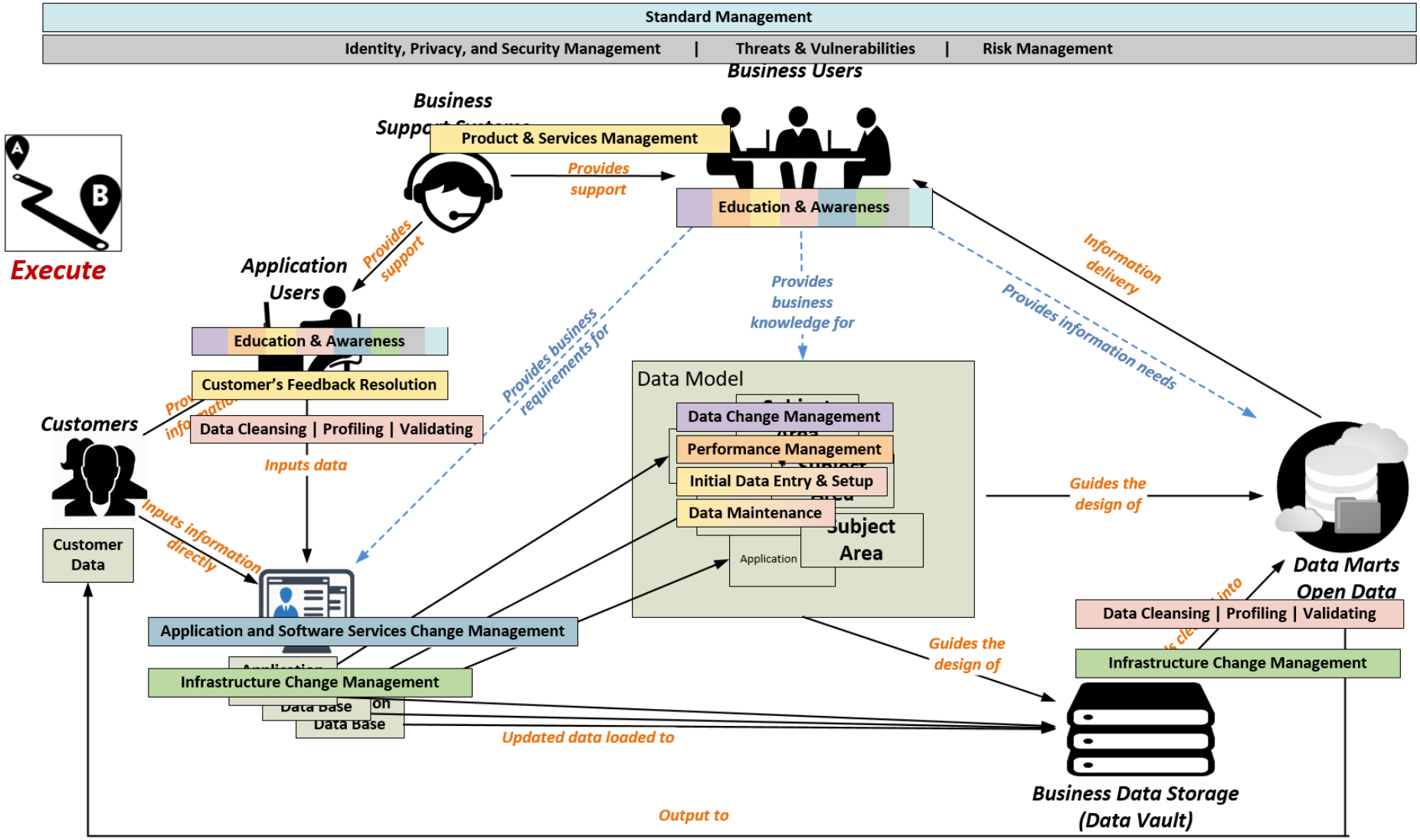

[30] An official record or original copy is an original document that is legally recognized and thus ensuring the quality of a fact when it is established.

# Execute

To *Execute* is to put a plan or course of actions into effect.

This icon will be used to indicate an execute component on diagrams. 

There are also actions that need to be executed to achieve high quality data and information:

