MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

# Ministry of Social Development

## *Preventing failure of critical services to clients*

Programme Business Case



| | |
|---|---|
| **Prepared by:** | s9(2)(a) |
| **Prepared for:** | s9(2)(a) |
| **Date:** | 08/02/2019 |
| **Version:** | 1.0.1 |
| **Status:** | Final |

# Better Business Cases
# Programme Business Case Template

## Document Control

### Document Information

| | Position |
|---|---|
| Document owner | s9(2)(a) |
| Issue date | 04/02/2019 |

### Document History

| Version | Issue Date | Changes |
|---|---|---|
| 0.1 | 30/11/2018 | Individual 'cases for change' feedback from subject matter experts incorporated to individual cases. |
| 0.2 | 07/12/2018 | Broad feedback from first complete draft excluding Financial Case accommodated from business case team |
| 0.3 | 10/12/2018 | Incorporate feedback from senior stakeholder group |
| 0.4 | 11/12/2018 | Incorporate CFO feedback from Bruce Simpson |
| 0.5 | 13/12/2018 | Incorporate DCE Feedback from Stephen Crombie and Nic Blakely |
| 0.6 – 0.9.2 | 14/12/2018 | Template, format and detailed review versions |
| 0.9.3 | 14/12/2018 | Draft business case to submit to Treasury and GCDO |
| 0.9.4 | 25/01/2019 | Updates covering actions from internal and external review, sent to ISGS |
| 0.9.5 | 31/01/2019 | Draft for Treasury and GCDO comment |
| 0.9.6 | 1/02/2019 | Draft for final internal and external review |
| 1.0 | 4/02/2019 | Final version |
| 1.0.1 | 8/02/2019 | Correct errors in the resource tables |

### Document Review

| Role | Name | Review Status |
|---|---|---|
| Project Manager | s9(2)(a) | Version 1.0 to submit to Treasury |

### Document Sign-off

| Role | Name | Sign-off Date |
|---|---|---|
| Project Manager | s9(2)(a) – draft version for release to Treasury | 04/02/2019 |
| Senior Responsible Owner/ Project Executive | s9(2)(a) | 04/02/2019 |

# Contents

# Executive Summary

## Proposal

This business case requests funding of $111.2M capital and $124.1M operating over four years (including steady state operating expense). This does not include a contingency of 15% ($27.0M) calculated by the Quantitative Risk Assessment (QRA). This funding will cover a four year programme of work comprising three funding and delivery tranches.

This initiative is necessary to avert the risk of serious failure in providing services[1] to over one million New Zealanders, and making $24B in essential payments annually. The risk also extends to selected shared services supplied to the Oranga Tamariki (OT), the Ministry of Housing and Urban Development (MHUD), the Social Investment Agency (SIA), and the Office of the Children's Commissioner (OCC).

Significant technology risk of failure has built up over a number of years due to the Ministry having to prioritise other expenditure ahead of the upkeep of the existing technology assets (see Financial Case). The Ministry has also tended, over the years, to deliver sub-optimal and non-strategic solutions to meet tight legislative deadlines and constrained project budgets, and this has created additional compounding technical debt[2]. Risk to Technology Systems Availability is one of the key risks monitored by the Ministry's Leadership Team. Currently this risk is assessed as 'Very High' with the trend 'Increasing'[3].

Exacerbating the shortfall in funding, the risk is rapidly accelerating due to: existing technical debt, ongoing deferred maintenance, increased complexity from new services, such as digital; and increasing volumes.

This business case covers Technology investments that:

- are for systems fundamental to the Ministry's operation,
- remediate elements of the Ministry's technology environment that are most at risk of failure,
- cannot be funded from existing budgets,
- have long term strategic value, and
- which are foundational pre-requisites to delivery of the Technology Strategy as a whole.

## Strategic Alignment

The investments articulated in this document are required in Budget 2019, regardless of any downstream changes to the Ministry's operating model. They have been selected as they mitigate the most risk, and will provide enablers for further Technology investments that support Te Pae Tawhiti, the Ministry's future strategy.
Any changes to the Ministry's operating model will be articulated in Te Pae Tawhiti, which will be elaborated throughout calendar 2019. Investments to support Te Pae Tawhiti are likely to be presented for consideration in Budget 2020.

The investments proposed in the document are primarily involved with systems supporting the Ministry's obligations as prescribed in the Social Security Act, as well as supporting ongoing operations for shared services

[1] A detailed description of the impacts of service failure is included in Appendix 1
[2] Technical debt includes the implied cost of additional rework caused by choosing an easy solution now instead of using a better approach that would take longer it also includes deferred upgrades and maintenance that will eventually have to be done and legacy defects that will eventually need to be fixed
[3] An overview of the Ministry's Technology Systems Risk is included in Appendix 2

partners OT, MHUD, SIA, and OCC. The value of these investments is therefore highly unlikely to be affected by changes to the Ministry's operating model[4].

In 2018, the Ministry developed a new Technology Strategy, which is aligned with the Statement of Intent, and endorsed by the Ministry's Leadership Team. The Technology Strategy describes the critical technology investments required over the next seven to ten years that underpin the Ministry's business strategy, based on the best current understanding of Te Pae Tawhiti. This includes the delivery of the Government's overall digital and data strategies. All of the investment requested in this business case is required by the Technology Strategy.

## Urgency

The Ministry has an existing budget allocated to maintaining technology assets, and a programme of risk focused maintenance. The current programme is oversubscribed, and the allocated budget is insufficient to prevent the Ministry's risk position continuing to worsen given the previous years of underinvestment.

The leading indicators of probable downstream system failure include the fact that 59% of the Ministry's computer hardware is over 5 years old and 61% of the software is not fully supported. Given the lead times required to remediate this position, at the point where the lead indicators are accompanied by lag indicators (e.g. escalating rates of actual failure), the Ministry will likely experience an extended period of highly disrupted front line operations, which would to varying degrees spill over into shared services partners OT, MHUD, SIA, and OCC. It would take months to stabilise the situation if the Ministry is already in crisis mode.

## Investment Targets

The investments covered by this business case include five system replacement projects which, in the main, are for very old software assets that have been fully depreciated and no provision has been made for their eventual replacement. The five 'Replacement' projects are:

- **Replacement of the Identity and Access Management System (IdAM)**, which controls all staff access to the Ministry's computer systems according to their access rights. The Ministry's current IdAM is a very high risk amalgam of obscure custom code and old unsupported versions of third party software. Some of the software is so old that it needs to run on a 14 year old server.
- **Replacement of DREW**, a 22 year old tool used by all frontline case managers and call centre staff[5] to calculate eligibility and entitlement related to income support applications. As a desktop application, DREW's risk of failure will be greatly increased with the impending Windows 10 operating system which will be compulsorily upgraded every 6 months, and the support arrangements are most unsatisfactory.
- **Replacement of Hindin**, a 17 year old platform used by all front-line staff that houses a number of knowledge bases in use across the Ministry, and client related processes such as Review of Decision and Complaints. This archaic platform cannot be moved to a different operating environment because the application code needs to run on Java 1.4, Solaris 9, and Oracle 9.2, all of which are many years out of support and can only operate on 8 and 9 year old servers.
- **Replacement of the Data Warehouse**, a 22 year old platform which is used for all of the Ministry's internal and external reporting, daily operational support, Data matching with other agencies to prevent benefit fraud, and analytics functions to inform policy and operations. The Data Warehouse contains millions of lines of custom code that are on the verge of being unsupportable.
- **Replacement of Digital Channels components that will not scale to meet client demand**, providing on-line self-service, used by 650,000 clients. The Digital channels (including MyMSD) have experienced very rapid growth in volumes. This is expected to continue, and there is a significant risk it will not scale to

[4] A description of why the value of these investments will not be compromised by any change in operating model is included in Appendix 3
[5] There are over 2,800 client facing front line staff and 5,500 total users of client oriented systems

meet that demand. While key elements of the digital architecture are modern and fit for purpose there elements that are weak and not well configured. Work to remediate this situation is essential.

In addition, the Business Case includes investment to cover the shortfall in on-going 'Business as Usual' upgrades designed to keep technology current and for which the Ministry lacks sufficient capital reserves (the 'Maintenance' projects):

- **Software and security upgrades** for third party software as a part of on-going maintenance as vendors such as Oracle, IBM, and Microsoft release new versions, and includes upgrades to address emerging security threats and vulnerabilities,
- **Hardware upgrades** to move off aging hardware owned by the Ministry to evergreen as-a-service consumption models.
- **Legislative changes** that arise on a regular basis, the cost of which historically the Ministry is expected to absorb.

The Replacement and Maintenance projects proposed represent the minimum case required to address the risk of service failure.

## Programme Delivery Method

The investments will be overseen by the existing Portfolio Executive Committee (PEC) and the Investment Strategy Governance Committee (ISGC). The Ministry's key objective is transparency, and external representation will be sought as part of the governance processes.

All projects will be delivered using the Ministry's successful and mature Agile approach, based on the SAFe[6] delivery framework. The Ministry has a track record of successful delivery of large scale Technology projects and programmes, as well as Technology enabled business projects and programmes. Recent examples include Welfare Reform, Housing transfer from HNZ, Client Management System, Simplification, End User Compute, and Availability and Resilience.

The Replacement projects will be grouped into a programme, broken down into 12 month tranches. The programme will be governed by a programme board, including external representation, reporting to PEC and ISGC.

The delivery approach will be to advance all of the Replacement projects concurrently through Tranche 1. It is not possible to meaningfully prioritise them in terms of risk, and deferring action on any one of them for another 12 months is not feasible. In the course of tranche 1 all of the replacement projects will have progressed through detailed design, proof of concept, and any necessary procurement phases. Some of the projects will have advanced to early delivery phases of the Minimum Viable Product (MVP).

In Tranches 2 and 3, decisions would be made on whether to accelerate or slow down the pace of individual projects based on emergent risk factors or changes in the business environment. The Maintenance projects will be administered by the Ministry's existing Portfolio Executive Committee (PEC) as part of the existing risk based prioritisation process.

## Alignment to Government Priorities

This proposal aligns with the Government's Wellbeing objectives. Details are included in Appendix 14.

[6] Scaled Agile Framework

## Four year cost breakdown summary

**Table 1:** Summary of the funding sought

| Funding Sought ($m) | 2019/20 | 2020/21 | 2021/22 | 2022/23 & outyears | TOTAL |
|---|---|---|---|---|---|
| Operating | 12.070 | 28.483 | 40.514 | 43.020 | **124.086** |

| Funding Sought ($m) | 2019/20 | 2020/21 | 2021/22 | 2022/23 | 2023/24 | 2024/25 | TOTAL |
|---|---|---|---|---|---|---|---|
| Capital | 61.662 | 41.400 | 7.100 | 1.000 | - | - | **111.162** |

# Introduction

This initiative seeks funding to commence a programme of technology upgrades. The purpose is to reduce the risk of severe failure with the Ministry's computer systems. This risk identified in the Ministry's register as 'Technology Systems Availability' is currently rated as 'very high' using the Ministry's risk management framework and trend for this risk is 'increasing'[7].

To prevent the condition of its technology assets from further worsening, the Ministry needs extra capital in the 2019/20 and 2020/21 years, as well as an on-going injection of operating funding.

At present the overall condition of the Ministry's hardware assets is poor with 59% being over 5 years old. The condition of the software assets is also poor with 61% not fully supported. The replacement cost of the Ministry's technology assets is estimated to be from $750m to $1.0 billion. Of this, $63 million is in computer hardware. The largest component is software, at over $700 million.

The current state of affairs poses a significantly elevated risk of systems failure for computer systems that directly support clients. The highly integrated nature of the Ministry's systems means a failure of one component has the potential to bring the whole system down. Security vulnerabilities are also increased through the use of older versions of software and hardware, which increases the risk of a security related incident.

This is at a time when the Ministry is experiencing increased demand for services across all channels, particularly digital. As an example (based on an actual event), the impact of a one day computer system outage is severe:

- 52,500 client logons to MyMSD are declined
- 112,000 client transactions including declaring wages, medical certificates and hardship applications cannot be processed
- 2,800 service centre and contact centre staff who have to revert to unsustainable manual processes
- Manual entry of client transactions would take approximately two weeks to clear with overtime and extra staff required.

Repeated outages within a two week period could result in a full suspension of services as manual processes become overwhelmed.

Any outage will also affect the Ministry's Shared Services partners Oranga Tamariki, the Ministry of Housing and Urban Development, the Social Investment Agency, and the Office of the Children's Commissioner. The potential impact on their services has not been estimated.

The additional funding will enable the Ministry to stabilise its technology by ensuring hardware is modernised, software is upgraded to acceptable levels, single points of failure are reduced, and it is funded at a level to prevent regression. If no additional funding is provided then the risk of this scenario becomes steadily worse. At present it is rated as a 'likely' probability (i.e. 50% - 80% chance in the next 12 months) with 'severe' consequences.

This conclusion is supported by PwC. Their review of ICT completed in July 2018[8] recommended "Given the scale of the backlog and the allocation of future budgets this should be addressed by obtaining additional funding through a defined business case."

The Ministry has created a new Technology Strategy to underpin Te Pae Tawhiti, its strategic direction. In budget 2020 the major investments in long-term systems replacement will be presented.