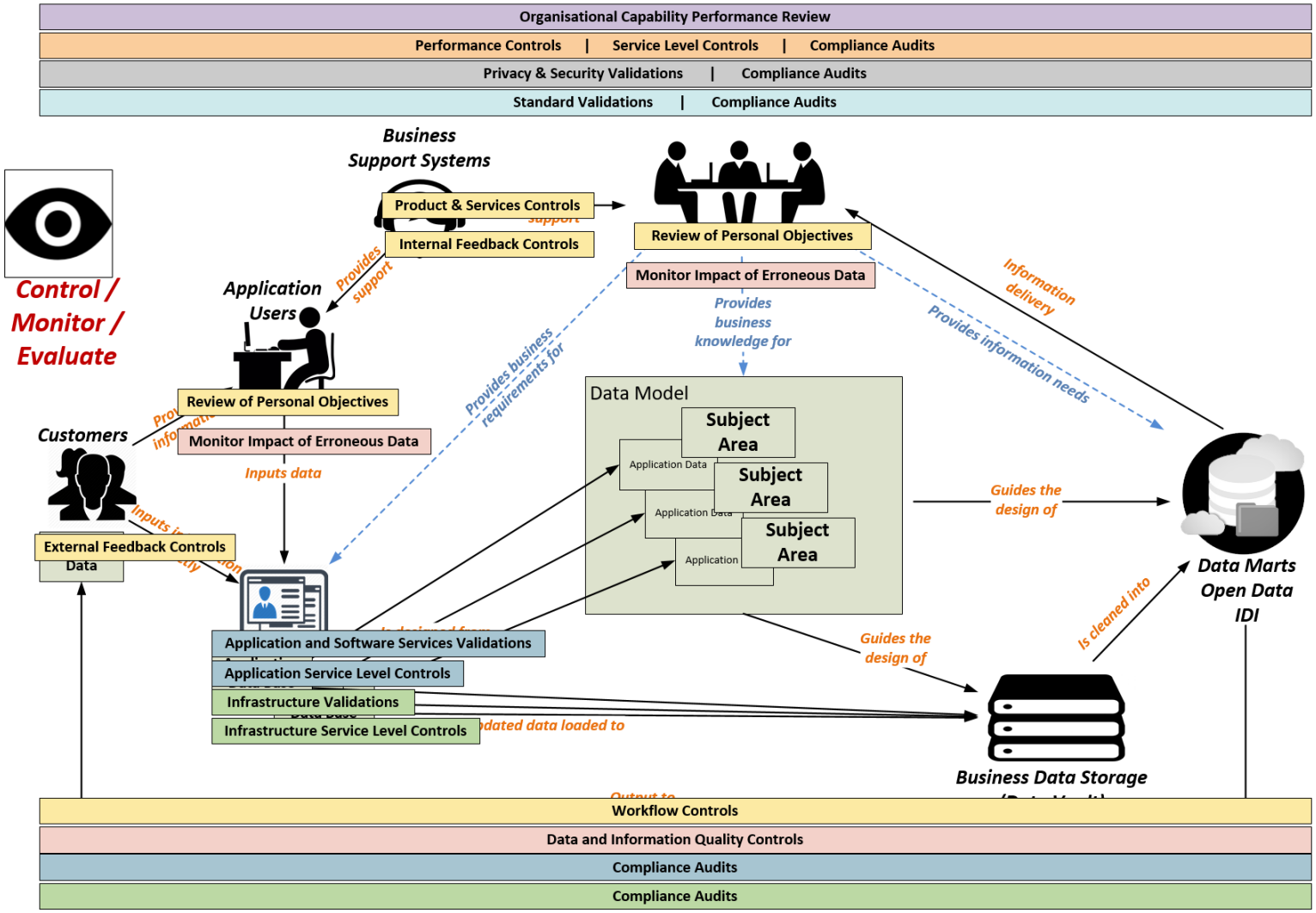


# Control / Monitor / Evaluate

To *Control* / *Monitor* / *Evaluate* is to exercise restraining or directing influence over the execution of an action, to regularly check something or watch someone in order to find out what is happening, and to determine the significance, worth, or quality of the results.

This icon will be used to indicate a control / monitor / evaluate component on a diagram.

Besides planning, documenting, and executing tasks there needs to be mechanisms to ensure that we know the data and information is of high quality. Additionally to be able to continuously improve the handling of data and information so there is a high trust in the integrity and liability of information assets.



# Appendix B - List of Know-MAT member agencies

**Know-MAT** stands for **Know**ledge **M**aturity **A**ssessment **T**eam.

The purpose of Know-MAT is to:

- Support alignment across agencies and IMs around the use of the AoG Data and Information Governance Framework.
- Assist in the use and execution of the Data and Information Governance Maturity Assessment.
- Have an open discussion around the assessment recommended steps and how and what organisations need to prioritise and focus on to mature their governance.
- Work collaborative on guidelines and recommendation around data and information.

Here is a list of agencies who contributed to the development of this guideline:

- ACC - Accident Compensation Corporation is a Crown entity responsible for administering the country's universal no-fault accidental injury scheme.
- Archives NZ - Archives New Zealand is responsible for the record of government.
- CAA - Civil Aviation Authority oversees aviation safety and the rules.
- CASS - Central Agencies Shared Services at Treasury delivers services to the Department of Prime Minister and Cabinet, State Services Commission and the Treasury.
- Corrections - Department of Corrections is the public service department charged with managing the New Zealand corrections system.
- DIA - Department of Internal Affairs serves and connects people, communities and government to build a safe, prosperous and respected nation.
- MoE - Ministry of Education is the Government's lead advisor on the New Zealand education system, shaping direction for sector agencies and providers.
- FaE - Fire and Emergency New Zealand is a new unified fire organisation that brings together our country’s urban and rural fire services for the first time
- GCIO/GCDO – Government CIO/CDO is responsible for ICT-enabled transformation across government agencies to deliver better services to citizens.
- IR - Inland Revenue is a public service department charged with advising government on tax policy, collecting and disbursing payments for social support programmes, and collecting tax.
- LINZ - Land Information New Zealand is the public service department charged with geographical information and surveying functions as well as handling land titles, and managing Crown land and property.
- MaritimeNZ - Maritime NZ is the national regulatory, compliance and response agency for the safety, security and environmental protection of coastal and inland waterways.
- MBIE - Ministry of Business, Innovation and Employment is the public service department charged with "delivering policy, services, advice and regulation" which contribute to New Zealand's economic productivity and business growth.
- MFE - Ministry for the Environment is the public service department charged with advising the government on policies and issues affecting the environment, in addition to the relevant environmental laws and standards.
- MoH - Ministry of Health is the public service department responsible for healthcare in New Zealand.
- MoJ - Ministry of Justice is an executive branch of the New Zealand Government, responsible for the enforcement of the law and administration of justice within New Zealand.
- MPI - Ministry for Primary Industries is the public service department charged with overseeing, managing and regulating the farming, fishing, food, animal welfare, biosecurity, and forestry sectors of New Zealand's primary industries.
- MSD - Ministry of Social Development is the public service department charged with advising the government on social policy, and providing social services.
- NZDF - NZ Defence Force provides essential support to the delivery of the Government’s national security interests.
- NZTA - NZ Transport Agency is a Crown entity tasked with promoting safe and functional transport by land, including the responsibility for driver and vehicle licensing, investigating rail accidents and administering the New Zealand state highway network.
- OAG - Office of the Auditor-General carries out strategic audit planning, sets policy and standards, appoints auditors and oversees their performance, carries out performance audits, provides reporting and advice to Parliament, and carries out inquiries and other special studies.