[7] An overview of the Ministry's Technology Systems Risk is included in Appendix 2
[8] "IT Strategy and Capability Review" July 2018

# The Strategic Case

*Making the Case for Change*

## Overview

The Ministry is operating in a context of extreme technical debt, at a time where it has ambition to greatly improve the client experience and partner with other organisations to improve client outcomes.

This business case is concerned with reducing the risk of failure to client services in a manner that positions the Ministry to pursue its strategic business goals as articulated in the Statement of Intent.

This Investment proposal only covers the severe technical debt (with the exception of funding for legislative changes) which poses a near term threat to ongoing client services.

The Ministry began dealing with technical debt and the funding shortfall in Budgets 2017 and 2018 when it successfully sought funding for three projects;

- **End User Compute** to address the state of the PC fleet in the Ministry which was between 5 and 8 years old (outside National Office), and the old versions of Microsoft software reaching end of extended support in late 2019
- **Availability** which addressed the fact that the Ministry's digital channels, including MyMSD, were unavailable for long periods of time when back-end systems were 'down' due to planned or unplanned outages
- **Resilience** which addressed the fact that the Ministry's core systems used in a significant Welfare response would take up to 20 days to recover if a significant earthquake (or similar event) struck Wellington.

Since then the state of other Technology components has further worsened, and the funding gap between what the Ministry needs to remediate and the available cash has widened.

## The Strategic Context

The Ministry's purpose is to help New Zealanders be safe strong and independent. This is achieved through a series of connections into almost every community in New Zealand. The Ministry's work and services touch nearly all New Zealanders at some point in their lives.

The Ministry's services and products span a wide range of social needs, from income and employment support to social housing assessments, from student allowances and loans, to New Zealand Superannuation. In recent times the Ministry has introduced multiple digital channels to provide better services to clients. Clients are expecting that they can transact with us digitally as well as through voice and face-to-face channels.

At the apex of these services the Ministry processes $24 billion in essential payments to New Zealanders every year. All of these services are delivered via a complex ecosystem of technology components of varying ages that have been built up over time and are also a legacy of the Ministry's preceding organisations.

The Ministry has developed a new Technology Strategy which is aligned with the Statement of Intent designed to help deliver the Ministry's emergent Te Pae Tawhiti strategic shifts. This outlines a series of technology investments over a 7-10 year period that need to be done in a certain sequence, and with a likely investment profile of $750m – $1 billion.

The Technology Strategy aims, over time, to address significant pain points associated with the current technology landscape. These pain points include:

- No single client view in the Ministry and across other social sector agencies
- Disparate business processes and lack of automation
- Slow to deliver government policy change
- Our systems are not client-centric
- Staff and clients don't have accurate advice and information
- Difficulty in providing services to partners
- Aging and complex technology

The Technology Strategy dovetails with other Ministry strategies that also seek to address these pain points. In particular, the Data and Analytics Strategy identifies the investments required for the information assets to improve the quality, security and value obtained from information.

The delivery plan associated with the Technology Strategy also deals with how all of the Ministry's bespoke legacy applications will be dealt with over time. It is important to note that there is not a current 'burning platform' imperative to replace the very large bespoke applications that deliver the bulk of the payments and debt management, (i.e. SWIFTT, TRACE and SAL), but these applications represent functionality and a user experience that is increasingly dated and inflexible. These will be the subject of much larger investments and likely to be incorporated into Budget 2020.

Cúram[9], the core client management system, differs from SWIFTT, TRACE and SAL in that it is a Commercial off the Shelf (COTS) software product provided by IBM. Cúram is purpose built for nations, states, and counties to administer their social programmes. It is continually being developed and enhanced by IBM and now has a quarterly release cycle. Among the enhancements planned for Cúram is to make amenable to operate in an IaaS environment (not part of this business case).

This process commenced 2016, when the Ministry completed the task of retiring two major legacy bespoke client administration/case management applications (SOLO and UCVII) by migrating all the data and functionality into Cúram. The Cúram platform has significantly more functionality available than the Ministry is currently using, and much of this is applicable in the MSD context. It is intended to expand the use of Cúram at the Ministry to incorporate those functions.

The assessment of the role of Cúram is an ongoing one. As part of the Technology Strategy, Cúram has been reassessed, and remains a significant part of the Ministry's strategic platform, and will support the objectives of Te Pae Tawhiti. The detailed assessment explaining this conclusion is in Appendix 4.

In broad terms the plan for our large applications is to migrate all statutory eligibility and entitlement calculations into the Rules Engine embedded in Cúram, and further standardise on the Cúram platform for all client administration and case management functions. Over time Cúram will be the 'single source of truth' as a system of record for the client. It will also be a single source of truth for the statutory rules of the benefit system enshrined in the social security act. This will also reduce the six technology pain points by using the out of the box features of Cúram.

In this context, SWIFTT and TRACE will be retired after the eligibility and entitlement rules are migrated to Cúram and the payment schedule moved to a new Financial Management Information System (FMIS).

There is a similar strategic plan for retirement of the Student Allowances and Loans (SAL).

[9] Cúram – Social Services framework from IBM. Recently re-branded as SPM, but Cúram as the product name is still widely used. MSD has licenses to this product

Back-office applications such as the FMIS and Payroll are generic commodity type applications where the Ministry plans to adopt wider government oriented solutions.

Systems of engagement and systems of innovation (systems that face client, partners and staff) will be predicated on an API strategy that opens up our systems of record for others to use, and which will involve open source approaches, and proprietary approaches. It will also involve a small set of bespoke applications such as MyMSD where rapid development and turnaround times are demanded.

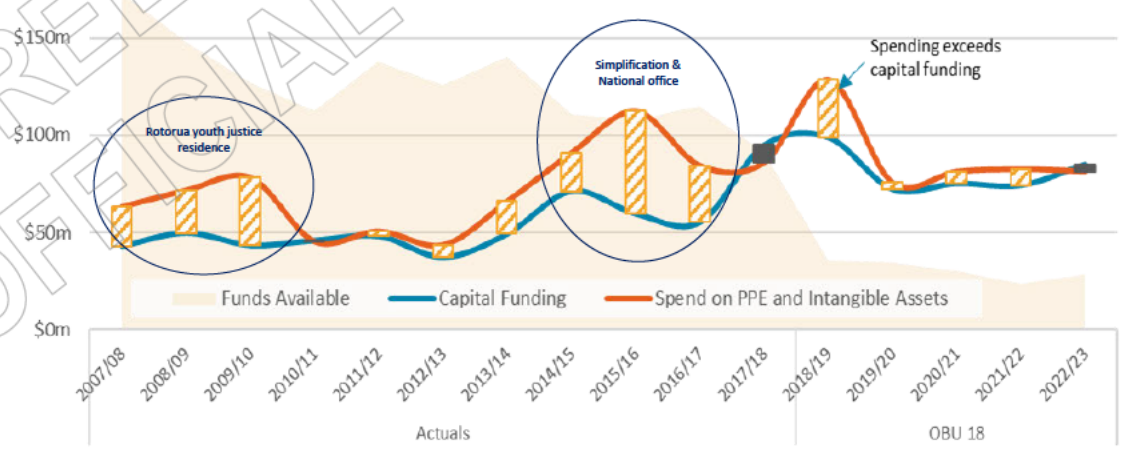
Whilst the full vision of the Ministry's Technology Strategy is not the subject of this investment proposal, it puts some of these replacement projects in context.

For example DREW retirement, which is in scope for this business case, is the foundational project for consolidation of statutory eligibility and entitlement rules into one place so they can be changed more easily to accommodate government policy change and present one source of the truth to staff, clients, and partner. It is also an essential pre-requisite to the eventual retirement of SWIFTT and TRACE. Once the rules are defined in Cúram they can be progressively removed from SWIFTT. The final part of SWIFTT retirement will be to generate payment instructions from Cúram directly to the FMIS, which will manage the payment schedule.

Also, in relation to the Hindin retirement, Cúram has the functionality to perform Review of Decision and Complaints, which are inherently functions of client administration and case management and belong in the core client management system. The overall reduction in discrete systems that case managers need to use will represent a reduction in the technology pain points.

## The Financial Context

Capital sustainability has also become an issue for MSD. Over the past decade, investment in assets has continually outpaced capital funding. Accumulated depreciation has been diverted to other priorities to build the asset base, (such as Simplification) while existing assets, particularly in IT, have been sweated.




The current challenge for MSD is escaping the legacy system trap in IT. The status quo is being maintained as the risk of service failure is greater than the risk of not having optimised systems aligned to the organisational strategy. The consequence of being stuck in the legacy system trap is that IT has become an inhibitor of organisational agility.

# The Case for Change

The Ministry has set a new strategic direction, Te Pae Tawhiti – Our Future, which sets ambitious goals for the Ministry and the role technology will play in that future. It is a future where technology fundamentally transforms the way the Ministry interacts with clients, partners and all New Zealanders. In response, a new Technology Strategy has just been completed, describing the new business and technology capabilities required to meet that vision.

In developing the strategy, it is clear that present-day technology impediments exist, and are a barrier to the strategic future.

The Ministry's technology environment is aging and complex, and is the result of short term thinking and expedient solutions. The overall condition of the Ministry's hardware assets is poor with 59% being over 5 years old. The condition of the software assets is also poor with 61% of software not fully supported. Consequently, the risk of operation failure is rated as 'very high' using the Ministry's risk management framework and this risk has a worsening trend in the immediate term. This risk is monitored by the Senior Leadership Team as one of the Ministry's significant risks. The detailed assessment is included in Appendix 2.

The Ministry's capital base has also been depleted, resulting in sweating technology assets to support other developments. This underinvestment has gone on for a significant period of time and we are now at the point where, there are significant risks of operational failure.

As a result of all these factors, the Ministry has a backlog of urgent technology investment needed to continue to provide services. This includes the upgrades to software applications and hardware replacements, as well as stabilisation of the data warehouse. This business case is the first step in addressing this backlog.

There are also significant pain points in the current IT environment that are being felt across the Ministry and the social services sector. These directly affect the quality and efficiency of services delivered to clients. They also affect the quality and reliability of services to shared service partners Oranga Tamariki, the Ministry of Housing and Urban Development, the Social Investment Agency, and the Office of the Children's Commissioner.

The complexity also makes implementation of policy changes difficult (which has implications for the Welfare Expert Advisory Group (WEAG) and Welfare Overhaul). Following Simplification, the criticality of digital channels for delivering key services has increased, leading to a commensurate increase in risk as these systems age.

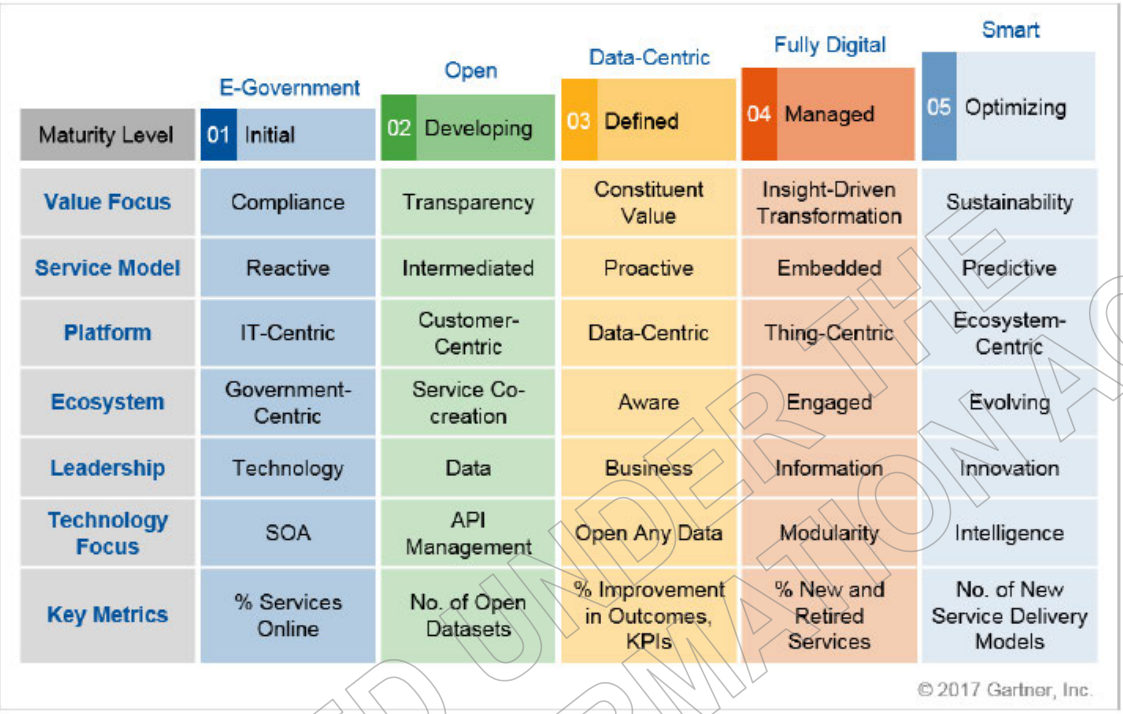
The systems that have the greatest impact on client services and the highest risk of failure have been selected to be part of this business case. Eight projects have been identified, which are described in sub-business cases as part of this programme case.

This business case seeks funding to address the urgent risk of failure, and at the same time put in place building blocks that are needed to support Te Pae Tawhiti.