- Ombudsman - The Ombudsman helps the community in its dealings with government agencies.
- RBNZ - Reserve Bank manages monetary policy to maintain price stability, promotes the maintenance of a sound and efficient financial system, and supplies New Zealand banknotes and coins.
- StatsNZ - Statistics New Zealand is the public service department charged with the collection of statistics related to the economy, population and society of New Zealand. To this end, Statistics New Zealand produces censuses and surveys.
- TEC - Tertiary Education Commission is a Crown entity who leads the Government's relationship with the tertiary education sector in New Zealand and provides career services from education to employment.
- Treasury - New Zealand Treasury is the central public service department charged with advising the government on economic and financial policy, assisting with improving the performance of New Zealand's economy, and managing financial resources.

# Appendix C - Measuring the Value of Information

## Introduction

Information is increasingly being recognised as a key economic resource and as one of the organisation's most important assets. Despite gaining recognition as an asset in its own right, information has so far resisted quantitative measurement. While it consumes vast and ever increasing quantities of organisational resources in terms of data capture, storage, processing and maintenance, it typically receives no financial recognition.

The first step in the process is to identify the Information Assets held by the organisation. On the assumption that these are assets like any other then conventional asset valuation processes could be applied.

This appendix firstly describes a number of existing measuring models and gauges their suitability for measuring the value of information. It then describes valuation methods specifically aimed at valuing information as an asset.

## Existing Models

### Communications Theory

The mathematical measure of information used in communications theory[31] has not proved to be a useful foundation for information measurement in practice, except in purely engineering contexts. The major limitation with this approach is that it focuses on the amount of information transmitted and ignores any consideration of content or meaning. However the meaning of a piece of information is of principal concern to most business users of information and the major determinant of its value. The fact that a certain volume of data per second is transmitted over a certain distance says nothing about its value. As discussed earlier (Information Characteristic 6), more information can actually lead to reduced effectiveness.

### Accounting Valuation Models

If we consider information to be an asset, it makes sense that it should be valued using the same methods used to value other assets. According to accounting theory, the value of an asset may come from two sources:

- Use of the asset
- Sale of the asset

Where the benefits come from use of the asset, it is said to have "value in use", and where the benefits come from sale, the asset is said to have "value in exchange". In the case of information, benefits generally arise from use rather than exchange. In many cases, there are no "buyers" of the information, so its value in exchange is zero.

[31] Shannon and Weaver, 1949

There are three major asset valuation paradigms used in accounting theory[32]:

- Cost (or Historical Cost)
- Market (or Current Cash Equivalent)
- Utility (or Present Value)

### *Cost (Historical Cost)*

Using this method, the asset is valued based on how much was originally paid to acquire the asset (purchase price or development cost). The rationale behind this is that cost approximates the value of the asset at the time of acquisition. The assumption is that a firm, behaving rationally, will only spend money to acquire an asset if it believes it will receive at least an equivalent amount in the future in service potential or economic benefits. This is the traditional cost accounting approach to valuing assets, and is still the most widely used method in practice. It has been the subject of much criticism, but no alternative model has gained sufficient support to replace it yet. The major advantage of the historical cost method is that it is the easiest to collect, and (arguably) the most reliable and objective. Its major weakness is that it may not reflect the current value of an asset. For example, a property or equipment item may have been purchased at a given price, but its value may have increased or decreased dramatically since that time.

### *Market (Current Cash Equivalent)*

Using this method, an asset is valued based on how much other people or organisations are prepared to pay for it -this equates to value in exchange. For example, property can be valued based on its estimated selling price. The major strength of this method is that it gives a good indication of the current value of the asset. A growing number of accountants believe that market prices should be used instead of historical costs for all valuations -this is called current cost accounting. Empirical evidence suggests that current cash equivalents are available for most assets, and that they can be determined with reliability comparable to historical cost. The weakness of this method is that it is more time-consuming and expensive than measuring historical cost. Related concepts to market price are replacement cost (the cost of replacing the asset by a new one), current cost (the cost of replacing the asset by a similarly used one) or net realisable value or NRV (which is the amount the asset could be sold for, less any costs of selling it). Open Government approaches mean that little data is ever actually “sold” thus diminishing the value of this method.

### *Utility (Present Value)*

Using this method, the asset is valued based on the present value of expected future economic benefits -this equates to value in use. For example, property may be valued based on the discounted value of expected future rents. There is wide agreement that, conceptually, this is the best approximation to the true economic value of an asset[33]. The major weakness of this method is the difficulty of determining the specific future cash flows related to the asset, which is often quite subjective and therefore of doubtful value to statement users. For most assets, there is great difficulty estimating future economic benefits; difficulties in converting these economic benefits to monetary equivalents which can be discounted; and there is the technical problem of choosing a discount rate. This is particularly difficult in the case of the value of information. In practice, this method is primarily used for long term monetary assets (e.g. bonds, leases), where the future cash flows are specified by contract and can therefore be determined objectively. For non-monetary assets, such as information, it is virtually impossible to determine their future cash flows.