In writing this business case the Ministry is mindful of not perpetuating the pattern of short term remediation, leading to investment in stranded assets. To address that, the preferred solutions proposed are aligned to the Technology Strategy, support the Ministry's strategic direction, and create assets of enduring value. Recent changes to the governance and prioritisation processes will ensure the programme has the oversight to meet the objectives of risk reduction and enduring value.

# Architectural Perspective

The architectural context for this business case is the maturity of the existing technology landscape. This is best illustrated using the Gartner Digital Government Maturity Model. The model is shown below;



| | E-Government | Open | Data-Centric | Fully Digital | Smart |
|---|---|---|---|---|---|
| Maturity Level | 01 Initial | 02 Developing | 03 Defined | 04 Managed | 05 Optimizing |
| Value Focus | Compliance | Transparency | Constituent Value | Insight-Driven Transformation | Sustainability |
| Service Model | Reactive | Intermediated | Proactive | Embedded | Predictive |
| Platform | IT-Centric | Customer-Centric | Data-Centric | Thing-Centric | Ecosystem-Centric |
| Ecosystem | Government-Centric | Service Co-creation | Aware | Engaged | Evolving |
| Leadership | Technology | Data | Business | Information | Innovation |
| Technology Focus | SOA | API Management | Open Any Data | Modularity | Intelligence |
| Key Metrics | % Services Online | No. of Open Datasets | % Improvement in Outcomes, KPIs | % New and Retired Services | No. of New Service Delivery Models |



The drivers of change, Te Pae Tawhiti and the Government Digital Strategy, require that MSD systems meet at least Defined (level 3). The Technology Strategy describes a future in which MSD will perform at Managed (Level 4).

A current state assessment places MSD at Initial (Level 1). In addition, many of the prerequisite modernisation targets assumed at this level are not in place, or have operation risk. These create barriers to progress, and mean that the enablers to move to higher levels of maturity need to be put in place. The assessment is contained in Appendix 5.

The path for MSD is to mature ICT services to the Defined stage. In that journey, the priorities are;

1. Inhibitors to progress, and issues impacting existing services,
2. Foundational capabilities required to support future digital objectives,
3. Digital capabilities that support client and ecosystem objectives, and
4. Capabilities that support the social sector ecosystem and service innovation

The focus at the Initial maturity level needs to be items that meet priorities 1 and 2.

# Investment Objectives, Existing Arrangements and Business Needs

## Investment Objectives

A series of facilitated case for change workshops were held with key stakeholders to identify the investment objectives and gain a better understanding of the business needs. The key stakeholders identified and agreed the following key investment objectives:

**Investment Objective One:** Reduce risk of operational failure
**Investment Objective Two:** Create assets of enduring value

A further category was also identified. As well as risk, the scope of the service was considered. The focus is on services that have the greatest impact on clients, and on the ability of staff to support clients.

**Table 2:** Investment Objectives

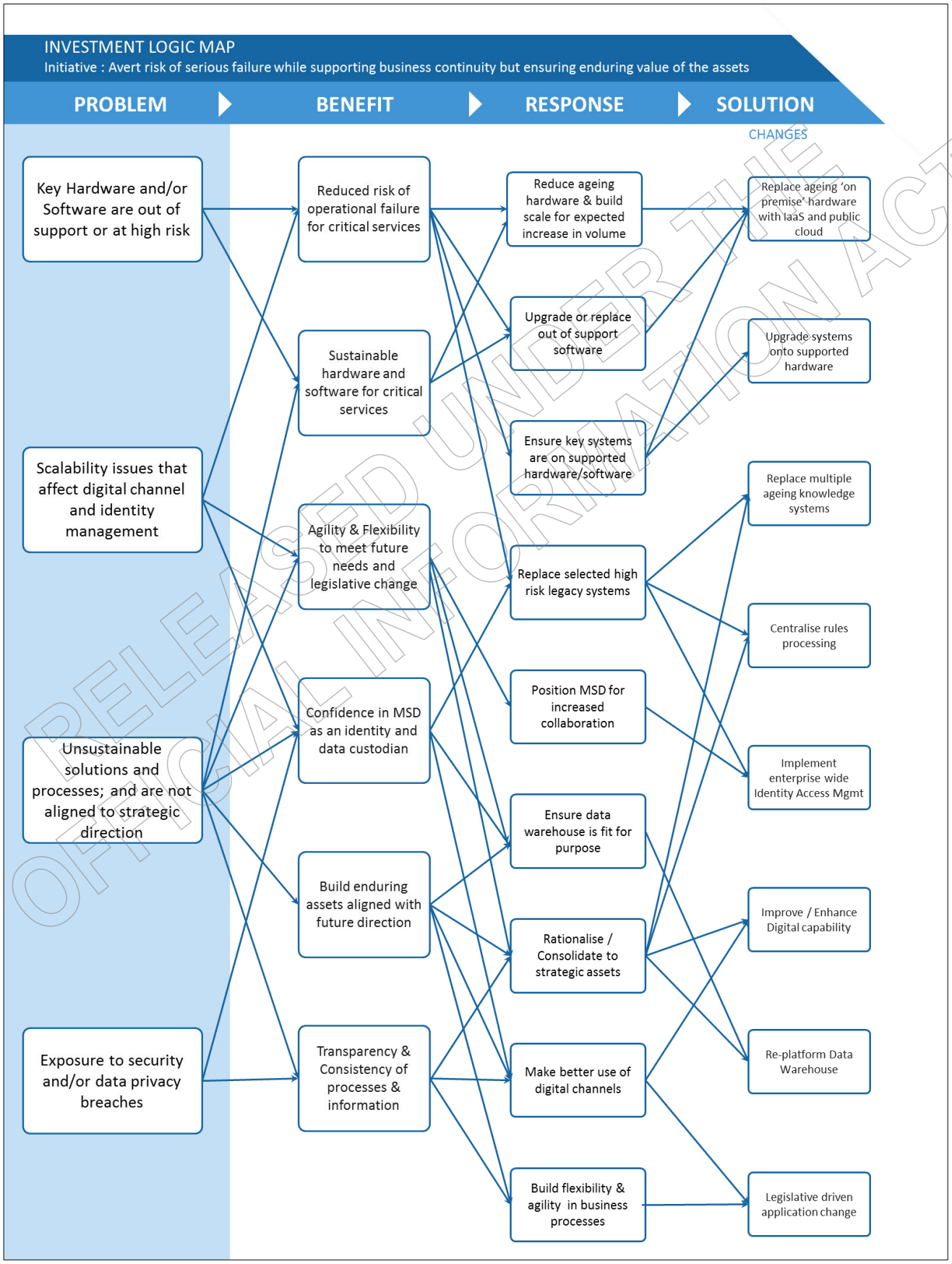
| Investment Objective One | Reduce risk of operational failure |
|---|---|
| **Existing Arrangements** | Approximately 60% of current applications are not fully supported and 59% of hardware assets are over 5 years old |
| **Business Needs** | Increase the supportability of systems to ensure critical client services are able to be delivered<br>Robust management of access to systems to ensure information security<br>Access to eligibility and entitlement rules and processes<br>Access to knowledge bases, data, and work management tools by staff<br>Digital channels that meet the performance expectations with increasing volumes |
| **Potential Scope** | Migrate or retire out of support systems to retire aged hardware<br>Replace specific end of life applications that have no upgrade path |
| **Potential Benefits** | Upgrade selected systems to bring them back into support |
| **Potential Risks** | Reduce the risk of operational failure |
| **Constraints and Dependencies** | Resource to remediate selected software to enable migration<br>Identified points of contention will need to be scaled to meet the programme |

| Investment Objective Two | Create assets of enduring value |
|---|---|
| **Existing Arrangements** | The Te Pae Tawhiti Technology Strategy identifies the significant gap between the applications in place and the future business need |
| **Business Needs** | Systems open to collaborating with agencies and partners<br>Single view of Client, that is extensible across the sector<br>Lower cost of change<br>Faster ability to adapt to legislative change<br>Better experience for staff, clients and partners |
| **Potential Scope** | Tailor the risk mitigations to meet future state strategy objectives |
| **Potential Benefits** | Reduce technology barriers to future change |
| **Potential Risks** | Stranded investments with changes in strategic direction |
| **Constraints and Dependencies** | Resource to remediate selected software to enable migration<br>Identified points of contention will need to be scaled to meet the programme |

Reviewing the investment backlog against these criteria, eight projects were identified that fully meet them, and are included in this business case.

## Investment Options

There is an extensive backlog of work items aligned to the Investment Objectives. To select the preferred choices an Investment Logic Mapping exercise was undertaken with stakeholders to select the highest priority items. The result of that process is summarised in the following figure;



## Assessment against Business Scope and Key Service Requirements

Over the next 5 -10 years, the Ministry needs to replace these applications which are now between 20 and 30 years old, along with a number of other (smaller) bespoke applications. This needs to be done before they become 'burning platforms'. At the current point in time, there are a number of more pressing issues and risks in relation to the application portfolio that need to be addressed as pre-requisite activities to the longer term programme of work.

A series of workshops were held with key Ministry stakeholders to identify the possible investments considering the investment objectives and the investment logic map. The list of initiatives was sourced from the following existing planning documents;

- The Portfolio Executive Committee (PEC) backlog, and
- The technology investments described in the Long Term Investment Plan (LTIP), and
- Initiatives identified in the Technology Strategy

From that list, a long list of items that met the criteria of posing sufficient operational risk, and whether potential solutions of enduring value would be created. This second criteria is significant as it captures the uncertainty that would mean an item may be worthy of investment, but at this time its future is not sufficiently clear to make that investment. They were then grouped by the related business area that they support.

**Table 3:** The potential investment candidates that were discounted and the reasons why

| Business capability area | Applications | Risk of Failure | Solutions of Enduring Value | Investment (L < $1M, M $1-$10M, H >$10M) | Reason for rejection | Treatment |
|---|---|---|---|---|---|---|
| **Rules consolidation** | SWIFTT<br>DART<br>SAL | M | M | H | • Dependent on retirement of DREW | Include in 2020 case |
| **Client Record consolidation** | SWIFTT<br>CMS<br>Service Plans, Outcome Management | L | M | M | • Required for the retirement of SWIFTT<br>• Needs to be sequenced with rules consolidation | Include in 2020 case |
| **Client Payment services** | SWIFTT<br>TRACE<br>WAM<br>COMET<br>AP1<br>SAL | M | L | H | • Dependent on FMIS capability<br>• Lower risk than other legacy systems | Include in 2020 case |
| **Provider Services** | FS-NET<br>ART<br>SORT | M | M | M | • Dependent on MSD partnering model<br>• Lower risk than other legacy systems | Include in 2020 case |
| **Provider Management** | Conquest<br>RDA<br>FAC | M | L | M | • Dependent on MSD partnering model<br>• Lower risk than other legacy systems | Include in 2020 case |
| **External information repositories** | Websites, FACS helpline, WFF | M | L | M | • Dependent on changes in operating model | Include in 2020 case |
| **Student management** | SAL<br>VOS<br>MSL<br>ODS | H | H | H | • Choose to focus on Work and Income business at this time<br>• Lower implementation risk of other projects by excluding a whole business segment<br>• Lower risk than other legacy systems | Include in 2020 case |
| **Client communication management** | Digi Objective, ECS, ECS Repository, VRetrieve, SWIFTT<br>SAL | M | H | H | • Lower risk than other legacy systems<br>• Comprehensive correspondence management solution has enduring value but is a lower implementation priority | Include in 2020 case |
| **FMIS** | Kea | L | H | H | • Lower risk than other legacy systems | Include in 2020 case or other funding bid |
| **HRMS suite** | Global<br>BCR | H | M | M | • Lower risk than other legacy systems | Include in 2020 case |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Supporting client management systems** | AIMOS<br>Notify<br>OBMAN<br>RecruitMe<br>ABT<br>CAD | M | M | H | • Lower risk than other legacy systems | Include in 2020 case |

Note that one of the strategic decisions made in the short-listing process was to focus on the Work and Income services, which resulted in excluding Student services from the short list. This was done to reduce complexity and lower the risk of delivery for the projects in the preferred way forward.

## Short Listed Options

The short list was assessed in more detail against the investment objectives. The following table is a summary of the priority areas identified, and the impact of realising the service risks. The detailed scope for each is described in the Economic Case section.

The table contains a summary of each initiative against the four drivers of the scope and urgency of each initiative.

The drivers are;

- The scope of the service – how the service is used and how prevalent it is, and the impact a disruption to that service would create
- Risk – the assessed likelihood of an impact to that service
- Impact – the observable outcomes of a disruption to the service
- Enduring Value – what extent the remediations proposed are aligned with the Te Pae Tawhiti Technology Strategy and have enduring value

**Table 4:** Summary of the priority areas identified, and the impact of realising the service risks

| Initiative | Scope of the services | Risk Rating | Impact | Enduring Value |
|---|---|---|---|---|
| **1. Identity Management** | • 650,000 registered online users<br>• 10,000 MSD staff | Very High | • No online services<br>• Staff unable to access line of business systems | • Fully supports Te Pae Tawhiti objectives<br>• Access control and security risks become Low |
| **2. Centralise Rules Processing** | • 2,800 service centre and call centre staff<br>• Calculates value and 'what if' scenarios for 21 benefit types<br>• 100,000 applications per year | Very High | • Inability to process benefit applications and change in circumstance queries / actions | • Fully supports Te Pae Tawhiti objectives<br>• Cost of rule changes lowered |

| Initiative | Scope of the services | Risk Rating | Impact | Enduring Value |
|---|---|---|---|---|
| **3. Foundational Knowledge Base** | • 2,800 service centre and call centre staff<br>• Staff daily use: 600 Work and Income and 500 Studylink<br>• 400,000 page views per month, 20,000 page views per day<br>• 4,500 Review of Decision annually<br>• 7,500 complaints annually<br>• Studylink: 15,600 interactions and 10,500 escalations annually | Very High | • Inability to process related Work and Income and Studylink inquiries<br>• Inability to manage Complaints within the Hindin platform<br>• Inability to manage Review of Decisions within the Hindin platform<br>• Inability to manage student related escalations and interactions within the Hindin platform | • Fully supports Te Pae Tawhiti objectives<br>• Increased service effectiveness |
| **4. Data Warehouse Re-platform** | • Data management and reporting for MSD, Oranga Tamariki and Housing and Urban Development<br>• Daily data from over 50 applications and 8 agencies<br>• 270,000 case manager reports monthly<br>• Service matching for 280,000 main benefit clients weekly | Very High | • Case managers and service centres significantly operationally impaired<br>• Increased security risks | • Fully supports Te Pae Tawhiti objectives<br>• Business critical functions integrated into the appropriate application<br>• Flexible and expandable analytics capabilities |
| **5. Digital Capability** | • 650,000 registered online users<br>• 284,000 active users per year | High | • No service via MyMSD<br>• Some transactions unable to be completed in a timely manner | • Fully supports Te Pae Tawhiti objectives |
| **6. Software and Security upgrades** | • 300+ applications<br>Compute:<br>• 9% 3-5 years old<br>• 67% 5 years +<br>Storage:<br>• 30% 3-5 years old<br>• 40% 5 years + | High *(operational failure)*<br><br>Very High *(security vulnerability)* | • Inability to access affected systems<br>• Long restoration times (hardware)<br>• Inability to restore service (security) | • Partially supports Technology Strategy objectives |

| Initiative | Scope of the services | Risk Rating | Impact | Enduring Value |
|---|---|---|---|---|
| **7. Replacing ageing 'on premise' hardware with Infrastructure-as-a-Service and public cloud** | • 300+ applications<br>Compute:<br>• 9% 3-5 years old<br>• 67% 5 years +<br>Storage:<br>• 30% 3-5 years old<br>• 40% 5 years + | Very High *(operational failure)*<br><br>Very High *(security vulnerability)* | • Inability to access affected systems<br>• Long restoration times (hardware)<br>• Inability to restore service (security) | • Fully supports Technology Strategy objectives |
| **8. Legislative Driven application change** | • System changes needed to execute legislative | Very High | • Legislation is delivered through combination of systems and manual staff actions, incurring admin overhead | • Correct and accurate delivery of legislation that does not require significant staff actions |



## Potential programme options

Within the potential scope of this proposal, the main programme options were identified by key stakeholders, and assessed against the key objectives. Potential programme options identified but discounted include:

### *Option 1: Do nothing*

The do nothing option would involve:

- Accepting that running the bulk of the hardware infrastructure further beyond the end of its useful life will incur increasing rates of serious failure affecting front line staff and client services
- Accepting that the backlog of deferred software and security upgrades will grow larger with increasing rates of serious failure affecting front line staff and client services; and may include serious information security and privacy breaches
- Accepting that the rules processing application currently used by front line staff might not be able to be changed in a timely manner to address Welfare Expert Advisory Group (WEAG) recommendations accepted by government
- Accepting that the current knowledge services platform will continue to confuse and misinform front line and call centre staff so they give inconsistent answers to clients
- Accepting that the current identity management systems will continue to be prone to error and serious failure affecting front line staff and client services; and that the Ministry will not have an identity management foundation to enable future digital initiatives for partners and clients
- Accepting the current risk of unauthorised access to information, including client records
- Accepting that the current digital platform will not have the ability to be unable to scale up to process rising levels of client self-service transactions.

Overall, failing to invest in these technology components will worsen the overall risk of systems failure for the Ministry and increase the cost, time and risk of any urgent system changes needed. It is therefore not a preferred option.

### *Option 2: Reduce services*

The Ministry could reduce services that depend on technology and thereby cut down on the number of systems that need to be supported, with the result that costs would come down. In particular this approach could be applied to systems that are not directly used in providing services to clients. This would allow reprioritisation of investment to high risk areas, but at a cost to other areas.

This approach would be very difficult to measure in that loss of staff productivity would likely lead to cost pressures elsewhere in the organisation or unintended adverse consequences for clients. This option is also not preferred because the great majority of the Ministry systems do in fact deal with client services, so it is highly unlikely that sufficient savings could be made.

### *Option 3: Rationalise the number of technology systems*

This option involves reducing the number of technology systems whilst maintaining (or increasing) the services supported. This will reduce costs (which may be offset by volume increases).

The Ministry's Te Pae Tawhiti Technology Strategy does plan for a reduction in the number of supported systems, and an elimination of large scale bespoke applications. The target environment has two broad approaches for retirement of legacy applications:

1. Standardising specialist eligibility and entitlement based functionality and client management onto the IBM Cúram COTS product
2. Moving all commodity and utility type applications to the cloud

This is part of the Ministry's long term strategy and is aligned with the New Zealand government digital strategy, but it is not preferred for budget 2019. This is due to the high risk of the current situation and higher cost in the short term. The long term strategy will take some years to put into place given the scale of the Ministry's operations. In the meantime the Ministry will be obliged to keep the systems up to date and running for the next three to four years in order to reduce the current risk of failure.

### *Option 4: Defer investment until budget 2020*

The Te Pae Tawhiti Technology strategy has identified a number of technology initiatives required to transform the Ministry. The system replacements in this proposal are in that set of initiatives, and need to be done in the short term because these systems are:

- beyond end of life, or
- have significant architectural flaws, and
- are pre-requisites to the full Te Pae Tawhiti strategy.

In developing the Technology Strategy, the Ministry has identified some serious pain points attributable to the current Technology landscape that need to be addressed regardless of Te Pae Tawhiti:

- no single client view
- disparate business processes and lack of automation
- slow to deliver government policy change
- product based systems rather than client outcome based
- staff and clients not having access to consistent and accurate advice

- ageing and complex technology.

This investment will result in reducing most of these pain points.

The defer investment option is not preferred because it will increase the Ministry's risk in the short term and will mean that the pain points will hamper staff and clients for a longer time.

# The Preferred Way Forward

The preferred programme involves performing necessary upgrades in a manner that reduces risk of operational failure, and creates assets of enduring value. There are eight projects that have been shortlisted that meet these criteria. Projects 1-5 are Replacement projects, and projects 6-8 are Maintenance projects.

The projects are:

| Project | Description |
|---|---|
| **1. Identity Management** | Implement an enterprise Identity Access Management solution for users (staff, partners and clients) to replace ageing platforms to position the Ministry for partnering effectively to deliver enhanced services to New Zealanders. |
| **2. Centralise Rules Processing** | Migrate benefit rules from ageing and out-of-support software, which can't be upgraded to an open, accessible and supported platform to create consistent eligibility and entitlement information to New Zealanders and partner organisations. |
| **3. Foundational Knowledge Base** | Move knowledge assets from an old repository, which can't be upgraded, to a knowledge repository for staff to seamlessly access consistent advice and process guidance, regardless of channel, and improve the client experience.<br><br>Move Review of Decision, Complaints and Provider Management functions currently resident on the old knowledge management platform to the MSD client and provider management system Cúram SPM. |
| **4. Data Warehouse Re-platform** | The Ministry's data warehouse has a high risk of breaching of privacy rules. It is also at high risk of operational failure resulting in clients' benefits and service to clients being disrupted and the inability to deliver organisational strategic goals due to the unusually high maintenance, unplanned work, recovery, and support load. |
| **5. Digital Capability** | To meet increasing client demand arising from hardship, client complexity, national superannuation, and housing, the Ministry will make more transactions available online. The current digital platform contains some profound weaknesses in terms of components that need to be replaced and/or re-engineered if the whole platform is to scale up to meet additional transactional demand. |
| **6. Software and Security upgrades** | For technology assets that need to be upgraded because they will be required for the next four years, due to the lead time needed to transform much of our existing technology setup as part of Te Pae Tawhiti. |
| **7. Replacing ageing 'on premise' hardware with Infrastructure-as-a-Service and public cloud** | In line with New Zealand government strategy to move to as-a-service hardware consumption, the Ministry will stabilise critical services by moving out-of-support infrastructure assets to Government Infrastructure cloud and public cloud options. |
| **8. Legislative Driven application change** | To enable MSD to enact legislation changes requires significant technology and process change which can incur significant cost. Historically MSD have absorbed these change costs within its baseline and have recently indicated that this practice can no longer be sustained. |

# Main Benefits and Risks

**The table summarises the problems from the realisation of the risk of failure in each case, the impact of an outage, and how the preferred solution supports longer term objectives of the Ministry.**

**The residual risk after implementing the proposed solutions, and the implementation risk, is described in each individual case.**

| 1. Identity Management | |
|---|---|
| **Problem** | Poorly understood bespoke applications such as AUM and CYFHUB are integrated into an in-house IdAM solution. Out of support third party software, such as iPlanet, is stranded on old hardware (up to 14 years old) due to a lack of an upgrade path. |
| **Impact** | 10,000 MSD staff unable to log in or access systems, stopping all client services.<br>45,000 clients unable to access online services on and single given day<br>Oranga Tamariki staff unable to access selected systems |
| **Solution** | Off the shelf software third party identity store for administration of identity and policy based access management. The solution is largely vendor based, and a mixture of COTS, SaaS and PaaS components. |
| **Alignment** | High.<br>The Technology strategy (Section 2.2, Agency Interoperability and Life Events) identified Identity Management as a core capability to enabling integration of cloud services, and delivering greater client digital services, integrating partner services, and providing seamless client experience across the social services sector. |
| **Risk of stranded investment** | None.<br>The solution has been developed to support the Ministry's strategy, and has been validated with other agencies and external experts. |

| 2. Centralise Rules Processing | |
|---|---|
| **Problem** | The system is supported by Venturi, a company that now consists of one 70 year old person living in France. The software is XpertRule version 1.4, which is out of support and for which skills are scarce. The application is PC based, making it vulnerable to faults introduced with an evergreen Windows 10 operating system. |
| **Impact** | 2,800 contact and service centre staff members unable to process income support applications (there are 100,000 applications per year) |
| **Solution** | Expand the existing statutory rule base in Cúram to include eligibility and entitlement rules, allowing staff to process application without switching between systems. Build APIs into Cúram Rule Sets and display 'what if' scenarios and/or client in-context scenarios. |
| **Alignment** | High.<br>The solution aligns with the Technology Strategy objective of consolidating rule into the core systems and making them reusable through APIs. (Tech Strategy, Section 4.6, Centralise rules into core systems) |
| **Risk of stranded investment** | Low.<br>Ideally policy work to simplify statutory rules would accompany any change to reduce the implementation cost and complexity. Given the timeframes this would not be feasible. |

| 3. Foundational Knowledge Base | |
|---|---|
| **Problem** | The Hindin system has been out of support for 10 years. It has a code base for an unsupported and stranded Java version. The software runs on Solaris and HP-UX operating systems, both of which are legacy and costly to support. The hardware needed to run these operating systems is nine years old. |
| **Impact** | 2,800 contact and service centre staff members unable to process selected inquiries.<br>Staff unable to;<br>• perform 20,000 page views per day to access knowledge bases,<br>• record 15,600 interactions (annually),<br>• manage 4,500 Review of Decisions (annually),<br>• manage 7,500 complaints (annually), and<br>• manage 10,500 escalations (annually) within the system. |
| **Solution** | Knowledge repositories moved to a repository that is able to integrate with other systems and support integration with smart agents (like smart assistants), to make finding the right information easier for staff. Processes implemented in Hindin (Review of Decision and Complaints) to be implemented as part of the client management systems. Education providers to be served by the appropriate provider management system. |
| **Alignment** | High.<br>The Technology Strategy roadmap for knowledge repositories includes Hindin and other legacy repositories (to be part of future work programmes). It also specifies the retirement of bespoke client related workflows into the core client management systems. (Tech Strategy, Section 7.4, Retire or upgrade out of system support) |
| **Risk of stranded investment** | Low.<br>The solutions leverage existing capabilities. |

| 4. Data Warehouse Re-platform | |
|---|---|
| **Problem** | Infrastructure and support model does not support the criticality of the service to front line staff. Data management configuration and practices expose MSD to data privacy breaches. The complexity of the system and reporting rules impacts the accuracy and timeliness of information, potentially leading to incorrect decisions |
| **Impact** | Daily case manager reports (270,000 monthly), and service matching reports for clients (280,000 weekly) are unavailable significantly disrupting client services and increasing security risks. Oranga Tamariki and HUD staff are not supplied with selected reports and data, with subsequent operational impact. |
| **Solution** | Rebuild the analytics platform on a modern, extensible, scalable solution. Decommission older components, migrating specific functionality into the appropriate line of business system (i.e. booking system for trespassed individuals). |
| **Alignment** | High.<br>The Technology Strategy describes the move to Smart Services (Tech Strategy, Section 4.5, Insight driven through analytics), which require the foundational analytics platforms be brought up to a modern standard to enable new digital services for clients, staff and partners. |
| **Risk of stranded investment** | None. |