[32] Godfrey et al, 1997
[33] Godfrey et al, 1997

# Information Based Models

## Market Value of Information

The market value of information is the amount that other organisations are prepared to pay for it. Using the internet, information is now being widely traded as a commodity. Information may be sold as a product or paid for on a usage basis. Market value is generally only applicable to a relatively small proportion of an organisation's information. Information cannot be bought and sold in the same way as other assets and is usually only of value as part of a going concern -therefore most information has no resale or liquidation value. The bulk of information in a commercial organisation is either:

- Administrative: such information is generally of little interest to other external parties and is only of use for internal management purposes (e.g. budget figures)
- Commercially sensitive: it is not in the firm's interest to sell the information for competitive reasons (e.g. sales information)
- Confidential: the firm is not allowed to sell or pass on the information for privacy reasons (e.g. personnel records or customer information).

In Government all information, apart from Sensitive or Confidential, is freely available and therefore has no sale value.

Interestingly, because information can be sold and still retained by the organisation, it may have both market value and utility value, with its total value being the sum of these (for normal assets, the greater of the two is used). Also, the information can be sold over and over again without losing the asset (unless exclusive rights to the information are sold). In this respect, its selling price is modelled more accurately as a utility value -the expected future cash flows as a result of sales of the information. For example, a retailing organisation sold their sales information to an information broker for $60 million per year. While this is a "market price" in that it represents what an external party is prepared to pay for it, it fits the utility model better because it generates future cash flows rather than a once off payment. Because information is not appropriable, the market value model does not apply except in special cases of intellectual property (e.g. a patent), where exclusive rights to use an information product are sold.

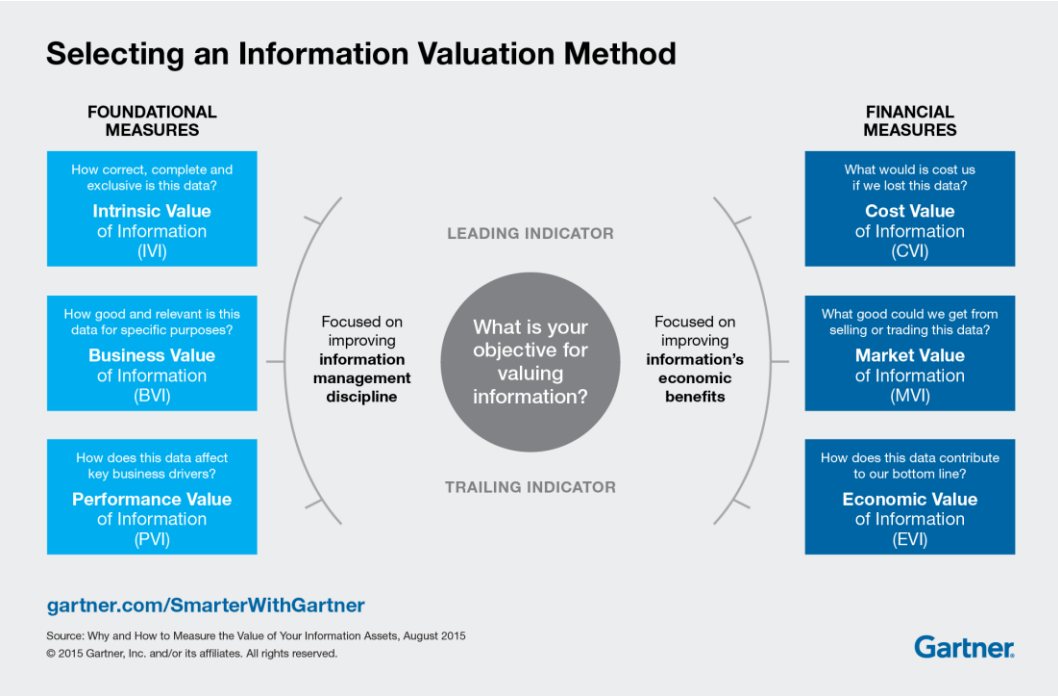
## Utility Value of Information

The utility value of information is measured by the benefits that can be derived from it, in terms of future cash flows, but only for commercial companies. A large electronics organisation used this method to value their customer transaction information in one product line at $25 million. This was done using managerial judgement to estimate the increased revenues or reduced costs to the organisation as a result of having the information. A decision calculus methodology was used to assist managers in arriving at the estimate, using an iterative series of questions and responses.

Theoretically, this is the best indicator of the value of information because it takes into account how the information is used (Information Characteristic 2). However the major weakness of this method is that estimates of the future benefits which can be obtained from information are highly subjective and time consuming to collect. It is difficult, if not impossible, to isolate the contribution of information to revenues or products. Information acts as a catalyst rather than a direct source of revenue. Its value lies in making better decisions, speeding the movement of products and services through the economy and gaining competitive advantage. With the exception of competitive advantage, this applies to all Government Information.

# Gartner's Information Valuation Method

Gartner, in collaboration with their clients, valuation experts, accountants and economists recently introduced the following six formal information valuation models—each with a different purpose. Some are financial measures while others are foundational metrics. Some are leading indicators, while others are trailing indicators.