| 5. Digital Capability | |
|---|---|
| **Problem** | The current digital platform will fail under increased load due to design limitations of the existing system:<br>The high number of exceptions requiring human intervention<br>Client identity for 650,00 client held in a bespoke database that is unable to scale further, and represent an operational risk<br>Inability to scale horizontally. MyMSD was originally architected for 1200 active concurrent users now needs to scale to 3,000 |
| **Impact** | Clients will be unable to complete online transactions. There are on average 45,000 client transactions a day. Alternative channels (contact centres and service centres) are unable to process the volume manually. |
| **Solution** | Implement a scalable architecture for MyMSD. This includes simplifying the components of the system, decoupling the client identity management (to the new IdAM solution), and simplify task management and straight-through processing. |
| **Alignment** | High.<br>Increasing the use and functionality available through digital channels are key objectives of the Ministry's business and technical strategies. (Tech Strategy, Section 1.1, Improve digital services). |
| **Risk of stranded investment** | Low.<br>The project growth of digital channel volumes means the investments will be fully utilised.<br>The pace of change in client digital channels requires frequent reinvestment. |

| 6. Software and Security upgrades | |
|---|---|
| **Problem** | Over 300 applications dependent on out of date hardware and software. There is a high risk of hardware failure, and a high risk of vulnerability to cyber-attack. |
| **Impact** | Loss of core services to over 1,000,000 clients. Loss of selected shared services for OT, SIA and HUD. |
| **Solution** | Upgrade all equipment and software to supportable levels as required by IT assurance and risk practices. |
| **Alignment** | High.<br>By extending the life of core systems in a manner that supports a move to as-a-Service offerings (Tech Strategy, Section 7.4, Retire or upgrade out of support systems). |
| **Risk of stranded investment** | None.<br>Investment is required in all scenarios. Sufficient compute workload that is not cloud ready remains to utilise the full fife of infrastructure investments. |

| 7. Replacing ageing 'on premise' hardware with Infrastructure-as-a-Service and public cloud | |
|---|---|
| **Problem** | Over 300 applications dependent on out of date hardware and software. There is a high risk of hardware failure, and a high risk of vulnerability to cyber attack. |
| **Impact** | Loss of core services to over 1,000,000 clients. Loss of selected shared services for OT, SIA and HUD. |
| **Solution** | Move compute workloads to as-a-Service offerings. |
| **Alignment** | High.<br>Supports the strategic objective of reducing infrastructure ownership by 75% by 2022. (Tech Strategy, Section 7.3, Retire ages infrastructure). |
| **Risk of stranded investment** | None.<br>Through use of as-a-Service offerings. |

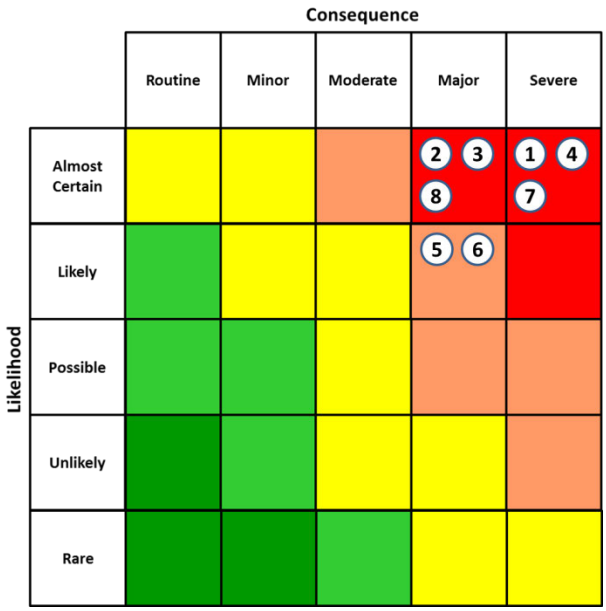
| 8. Legislative Driven application change (Recapitalisation) | |
|---|---|
| **Problem** | The on-going implementation of legislative change has traditionally been absorbed within baselines. This has led to changes being kept to the minimum required to enact legislation. |
| **Impact** | Change has been slow to implement, and still reliant on manual intervention. |
| **Solution** | Allocate sufficient funding to support the timely and accurate implementation of the legislative change programme. |
| **Alignment** | High. |
| **Risk of stranded investment** | Low.<br>Implementation is focused on updating core systems that are part of the long term strategy. |



## Operational Risk Impact

One of the key risks monitored by the Leadership Team is the Technology Systems Availability, which is assessed as Very High, with the trend Increasing.

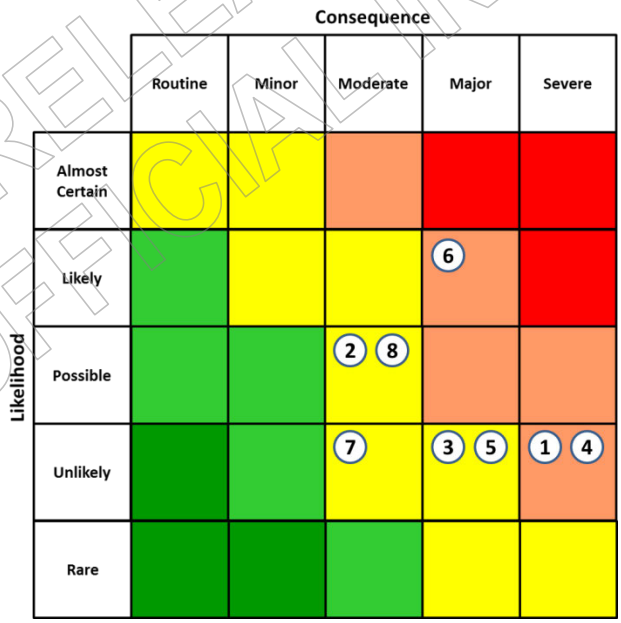
Using the Ministry's risk assessment matrix of Likelihood and Consequence, the systems that are included in the preferred way forward can be represented in the following summary chart;




The systems involved are represented using the eight Business Case Initiatives:

1. Identity and Access Management Replacement
2. Centralise Rules Processing
3. Foundation Knowledge Management
4. Data Warehouse Replacement
5. Digital Capability
6. Software and Security Upgrades
7. Replacing on-premise hardware with IaaS and Public Cloud
8. Legislative Driven Change

The target risk profile at the successful completion of the Preferred Way Forward is shown in the next chart;



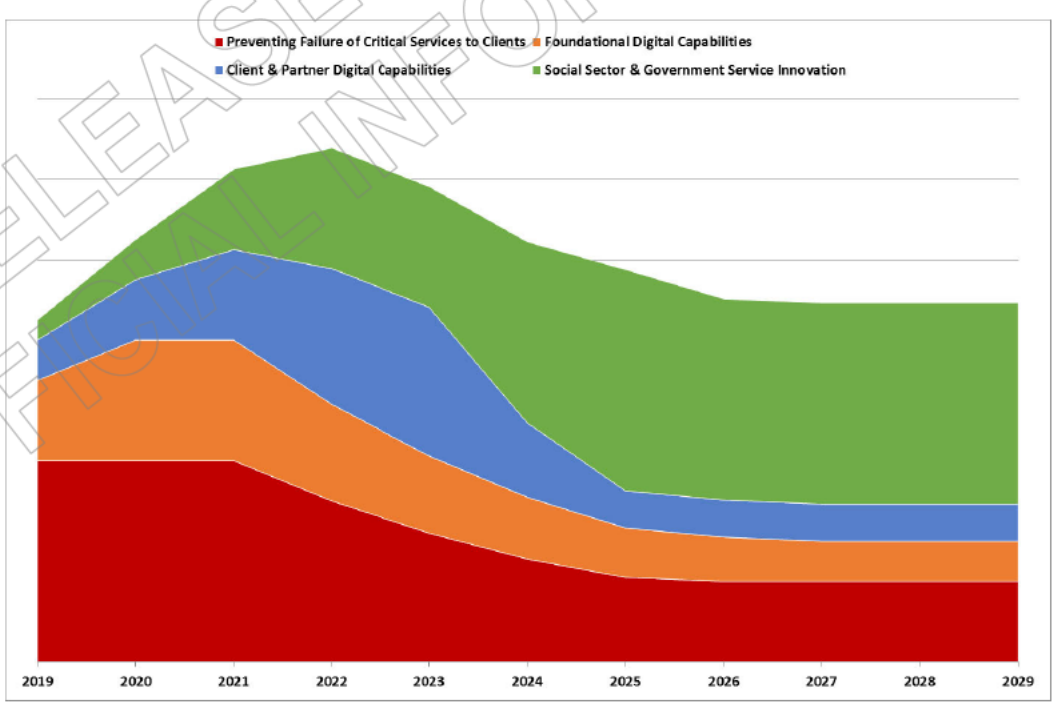
## Alignment with Ministry Technology 10 Year Strategic Roadmap

The short-listed investment options in this Business Case focus on the immediate need to **Prevent Failure of Critical Services to Clients**. These investments are necessary in the near-term in order to bring the MSD technology platform to an acceptable level of risk. After successfully addressing these immediate technology risks in the near-term, the Ministry will then be able to prioritise more of its technology investment on digital transformation in the future.

This continued digital transformation will enable the Ministry to achieve its future technology vision; ***"To transform to an open technology platform, to connect MSD to clients, partners, and other social sector participants as the keystone of the social services ecosystem."*** The Ministry's future technology platform will enable the success of the Ministry's organisational strategy, Te Pae Tawhiti, and the Government Digital Strategy.

The characteristics of the Ministry's planned digital transformation are described in more detail below. Although these phases are predominantly sequential, MSD has already been investing in client and partner digital capabilities for several years, and continues to provide on-going enablement of sector service and government service innovation.


The following indicative timeline illustrates the anticipated focus areas for the Ministry over the next ten years.




In order to enable the **MSD Future Digital Platform** to participate more in the social services and public ecosystem, the Ministry needs to first ensure that the prerequisite **Foundational Digital Capabilities** are in-place.

The key foundational capabilities planned for the near-term include the following:

- Identity and Access Management (IdAM) capabilities to support client and partner identity and access management; which are already in- place using tactical implementations and need to be moved to a strategic and sustainable IdAM platform in the near-term
- Application Programming Interfaces (APIs) to enable greater information sharing with partners in alignment with the Government API Strategy; for which the Ministry is currently underway with establishing its strategic API platform to share information with partners in the near-term and mid-term
- Cloud capabilities to enable the Ministry to host technology services on Cloud computing services; which began with the Ministry's Availability and Resilience programme, and will continue with migration of Infrastructure to as-a-Service (aaS) cloud models in the near-term, enabling greater consumption of Public Cloud services in the mid-term and long-term

Once all of the Foundational Digital Capabilities are in-place, the Ministry needs to continue to mature its existing **Client and Partner Digital Capabilities**:

- **Client Digital Capabilities** have been initially established across the Ministry:
    - **Work & Income:** MyMSD and Cúram Universal Access enable the Ministry's MyMSD digital experience; which requires immediate investment described in this Business Case to ensure it can scale to meet future client demand
    - **StudyLink**: MyStudyLink (MSL) is a bespoke digital experience for Students; which will require near-term investment to migrate to a more modern and sustainable technology platform
    - **Seniors**: Has a very basic digital presence, limited to digital content, and investment is needed to enable a tailored digital experience for Seniors in the near-term
- **Partner Digital Capabilities** are in early stages of maturity across the Ministry:
    - The Ministry's strategic **API platform** is beginning to be used to enable APIs to share information with trusted partners
    - The Ministry has several siloed legacy channels to enable **partner digital self-service**; which will require near-term investment to rationalise to a more modern and sustainable technology platform

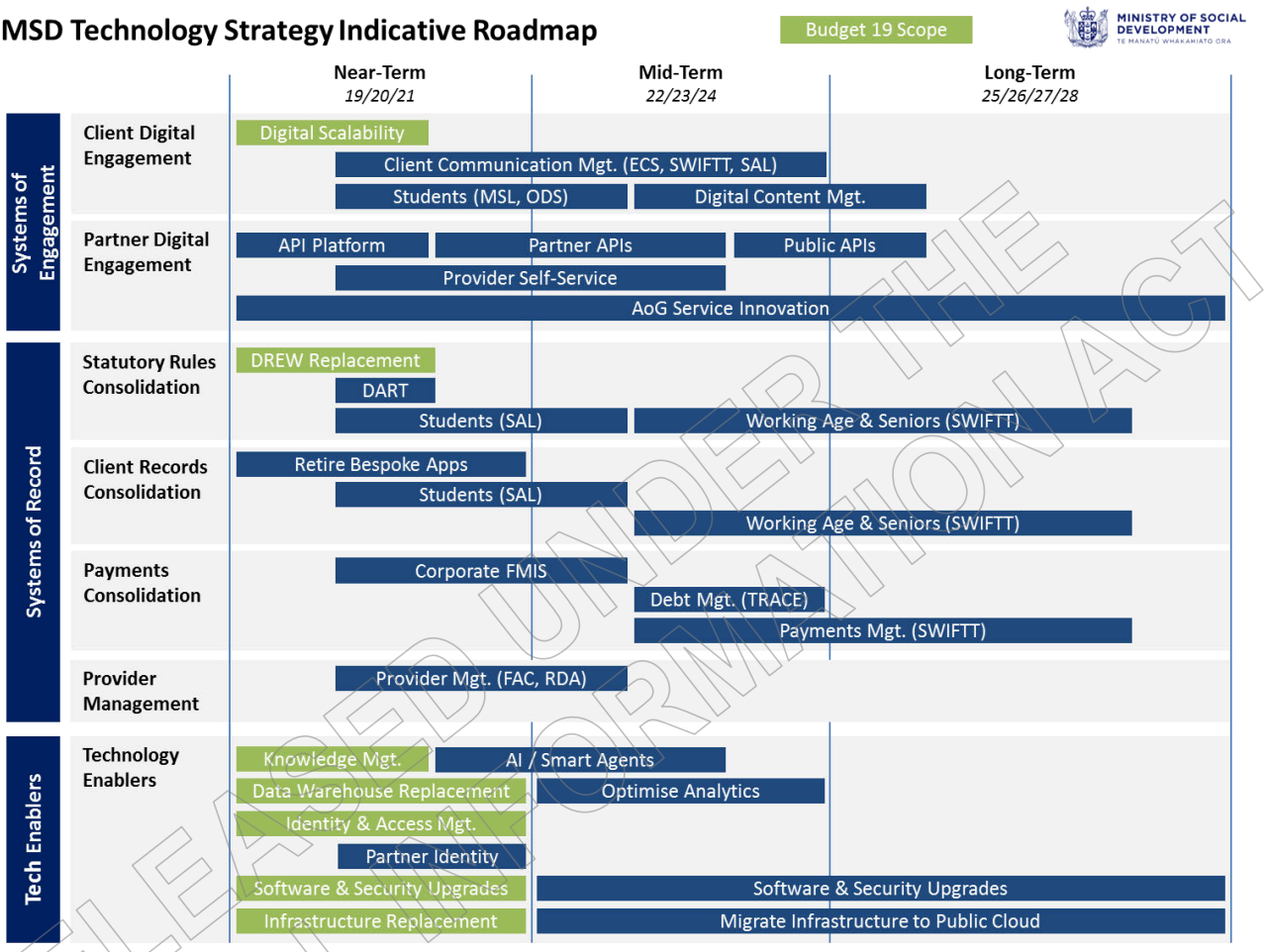
The Ministry's recent participation in **Social Sector & Government Service Innovation** includes the SmartStart initiative; which involved MSD collaborating with Department of Internal Affairs, Inland Revenue, and Ministry of Health, to enable greater integrated Government support for expecting parents.

Once the MSD technology platform has achieved an acceptable level of risk, and foundational digital capabilities have been established, greater focus in this area will become possible.

As illustrated in the below **MSD Technology Strategy Indicative Roadmap**, each of the short list investments are critical enablers for the Ministry to digitally transform MSD's technology platform and will deliver strategic assets which provide enduring value:

1. **Digital Scalability** will enable the Ministry's digital client channels to scale to future client digital demand, and will enable greater conversion of clients to digital channels in the future; which will empower clients with self-service capabilities and will reduce barriers to clients connecting with the Ministry
2. **DREW Replacement** is the initial step in enabling the Ministry's long-term strategy for consolidating statutory rules; which will lead to less duplication across technology systems, greater re-use, and faster and cheaper change of statutory rules in the future
3. **Knowledge Management Replacement** will provide a new technology platform for staff-facing knowledge management, which will be able to take advantage of recent breakthroughs in Artificial Intelligence (AI) and Smart Agents, and scale to enable digital client-facing and partner-facing knowledge management in the future
4. **Data Warehouse Replacement** will enable the Ministry to take advantage of advanced analytics to support operational decision-making

5. **Identity & Access Management** will enable a sustainable technology platform for staff identity, and will enable sustainable foundational digital capabilities for client and partner identities in the future
6. **Infrastructure Replacement** will continue to migrate the Ministry's technology services onto Cloud services; reducing physical ownership of infrastructure assets, and enabling greater consumption of Public Cloud services in the future






## Risk of Stranded Investment

The Ministry is continuing to elaborate the Te Pae Tawhiti strategy during calendar 2019, which will firm up some changes to the Ministry's operating model. There is a high probability that this will result in proposals in budget 2020 for technology changes to support Te Pae Tawhiti. It is therefore reasonable to ask the question whether any of the proposed Budget 19 investments would be impaired by subsequent changes to the operating model.

However the Ministry has assessed that risk (of impaired or stranded assets) as very low.

The budget 2019 business case covers Technology investments that:

- are for systems fundamental to the Ministry's operation,
- remediate elements of the Ministry's technology environment that are most at risk of failure,
- cannot be funded from existing budgets,
- have long term strategic value, and
- which are foundational pre-requisites to delivery of the Technology Strategy as a whole.

The Ministry's assessment is that all of the proposed investments meet the above criteria and therefore are a low strategic risk. This is described fully in Appendix 3.

# Key Constraints and Dependencies

The proposal is subject to the following constraints and dependencies. Dependencies are monitored as part of the programme management process and are reported to the Programme Board and PEC. Constraints are managed through the risk management processes, and are also reported to the Programme Board and PEC.

**Table 5:** Key constraints and dependencies

| Constraints | Notes |
|---|---|
| **Limited Workforce Capacity** | A high number of the MSD workforce will be required to participate and support the programme delivery due to their expert knowledge of Ministry business processes and technology systems.<br><br>This additional demand will compete with existing workforce demand; including delivering existing legislative commitments, implementing the recommendations from the Welfare Expert Advisory Group (WEAG), supporting Business-as-Usual (BAU) organisational activities, and the existing pipeline of technology systems maintenance and change activities. |
| **Limited Organisational Change Capacity** | This programme will result in multiple significant changes to key technology systems used by staff over two years. The organisation has a limited capacity to absorb organisational and technology change before it suffers from "change fatigue". |
| **Dependencies** | **Notes and Management Strategies** |
| **Additional Workforce** | The Ministry will need to be able to hire the required additional workforce, which is dependent on the availability of specialist business and technology resources in the New Zealand labour market. |
| **Technology and Consulting Vendor Support** | The Ministry will require expert advice and resource capacity provided by current and future technology and consulting vendors. |
| **Procurement Activities** | The programme delivery is dependent on the successful and timely outcome of procurement activities across multiple programme streams. |
| **Government Cloud Services Certification & Accreditation** | The programme delivery is dependent on agreement from GDCO that the cloud services being used to replace high-risk infrastructure assets meet New Zealand information security and privacy standards. |
| **Sequencing of WEAG Delivery** | Future legislative changes, including implementing recommended WEAG changes, will be easier to implement if this work is able to progress, and the sequencing of programme deliverables can be coordinated. |

# Scaling Options

## Background

In October 2018, the Ministry submitted two budget bid templates technology investments for recapitalisation and system replacement initiatives. Combined these totaled $390m ($148m capital and $242m operating).

Subsequently, considerable work has been done to refine these numbers and pare back the scope of the exercise to the minimum investment required to meet the optimal combination of risk mitigation and strategic future value.

The two bids have been combined into this single business case which is now requesting a total investment of $235m ($111m capital and $124m operating). This is $155m less than originally indicated ($37m less capital and $118 less operating).

What follows in the section is a discussion of further options for reducing the cost with commensurate reduction in benefits. In options other than the preferred way forward, this typically represents a deferral of essential work that will still need to be done at a future time.

## Options Analysis

This business case has identified the technology components and applications that are most urgently in need of replacement or serious remediation, as they are on the brink of causing serious interruption to key client services. In other words, they cannot wait another year before the problem starts to be addressed.

As stated above, this is merely the start of a multi-year technology modernisation programme, and the Ministry's Technology strategy has identified the proposed Budget 19 items as being strategic enablers for additional downstream investments.

Below are three scenarios that not only consider risk mitigation and enduring value, but also feedback on the GCDO investment principles. Scenario 1 represents the minimum viable case for mitigation of risk for technology systems availability. Scenario 2 includes additional tactical risk mitigation investments, and Scenario 3 is the full Preferred Way Forward.

Note that relative to Scenario 3 (the preferred way forward); Scenarios 1 and 2 do not include a discussion on 'software and security upgrades'. In all three scenarios, the hardware infrastructure move to IaaS/cloud would be funded. This would mean that by removing the need to invest in hardware from the Ministry's existing Technology capital budget, the existing budget of circa $43M per annum would be sufficient to cover the majority of the required 'software and security upgrades' programme.

**Table 6:** Description of scaling scenarios

| Scenario | Description |
|---|---|
| 1 | • Full IdAM replacement<br>• Full Data Warehouse replacement<br>• Full Hardware Infrastructure to IaaS/Cloud<br>• Full legislative changes |
| 2 | Includes initiatives from Scenario 1 plus:<br>• Second preferred digital channels option<br>• Third preferred Hindin option<br>• Second preferred DREW option |
| 3 | Includes initiatives from Scenario 1 plus:<br>• Full preferred DREW Replacement<br>• Full preferred Hindin option<br>• Full preferred Digital option<br>This is the preferred way forward. |

**Table 7:** Summary of scaling scenario costs

| Scenario | Funding Sought ($m) | 2019/20 | 2020/21 | 2021/22 | 2022/23 + outyears | 4 Year Total | Total Savings |
|---|---|---|---|---|---|---|---|
| 1 | Capital | 28.8 | 26.1 | 7.1 | 1.0 | 63.0 | 98.1 |
| | Operational | 6.6 | 16.8 | 24.0 | 26.5 | 74.0 | |
| | **Total** | **35.4** | **42.9** | **31.1** | **27.5** | **137.0** | |
| 2 | Capital | 38.2 | 29.0 | 7.1 | 1.0 | 75.3 | 72.2 |
| | Operational | 8.2 | 20.0 | 28.4 | 30.9 | 87.6 | |
| | **Total** | **46.4** | **49.0** | **35.5** | **31.9** | **162.9** | |
| 3 | Capital | 61.3 | 41.6 | 7.1 | 1.0 | 111.0 | n/a |
| | Operational | 12.1 | 28.5 | 40.5 | 43.0 | 124.1 | |
| | **Total** | **73.4** | **70.1** | **47.6** | **44.0** | **235.1** | |

# Scenario 1

## Description

Not the Ministry's preferred scenario, but nonetheless arrests the spiral into deeper technical debt and associated trend of increasing risk of failure.

Whilst the trend for Technology Systems Availability risk would likely be reset from 'increasing' to 'decreasing' the risk rating would likely remain at 'very high'.

This scenario includes:

- the preferred option for IdAM Replacement (see Economic case)
- the preferred option for Infrastructure move to IaaS / Cloud (see Economic case)
- the preferred option for Data Warehouse replacement (see Economic case)
- the preferred option for Legislative change

It does not include:

- any mitigation of the risks concerning the Hindin platform
- any mitigation of the risks concerning the DREW application
- any mitigation of risk to scaling the digital channel to meet future demand.

## Advantages

The Ministry considers this to be the minimum viable option to (partially) mitigate the risk of system failure and reset the risk trend from increasing to decreasing. It reduces risk to shared services customers MHUD, OT, SIA, and Office of the Children's Commissioner.

It has some advantages for strategic positioning via moving to Cloud, The IdAM platform being a foundation for partner access to MSD systems, and the Data Warehouse Replacement providing a superior foundation for analytics and data services.

It also protects the Ministry from the consequences of unfunded legislative change.

## Disadvantages

Conversely this scenario leaves (MSD only) services on the Hindin and DREW platforms exposed to an increasing risk of failure which would impact the majority of the Ministry's front line staff. The risks associated with DREW and Hindin platforms are isolated to certain (albeit critical) business functions but are unlikely to bring the whole system down. From a strategic perspective, retiring DREW and Hindin would remain 'must do' initiatives in any conceivable Business Operating Model for MSD, and this cost would therefore be deferred until Budget 2020, placing additional size and risk on any the Te Pae Tawhiti predicated technology transformation.

This also leaves the Digital Channel (MyMSD and Apply Online) with the risk that it will be unable to scale up to meet increasing client driven volumes. For now the channel is working satisfactorily, especially with impending implementation of the Availability solution, but the work to re-architect and replace elements of the Digital channel will still need to be done to meet rising volumes and business model changes to meet Mana Manaaki (Te Pae Tawhiti) requirements.

## Residual risks for Scenario 1

### *Hindin*

This scenario does not achieve any reduction in risk around the Hindin platform and therefore the Hindin risk continues to grow.

Creation of a modern, intuitive, intelligent knowledge base is deferred which means that front line staff will continue to get different answers depending on navigation paths, and continue to provide clients with inconsistent advice

Important client and provider processes Review of Decision, Complaints, and Education Provider escalations would continue to be conducted on a disparate non-integrated platform at very high risk of failure.

### *DREW*

The DREW application remains at very high risk of failure and the situation continues to worsen, affecting front line staff in their ability to calculate many benefits amounts.

The current support arrangements are likely to worsen, meaning that if DREW does fail it would be extremely difficult to restore service.