## Foundational Measures

- **Intrinsic Value of Information (IVI)**

Breaks the information asset into the Principles for Information Quality[34] such as accuracy, accessibility, completeness, and then rates each principle and tallies for final score.

- **Business Value of Information (BVI)**

Measures information characteristics[35] in relation to business processes.

- **Performance Value of Information (PVI)**

Measures data impact on key performance indicators over time.

## Financial Methods

- **Cost Value of Information (CVI)**

Measures the cost of "acquiring or replacing lost information" as well as lost revenue caused by loss of data.

- **Market Value of Information (MVI)**

Measures the revenue generated by "selling, renting or bartering" corporate data.

- **Economic Value of Information (EVI)**

Measures how data contributes to revenue.

[34] See Principles for Information Quality

[35] See The Seven Characteristics of an Information Asset

# How to Value the Quality of Your Information Asset[36]

Knowing how much of a value an information asset has depends on the quality of that asset for a certain purpose. To calculate the value you need to know the criteria. Information is utilised, for example, when it improves operational processes, used for making fact based decisions, etc. This means that the Usability, Usefulness, or Utilisation of an information asset is an important benchmark for its Value.
Because Usefulness and Utilisation are very similar to Usability, there is no distinction made between them in this method. The perceived Usefulness of information is significantly influenced by User Information Satisfaction. The most important input criteria for measuring User Information Satisfaction are Accuracy and Completeness which are components of Information Quality. Reliability and Accessibility are also important and these are components of System Quality. When decisions are more operational, aspects like Timeliness will possibly play a more important role. The criteria in the method for Information Quality, shown in the diagram below, were selected because they are widely used, representative, and relevant to technology. The list is not extensive, which means you can add other criteria which are relevant to your organisation.

**Note**: The method described was designed to be used for decision making information, but has been adapted to be usable to assess **Information Assets (IA)** for any purpose.

## How to Calculate the Quality of the Information Asset?

First you need to identify the right criteria and the weight of those criteria (see questionnaire above), then you can put a value on each of those criteria and calculate the value.
To identify which criteria that are important for your organisation and the weight you can put on them, its purpose, end users, customers, and stakeholders you can issue a survey. Here is some example of questions that can be asked:

***Criteria of the System that provides the Information Asset:***

**Accessibility -** *The ease with which information can be accessed or extracted from the system. The information should be continuously accessible without to many obstructions*

- Do you need to easily access the information?
- How easy is it the retrieve the information? Is there a continuous and unobstructed way to get to the information?
- Can you access the information at any time?
- Is the process to retrieve the information complex and time consuming?

**Flexibility -** *The way the system can be adapted to changing demands of the user.*

- Does the information need to be used in different forms (raw data, report, graph, etc.)?
- Is the information asset adaptable to changing demands of the user?
- Is it easy to retrieve the information in any form you want?

**Integration -** *The way the system allows data to be integrated from various sources*

- Does the information asset need to be exchanged with several other internal or external systems?
- If so, how easy is it to adjust the system that provides the information to easily accommodate new integrated systems?
- Does the system allow data to be integrated from various sources?
- Is it very costly to adopt the system to integrate the information into new systems?

**Reliability -** *The dependability of system operation*

- Is the system that provides the information up and running 24/7 without or with very little interruptions? And does it need to be?
- Is the system that provides the information reliable?

[36] Based on "Information value in a decision making context" case study from Radboud University Nijmegen by Joep Top, 2015 which looked at how to calculate the value of information assets needed for decision making for an energy company.

**Timeliness / Speed -** *The information should be processed and delivered rapidly without delays. The information should also match the user's working pace*

- How timely do you need to receive the information?
- Is the information processed and delivered rapidly without delays?
- Is the information delivered at a speed that matches the user's working pace?

**Security –** *How well the information is protected against loss or unauthorized access*

- Is there a need to secure the information from unauthorised access or loss (can it be retrieved easily)?
- If so, how secure does it need to be?

***Criteria for the Information Asset itself:***

**Accuracy / Precision -** *Freedom from error (correctness), or closeness to truth or fact. Accuracy depends on how the data is collected, and is usually judged by comparing several measurements from the same or different sources.*

- How accurate or precise does the information need to be?
- Is the information precise enough and close enough to reality?
- Is the information free of distortion, bias, or errors?

**Applicability –** *The degree to which the information can be directly applied / used.*

- Does the information need to be applied to this particular purpose?
- Can it directly be applied?
- Is it useful?

**Completeness -** *The degree to which the information provides all necessary content for the purpose*

- Does the scope on the information matter to the purpose of use?
- If so, is it adequate to the purpose (not too much or too little)?

**Convenience –** *The degree the information corresponds to the user's needs / purpose*

- Does the information correspond to the user's needs and habits?

**Conciseness –** *The degree the content only covers the needs of the purpose***.**

- Is the information to the point and void of unnecessary elements?

**Consistency –** *The freedom of contradiction or convention breaks*

- Is the information free of contradictions or convention breaks?

**Currency -** *The degree the information is up-to-date and not obsolete*

- Is the information asset up-to-date and not obsolete?

**Format / Clarity -** *Information should be well, understandably and clearly presented to user*

- Is the information understandable and clearly presented to the target group?

**Traceability –** *The background of the information should be traceable, such as the used data, author(s)*

- Is traceability of the source important?
- Is the background of the information visible (author, date, used data, etc.)?

**Acceptable Risk -** *The degree in which the information can mitigate potential risk for the user*

- Is there any risk around the use of the information?
- Is so, is it acceptable?