The long term strategic plan to consolidate statutory rules into one source of truth is delayed, meaning that there remain multiple sources for up to an extra 12 months, and delaying downstream initiatives to retire large bespoke backend systems

### *Digital Channel*

The Digital Channel (MyMSD and Apply Online) remains prone to significant throughput (scalability) constraints which would affect availability due to unprecedented load conditions. Given that MyMSD volumes are predicted to grow rapidly this could start happening in the short to medium term.

Part of the work (proposed in Scenario 3) is to remove technical bottlenecks that affect the rate of straight through processing, leading to extra manual effort and staff costs in the Ministry's back office.

### *Note*

Note that relative to Scenario 3 (the preferred way forward); Scenario 1 does not include a discussion on 'software and security upgrades'. In Scenario 1, the hardware infrastructure move to IaaS/cloud would be funded.

This would mean that by removing the need to invest in hardware from the Ministry's existing Technology capital budget, the existing budget of circa $43M per annum would be sufficient to cover the majority of the required 'software and security upgrades' programme.

## Scenario 1 Summary

- Full IdAM replacement
- Full Data Warehouse replacement
- Full Hardware Infrastructure to IaaS/Cloud
- Full legislative changes

| | |
|---|---|
| Capital cost | $63.0m |
| Operating cost | $74.0m |
| **Total 4 year cost** | **$137.0m** |

| | | IdAM Replacement | Data Warehouse Replacement | Infrastructure to IaaS/Public cloud | Legislative Changes |
|---|---|---|---|---|---|
| **GCDO Investment Principles** | | | | | |
| Critical Investments to prevent systems failure | | ✓ | ✓ | ✓ | ✓ |
| Supports Digital Foundations | | ✓ | N/A | ✓ | N/A |
| Not Investing In Legacy Business Models | | ✓ | ✓ | ✓ | N/A |
| Supports Information and Data Services | | N/A | ✓ | N/A | N/A |
| **Risks** | | | | | |
| **Risk of Not Investing** | Business Operations Risk | **Very High** Current IdAM is at extremely high risk of catastrophic failure potentially rendering all MSD services inoperable. | **High** The current Data Warehouse is at a high risk of failure which would impact critical operational functions required by front-line staff. | **Very High** Over 60% of hardware infrastructure is over five years old. integrated nature of MSD systems means that the whole system can be rendered unavailable *for new business* if one component fails | **High** Unfunded legislative changes, typically to statutory rules, leads to difficult manual workarounds and operational instability |
| | Strategic Risk | **High** IdAM is a foundational capability required to enable client and partner identity in the digital ecosystem. | **High** Delay to delivering a modern analytical capability, restricting innovation and evidence-based decision-making, and inhibiting information and insights sharing across government. | **High** Delay to delivering on government Digital Foundations | **High** Time expedient tactical solutions that lead to increased technical debt |
| **Risk of Investing** *E.g. Stranded asset or opportunity cost of better investment* | | **Low** Industry standard and cloud based components to be used, increasing interoperability and creating a foundation for partners and other agencies to use based on MSD's API strategy | **Low** Ministry procurement processes will manage the risk of selecting the preferred technology platform. Will ensure solution is cloud hosted, flexible, and future-proof. | **Very Low** IaaS/Cloud target environment is part of government digital strategy | **Very low** Change is mandated by legislation |

| | IdAM Replacement | Data Warehouse Replacement | Infrastructure to IaaS/Public cloud | Legislative Changes |
|---|---|---|---|---|
| **GCDO Investment Principles** | | | | |
| **Delivery Risk** | **Low - Medium**<br>Initiative to be 'chunked up' using scaled agile and DevOps delivery methods Some complexity arises from transition states as current IdAM components are progressively de-commissioned | **Medium**<br>Initiative to be 'chunked up' using scaled agile and DevOps delivery methods. Complexity arises from migration approach and challenge of new technology and capabilities. | **Low**<br>Initiative to be 'chunked up' using scaled agile and DevOps delivery methods | **Low**<br>Initiative to be chunked up' using scaled agile and DevOps delivery methods |

# Scenario 2

## Description

This is not the Ministry's preferred scenario. It is the same as Scenario 1 in that it arrests the spiral of technical debt and associated risk of service failure. It would change the trend of the Technology Systems Availability risk from 'increasing' to 'decreasing'.

The rating of the Technology Systems Availability risk would likely be reset to High from Very High
The difference from Scenario 1 is that there are short term (throw-away) and a partial risk mitigants concerning the Hindin and DREW platforms, and a partial implementation of the Digital Channel re-architecting.

Scenario 2 includes:

- All of Scenario 1 initiatives
- Option 3 from Digital channels case which excludes removing bottlenecks to Straight Through processing. (See Economic case)
- Option 3 from Hindin replacement case which only moves knowledge bases to Confluence, but leaves Review of Decision, Complaints, and Education Provider escalations in Hindin (See Economic Case).
- Option 2 from DREW replacement case which mitigates the support/supplier risk by bringing support in house (See Economic Case).

Scenario 2 does not include:

- Full retirement of DREW
- Full retirement of Hindin
- Full scalability of Digital channel, including removing bottlenecks in Straight Through Processing.

## Advantages

The Ministry considers this to a somewhat better scenario compared to Scenario 1 in that it mitigates operational risk to a greater degree.

As with Scenario 1 it partially mitigates the risk of system failure and reset the risk trend from increasing to decreasing.

As with Scenario 1, it reduces risk to shared services customers MHUD, OT, SIA, and Office of the Children's Commission.

It has the same Strategic advantages as Scenario 1. These strategic advantages arise from via moving to Cloud; the IdAM platform being a foundation for downstream partner access to MSD systems, and the Data Warehouse Replacement providing a superior foundation for analytics and data services; and protecting the Ministry from the consequences of unfunded legislative change.

It has additional risk mitigation advantage compared to Scenario 1 in that it reduces the size of the risk in relation to Hindin, DREW, and the Digital Channel

## Disadvantages

Conversely this scenario only reduces operational risk arising from Hindin, DREW, and the Digital channel. Significant risk would remain.

The tactical solutions for Hindin and DREW would have to be considered 'throwaway'.

From a strategic perspective, retiring DREW and Hindin and full re-architecting work for the Digital Channel would remain 'must do' initiatives in any conceivable Business Operating model for MSD, and this cost would therefore be deferred until Budget 2020, placing additional size and risk on any Te Pae Tawhiti predicated technology transformation.

## Residual Risk

### *Hindin*

This scenario does advance the work to get off the Hindin Platform by moving the knowledge bases to a supported platform so reduces operational risk more quickly.

However, as with Scenario 1:

- Creation of a modern, intuitive, intelligent knowledge base is deferred which means that front line staff will continue to get different answers depending on navigation paths, and continue to provide clients with inconsistent advice
- Important client and provider processes Review of Decision, Complaints, and Education Provider escalations would continue to be conducted on a disparate non-integrated platform at high risk of failure.

### *DREW*

This scenario reduces the severity and therefore the overall risk profile of the DREW application by proving more assurance that it can be recovered in the event of failure.

However, as with Scenario 1, the long term strategic plan to consolidate statutory rules into one source of truth is delayed, meaning that there remain multiple sources for up to an extra 12 months, and also delays downstream initiatives to retire large bespoke backend systems such as SWIFTT and TRACE

### *Digital Channels*

While this scenario includes the set of technical scalability improvements that would improve the theoretical throughput of the digital platform and effectively buy some time before the straight through processing improvements were commissioned.

However, deferring the work to resolve key bottlenecks in the straight-through-processing architecture means that under unprecedented load condition staffs in back office teams would be insufficient to deal with the volumes.

### *Note*

Note that relative to Scenario 3 (the preferred way forward); Scenario 2 does not include a discussion on 'software and security upgrades'. In Scenario 2, the hardware infrastructure move to IaaS/cloud would be funded. This would mean that by removing the need to invest in hardware from the Ministry's existing Technology capital budget, the existing budget of circa $43M per annum would be sufficient to cover the majority of the required 'software and security upgrades' programme.

## Scenario 2 Summary

Includes initiatives from Scenario 1 plus:

- Second preferred digital channels option
- Third preferred Hindin option
- Second preferred DREW option

| | |
|---|---|
| Capital cost | $75.3m |
| Operating cost | $87.6m |
| **Total 4 year cost** | **$162.9m** |

| | | **Digital Capability - Option 3**<br>*Digitals Channels only, no Straight-through Processing* | **Hindin Replacement - Option 3**<br>*Defer Cúram move until Budget 2020* | **DREW Replacement - Option 2**<br>*Defer Cúram move until Budget 2020* |
|---|---|---|---|---|
| **GCDO Investment Principles** | | | | |
| Critical Investments to prevent systems failure | | ✓<br>Does not complete risk mitigation Does not address straight through processing. | ✓<br>Retires risk for knowledge bases but not for Review of Decision and Client Complaints. | ✓<br>Impact of failure is only reduced not mitigated. |
| Supports Digital Foundations | | N/A | N/A | N/A |
| Not Investing In Legacy Business Models | | ✓ | ✓<br>Does not support MSD strategy of moving away from bespoke systems. | ✓<br>Ministry staff on much better supported platform but still very old legacy. |
| Supports Information and Data Services | | N/A | N/A | N/A |
| **Risks** | | | | |
| **Risk of Not Investing** | Business Operations Risk | High<br>Current digital architecture and straight through processing architecture is at high risk of failing to scale to future client online demand. This would cause client online self-service to become unavailable and result in unmanageable levels of online application related tasks for staff. | High<br>Current Hindin platform is at high risk of failure in which the staff knowledge base and critical business operational processes that operate on it would be unavailable for a period of days or weeks. | High<br>DREW is at high risk of failure due to key support and aging technology risks key availability, processing integrity, and support risks associated with the application |
| | Strategic Risk | High<br>Delay to maintaining fit for purpose digital foundations to provide clients with online self-service capability. | High<br>Would delay hosting knowledge management on a platform capable of scaling to clients and partners in the digital ecosystem in the future. Would delay the rationalisation of client management and partner engagement functions to the Ministry's strategic platforms. | High<br>Would delay strategic consolidation of Ministry statutory rules to the Ministry's strategic platforms. |
| **Risk of Investing**<br>*E.g. Stranded asset or opportunity cost of better investment* | | Medium - High<br>Changes to existing digital channels which are strategic to MSD's digital capability. They will modernise MyMSD to become cloud hosted and leveraging APIs connected to core system. Straight through processing will remain at high risk of failure. | High<br>Critical business processes remain on high risk Hindin platform. | Low<br>Will remove critical vendor dependency but technology asset profile remains unchanged. |
| **Delivery Risk** | | Low<br>Initiative to be 'chunked up' using scaled agile and DevOps delivery methods. Risks will be managed by project management and test management practices. | Low<br>Initiative to be 'chunked up' using scaled agile and DevOps delivery methods. Some complexity arises from data migration. | Low<br>Initiative to be 'chunked up' using scaled agile and DevOps delivery methods. Low complexity due to no technology migration taking place. |

## **Scenario 3** - *The preferred way forward*

### Description

This is the Ministry's preferred scenario.

This is the same as Scenario 1, except that it adds the full preferred solutions for DREW, Hindin, Digital Platform, and Software and Security.

This scenario would arrest the slide into technical debt and associated risk to systems availability. It would turn the trend of Technology Systems Availability risk to 'decreasing' from 'increasing'.

This scenario would likely turn the risk to Technology Systems Availability from 'very high' to 'high'.

This scenario would have the optimal balance between risk mitigation and executing the minimum set of strategic, foundational and pre-requisite initiatives to support downstream Te Pae Tawhiti strategy execution.

Scenario 3 includes:

- All of Scenario 1 initiatives
- The full preferred option for Hindin retirement (See Economic Case)
- The full Preferred option for DREW retirement (See Economic Case)
- The Full preferred option for scaling the Digital Channel (See economic case)
- The Full preferred option for Software and Security upgrades.

### Advantages

- Optimum investment value arising from mitigating operational risk and creating enduring strategic value.

### Disadvantages

- Only partially reduces Technology Systems Availability risk due to large remaining legacy of bespoke systems at the Ministry.

### Note

This business case, even with the preferred way forward, does not fully bring the Technology Systems Availability risk to a state of equilibrium. This is because investing in additional large scale legacy retirement is not appropriate at this time, given that the Ministry is in the process of taking the Te Pae Tawhiti business strategy down to a more granular level. The Ministry is only proposing investment in areas where there is little or no risk of creating stranded assets. A potential Te Pae Tawhiti business case, where the target business model is agreed, is likely to be presented for consideration in budget 2020; and this would also complete the stabilisation of the Ministry's Technology systems.