***Criteria that are Useful or Usable for the User:***

**Operability -** *The capability of the information asset to enable the user to operate and control it for a purpose*

- Is the information asset used for operational usage?
- If so, does it enable the user to operate and control processes?

**Attractiveness -** *The capability of the information asset to be attractive to the user for a purpose*

- Is the information asset used for internal or external branding or marketing?
- If so, is the information asset attractive to the end user?

**Learnability -** *The capability of the information asset to enable the user to learn its use*

- Is the information asset used for awareness, education or training, or guidance of any kind?
- If so, does the information asset enable the end user to easily learn from it?

**Fun -** *The amount fun in using the information for a purpose*

- Is the information used for games, quizzes, entertainment, etc.?
- If so, what's the amount of fun in using the information asset?

***Criteria that are Useful and Usable for the 'Enterprise' that are influenced by the Goals:***

**Efficiency -** *The efficiency in using the information for the enterprise's goals*

- How many times per week do you use the information asset?
- How many minutes do you spend reviewing and using the information asset each time you receive it?
- How long does it time to completely review and understand the content of the information asset?

**Maintainability -** *The information should be easily maintainable*

- Does the information asset need to be organised and updated on an ongoing basis?
- If so, how easy is it to maintain the asset?

**Context Coverage -** *The degree in which the information asset can be used in different contexts and multiple times*

- Does the information asset need to be used in different context?
- If so, to what degree can be used in different contexts and multiple times?

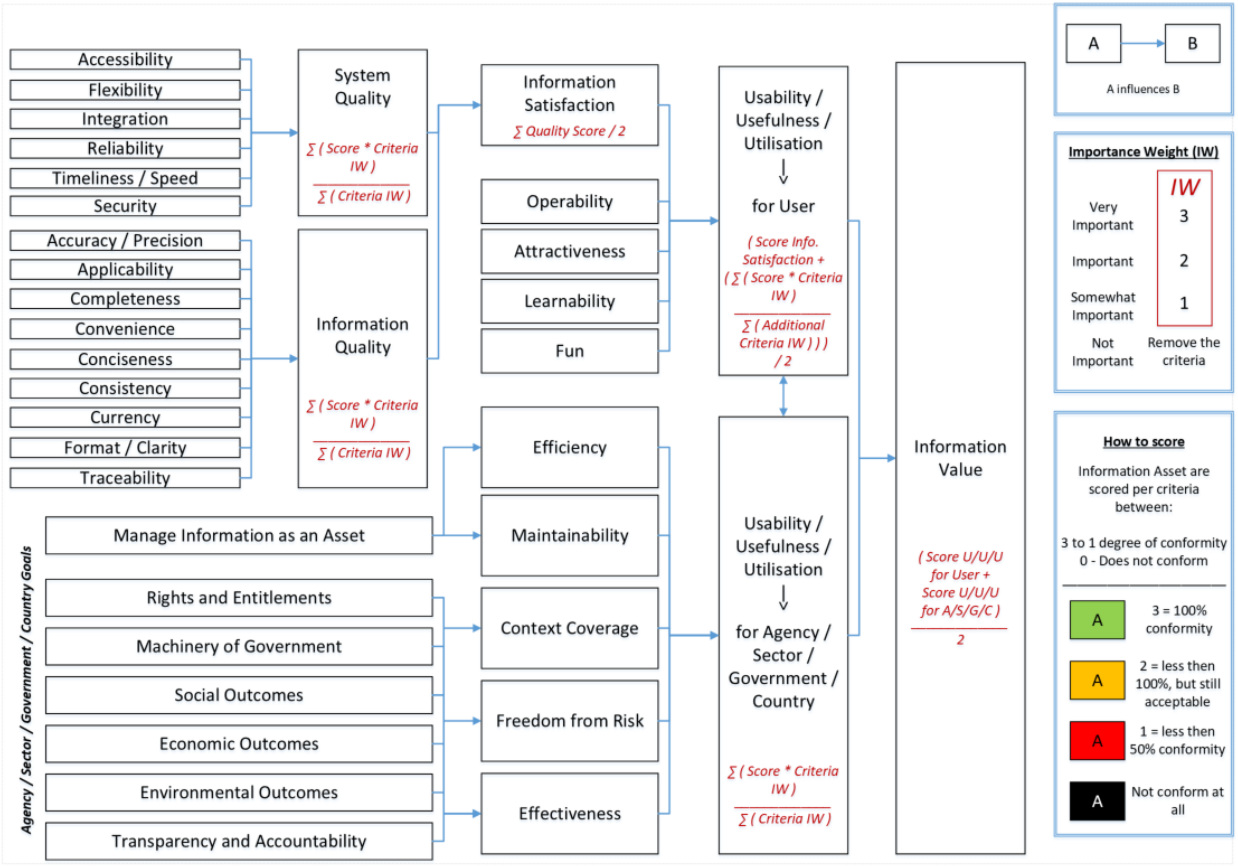
**Freedom from Risk -** *The degree in which the information can mitigate potential risk for the enterprise*

- Does the use of the information asset have potential risks?
- If so, to what degree does the organisation allow this risk?

**Effectiveness -** *The contribution of the information to the goals of the information and the organisation*

- What kind of decisions do you make based on the information asset?
- How sure are you in making the right decision based on the information asset?
- Would you be able to make the same decision WITHOUT having access the information asset?
- How sure are you in making the right decision WITHOUT having access to the information asset?
- What is the alternative if you would not have access to the information asset?
- How much time to you save with this information asset?
- Can risks to the organisation be avoided based on the information asset? If so, to what extend does it help?
- To which goals does the information asset contribute?

Once you have identified the criteria and the weights you then can calculate the quality of the information asserts you receive with the following formula[37].

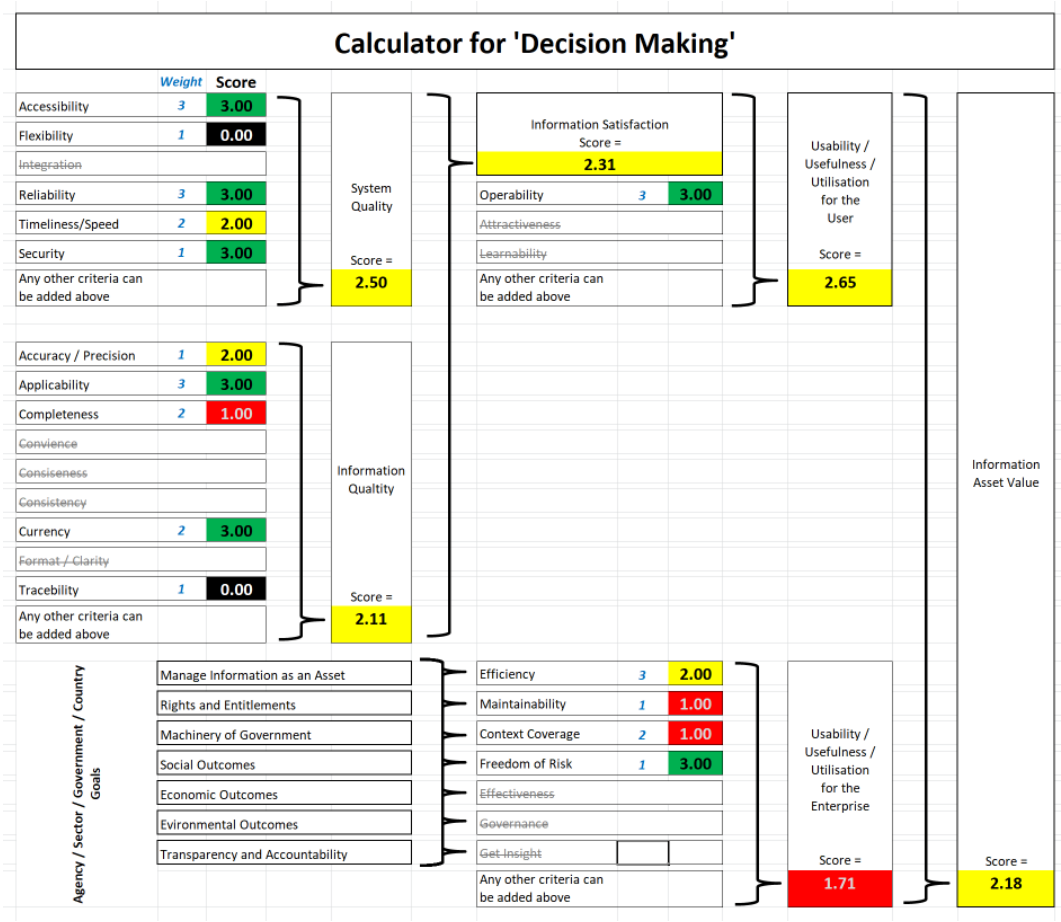



Here is a verification of the formulas and the maximum score:

| What is scored | Formula | Verification Calculation using maximum scores | Score |
|---|---|---|---|
| Max System Quality | ***∑ (Score * Criteria IW) / ∑ (Criteria IW)*** | 3*3 + 3*1 + 3*3 + 3*2 + 3*1) / (3 + 1 + 3 + 2 + 1) = 30 / 10 | **3** |
| Max Information Quality | ***∑ (Score * Criteria IW) / ∑ (Criteria IW)*** | (3*1 + 3*3 + 3*2 + 3*2 + 3*1) / (1 + 3 + 2 + 2 + 1) = 27 / 9 | **3** |
| Max Information Satisfaction | ***∑ Quality Score / 2*** | (**3 + 3**) / 2 | **3** |
| Max Usability for User | ***(Score Info. Satisfaction + (∑ (Score * Criteria IW) / ∑ (Additional Criteria IW))) / 2*** | (**3** + ((3*3) / (3)) / 2 = (3 + 3) / 2 | **3** |
| Max Usability for A/S/G/C | ***∑ (Score * Criteria IW) / ∑ (Criteria IW)*** | (3*3 + 3*1 + 3*2 + 3*1) / (3 + 1 + 2 + 1) = 21 / 7 | **3** |
| Max Information Value | ***(Score U/U/U for User + Score U/U/U for A/S/G/C) / 2*** | (**3 + 3**) / 2 | ***3*** |

[37] ***∑ (Score * Criteria IW)*** can be read as the sum of Score times Criteria Important Weight (IW).

*An Example of calculating the value of an IA you received for a certain purpose, where **AS = Assessment Score** and **IW = Importance Weight.***




- Accessibility (IW = 3) AS = **3**
- Flexibility (IW = 1) AS = **0** – the system is not flexible to adjust.
- Reliability (IW = 3) AS = **3**
- Timeliness (IW = 2) AS = **2** – the system can't always deliver the IA on time.
- Security (IW = 1) AS = **3**

System Quality AS: *∑ (Score * Criteria IW) / ∑ (Criteria IW)* => 25 / 10 = **2.5**

- Accuracy (IW = 1) AS = **2**
- Applicability (IW = 3) AS = **3**
- Completeness (IW = 2) AS = **1**
- Currency (IW = 2) AS = **3**
- Traceability (IW = 1) AS = **0**

Information Quality AS: *∑ (Score * Criteria IW) / ∑ (Criteria IW)* => 19 / 9 = **2.1**

Information Satisfaction AS: *∑ Quality Score / 2* => **4.6** / 2 = **2.3**

- Operability (IW = 3) AS = **3**

Usability for User AS: *(Score Info. Satisfaction + (∑ (Score * Criteria IW) / ∑ (Additional Criteria IW))) / 2* => (**2.3** + 3) / 2 = **2.65**

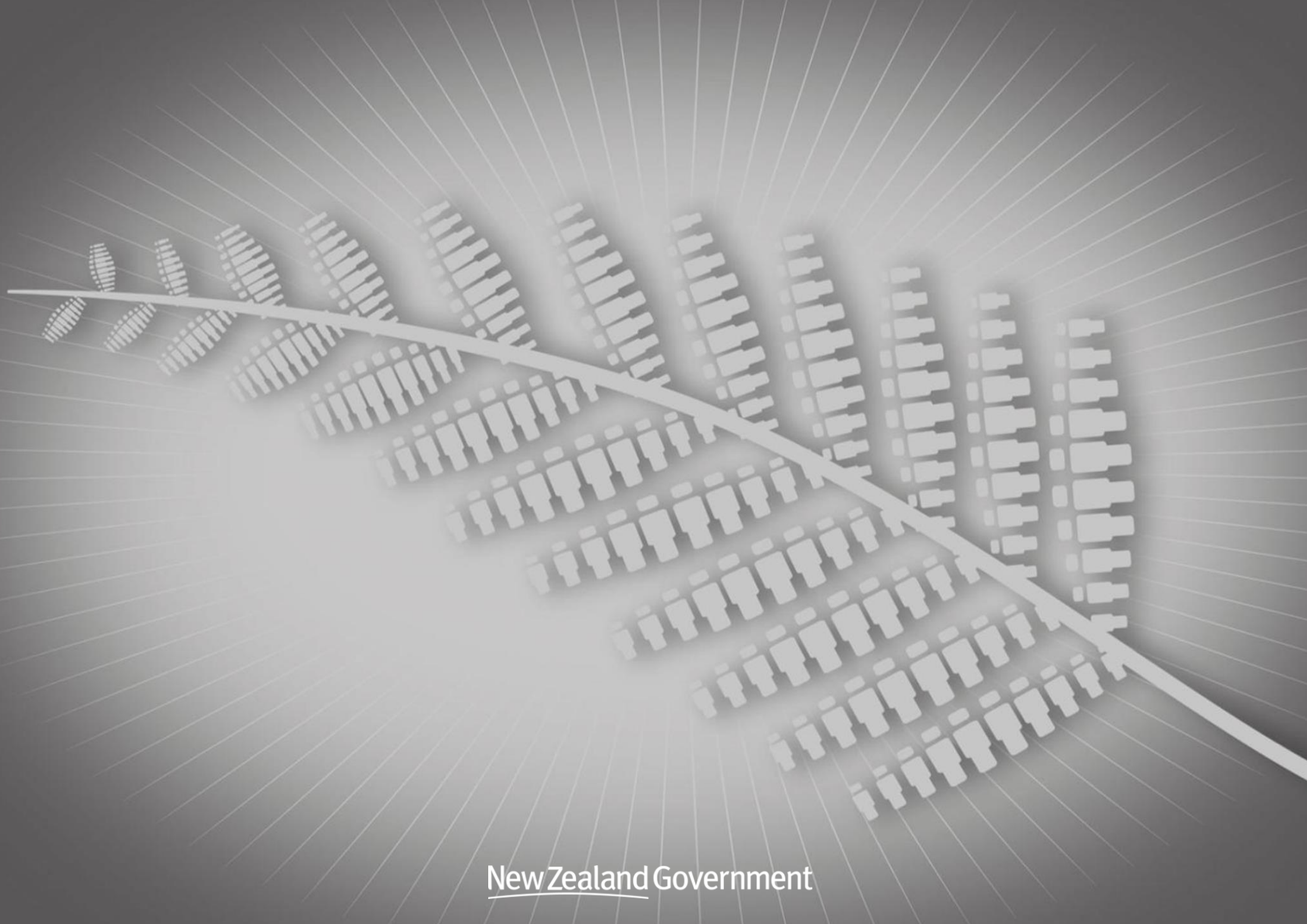
- Efficiency (IW = 3) AS = **2** - the IA isn't so easy to produce
- Maintainability (IW = 1) AS = **1** - the IA is difficult to maintain
- Context Coverage (IW = 2) AS = **1** - the IA does not cover the complete context
- Freedom from Risk (IW = 1) AS = **3**

Usability for A/S/G/C AS: *∑ (Score * Criteria IW) / ∑ (Criteria IW)* => 12 / 7 = **1.71**

**Note**: The calculator is available for use. Send request to the Government Enterprise Architecture team at gea@dia.govt.nz.

Information Value AS: *(Score U/U/U for User + Score U/U/U for A/S/G/C) / 2* => 4.35 / 2 = **2.18**

So the value of that particular information asset for decision making is ***2.18/3***.
This means that this asset is of somewhat **low quality** to be used for accurate decision making, mainly **because of its efficiency, coverage, and maintainability**.


New Zealand Government