## Scenario 3 Summary

Includes initiatives from Scenario 1 plus:

- Full preferred DREW Replacement
- Full preferred Hindin option
- Full preferred Digital option

| | |
|---|---|
| Capital cost | $111.0m |
| Operating cost | $124.1m |
| **Total 4 year cost** | **$235.1m** |

| | | DREW Replacement - Option 4.1 *(Preferred)* | Hindin Replacement - Option 1 *(Preferred)* | Digital Capability - Option 4 *(Preferred)* |
|---|---|---|---|---|
| **GCDO Investment Principles** | | | | |
| Critical Investments to prevent systems failure | | ✓ | ✓ | ✓ Impact of failure is only reduced not mitigated. |
| Supports Digital Foundations | | ✓ | ✓ | N/A |
| Not Investing In Legacy Business Models | | ✓ Leverages API strategy to expose Know-ledge Content | ✓ | ✓ Ministry staff on much better supported platform but still very old legacy. |
| Supports Information and Data Services | | N/A | N/A | N/A |
| **Risks** | | | | |
| **Risk of Not Investing** | Business Operations Risk | **High** DREW is at high risk of failure due to key support and aging technology risks, key availability, processing integrity, and support risks associated with the application | **High** Current Hindin platform is at high risk of failure, in which the staff knowledge base and critical business operational processes that operate on the system would be unavailable for a period of days or weeks. | **High** Current digital architecture and straight through processing architecture is at high risk of failing to scale to future client online demand. This would cause client online self-service to become unavailable and result in unmanageable levels of online application related tasks for staff. |
| | Strategic Risk | **High** Would delay strategic consolidation of Ministry statutory rules to the Ministry's strategic platform. | **High** Hindin replacement will enable knowledge management to be expanded to clients and partners in the digital ecosystem in the future. It will also support the rationalisation of client management and partner engagement function to the Ministry's strategic platforms. | **High** Delay to maintaining fit for purpose digital foundations to provide clients with online self-service capability. |
| **Risk of Investing** *E.g. Stranded asset or opportunity cost of better investment* | | **Low** Migrating rules to known strategic platform. Functions will be assessed to determine whether Cúram SPM remains the best-fit Ministry platform to host these. Execute in parallel to MSD API strategy to expose these authoritative rules to other agencies. | **Low** Changes to existing digital channels and straight through processing, which are strategic to MSD's digital capability. This will modernise MyMSD to become cloud hosted leveraging APIs. | **Low** Ministry procurement will manage the risk of selecting the preferred technology platform to replace Hindin for Knowledge Management. Rationalisation of functions will be to known and preferred strategic Cúram SPM platform. |

| | DREW Replacement - Option 4.1 *(Preferred)* | Hindin Replacement - Option 1 *(Preferred)* | Digital Capability - Option 4 *(Preferred)* |
|---|---|---|---|
| **GCDO Investment Principles** | | | |
| **Delivery Risk** | **Medium - High**<br>Initiative to be 'chunked up' using scaled agile and DevOps delivery methods. Reasonable complexity of business rules and functions to be migrated. | **Medium**<br>Initiative to be 'chunked up' using scaled agile and DevOps delivery methods. High complexity arises during optimisation of straight through processing. Risks will be managed by project and test management practices. | **Medium**<br>Initiative to be 'chunked up' using scaled agile and DevOps delivery methods. Some complexity arises from data migration and integration of new cloud SaaS platform with MSD core systems. |

# Commercial Case

The commercial model for delivery is different for each of the eight projects. They vary from market approach and a partner vendor for implementation (IdAM), to focused delivery teams of in-house resource using existing commercial arrangements and All-of-Government services (Infrastructure).

There are some principles that apply to how, in general, the sub-projects will be approached. These are concerned with reducing the delivery risk by addressing the highest risk areas as early in the programme/project lifecycle as possible to gain delivery certainty.

The Ministry has two key principles which are used to validate the target solution as quickly as possible. The first involves performing Proofs of Concept early in the life-cycle. Doing this early formally validate 'fit' with the business environment/requirements, and a technical Proof of Concept (PoC) to validates that the proposed solution will actually work in the Ministry's environment. The technical PoC also serves to allow the eventual users of the system to visualise how it will work early in the process.

The second key principle is that the first deployment to 'production' is a Minimum Viable Product so that subsequent iterations of development are commissioned In the light of direct end user feedback. This means that the risk of investing in low value features is greatly reduced and greatest value is extracted.

## Commercial Approach

MSD recognises there is a need for significant capability to support the delivery of the Programme, to reduce risk through technical expertise and delivery experience, and improve the quality of the outcomes delivered.

This programme is reliant on its strategic partners, to support the delivery of this programme. Our engagement approach with our partners is to operate under a Master Services Agreement (MSA) using a Statement of Work (SOW) arrangement. The MSA does not limit the commercial arrangements for each SOW, meaning that a variety of risk sharing and commercial mechanisms can be adopted.

Moving into the future delivery phase, MSD will adopt a Statement of Work-based commercial framework, based on a Time and Material approach. Fixed price segments can be accommodated within SOWs where the scope and deliverables are clear and where commercial mechanisms allow. However, the programme has elected not to use a fixed price arrangement, to allow flexibility for a collaborative, agile approach that utilises a range of vendor resources to deliver product-led, but MSD-specific, configuration and features.

During delivery MSD will employ a number of commercial levers with vendors and these include; retention sums, liquidated damages, warranty provisions, disengagement and termination clauses which allow MSD to minimise risk and ensure that vendors have proven the configuration in an MSD environment prior to release of any retention sums. Such provisions are designed to ensure vendors are focused on the delivery of functionality into the MSD environment. The disengagement and termination clauses allow MSD to minimise future costs if changes to the programme happen, whilst allowing MSD to retain the deliverables.

The detailed commercial cases are included in each of the sub business cases.

# Financial Case

**Table 8:** Summary of the funding required to support the business case

| Funding Sought ($m) | 2019/20 | 2020/21 | 2021/22 | 2022/23 & outyears | TOTAL |
|---|---|---|---|---|---|
| Operating | 12.070 | 28.483 | 40.514 | 43.020 | **124.086** |

| Funding Sought ($m) | 2019/20 | 2022/23 | 2023/24 | 2024/25 | 2025/26 | 2026/27 | TOTAL |
|---|---|---|---|---|---|---|---|
| Capital | 61.662 | 41.400 | 7.100 | 1.000 | - | - | **111.162** |

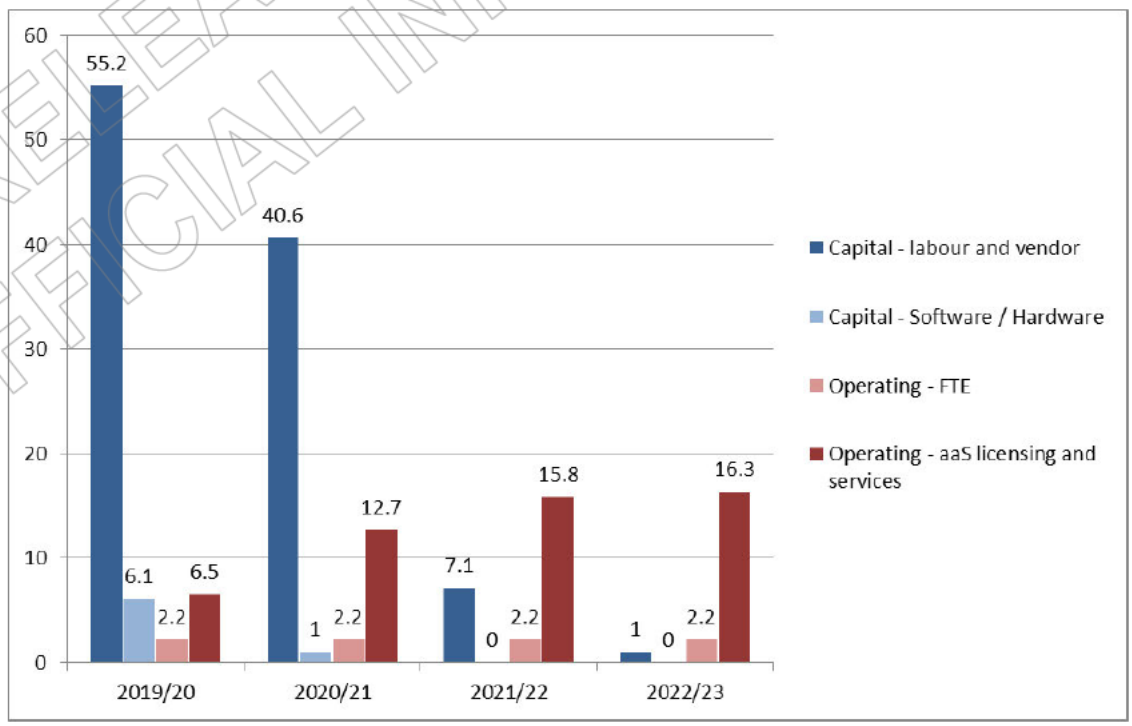
The estimates are based on the 'likely' case estimates of the preferred way forward. The breakdown of funding for each of the projects for their preferred case is shown in the section The Financial Case.

The more detailed cost breakdown of each project's preferred and alternative options are described in each of the sub business cases, and further supporting material in the appendices.

The funding addresses the creation of new software assets, based on cloud services, and the transition to as-a-Service services. For the replacement projects, all assets are end of life and are not invested in further.

The estimation process used a combination of internal and external assessments. In particular, the IdAM implementation and licensing costs (PwC) and the Data Warehouse Re-platform implementation and transition costs (Accenture) were independently sourced. The estimates for DREW, Hindin and the Digital channels came from the experience of the teams that have worked with these systems for many years, and have a history of estimation and delivery.

The majority of the capital required supports capitalised MSD or vendor labour in creating the new assets. The breakdown is shown below.



The estimates were assessed using a Quantitative Risk Assessment. For the purpose of this business case an 85% confidence level[10] has been used. This means that there is an 85% chance that the actual cost of the programme will not exceed the estimated cost plus the contingency. The analysis shows that the contingency required to meet the 85% confidence target is $27.0M, or 15% of the total estimated costs.

# Management Case

The management case addresses the achievability of the proposal and planning arrangements required to both ensure successful delivery and to manage programme risks.

The key governance objective is to ensure transparency for all the key stakeholders. This includes Treasury and GCDO, as well as key partner agencies, Oranga Tamariki and Housing and Urban Development.

The programme structure is based on the existing portfolio management model used in MSD. The Portfolio Executive Committee (PEC) will oversee this programme and the overall investment portfolio. This will enable prioritisation across the full investment portfolio, and ensure visibility of the programme. The PEC reports to the Investment Strategy Governance Committee (ISGC).

These governance processes have recently been put in place, and have improved the prioritisation and allocation of funding. A summary of the governance process is included in the appendices.

The details of the proposed governance structures are shown in the section Management Case.

### Implementation Completed in 2023

Earlier analysis work has significantly improved our understanding of the complexities of the current infrastructure service and this has helped us to understand the delivery risks. Large projects, such as Novopay and Police HRIS, serve as an insight to issues of system complexity as one of the common drivers of scope, cost and schedule overruns in large-scale technology programmes.

In developing the implementation roadmap for the Programme, consideration was given to what was an optimal return on investment against an acceptable level of delivery and operational risk. This consideration together with the degree of change the organisation could absorb was balanced with the need to maintain current operational performance throughout the change. As a result, this programme is planned for an implementation period of four years.

It is proposed that the Programme will be implemented in three tranches. Tranche One will be completed by FY2020 and Tranche two by FY2021 with the final, Tranche Three delivered in FY2023.



[10] The 85% confidence level matches one standard deviation from the mean for a normally distributed cost profile.

### *Tranche One*

This tranche will:

- Select the strategic partner and solution for IdAM
- Migrate most business rules from DREW and validate the preferred platform
- Select the preferred knowledge platform, and migrate 25% of the Hindin content
- Migrate and decommission the Complaints function of Hindin
- Select the strategic partner and solution for the Data Warehouse
- Decommission the EOS instance of the Cúram to simplify client experience
- Deliver the new Cúram client channel experience, and complete development of the MyMSD component
- Migrate and decommission half of the obsolete hardware and out of support software, and
- Complete the plans and estimates for Tranche Two.

### *Tranche Two*

This tranche will:

- Deliver Client identity on the new IdAM platform
- Deliver the new Review of Decision, Provider Management systems, and all the Hindin content on the new knowledge platform
- Retire DREW and Hindin
- Deliver the Warehouse MVP and the highest priority information products
- Deliver a more scalable MyMSD client channel, and deliver straight through processing optimisations to reduce the rate of exceptions for staff
- Complete the upgrade of software to supported levels, allowing 75% of compute capacity to be delivered from IaaS
- Complete the plans and estimates for Tranche 3

### *Tranche Three*

This tranche will:

- Deliver Staff identity on the new IdAM platform
- Deliver the required set of information products on the new Warehouse platform
- Retire the old IdAM solution set
- Retire the old Warehouse

The technology solutions to support this implementation roadmap will:

- Remove the operation risks commencing with the highest risks
- Reduce implementation risk by selecting strategic partners where possible
- Reduce implementation and privacy risk by limiting data conversion and manipulation to only those instances where the outcomes require it.

MSD is ready to commence the Inception Phase of the Programme. This will involve detailed design of the future business processes, roles and information flows, and implementation of new technology.

## Dependency management

The proposed projects have multiple dependencies between each other and with other projects and programmes undertaken independent of the business case. These dependencies include both technical (one system depends on another) and resource based (specialists may be needed by multiple streams).

MSD has a strong history of managing large programmes of work incorporating many systems and multiple workstreams. MSD manages programmes of work using the Scaled Agile framework (SAFe). A core practice of SAFe is Programme Increment (PI) Planning. During PI planning dependencies are identified and communicated. Conflicts are escalated to the management team to resolve using prioritisation or scope management.

The broader project governance structures include Programme Boards and the Portfolio Executive Committee (PEC). Dependencies across the programmes are monitored and reported to the PEC. Refer to the appendices for a more detailed description of the various programme governance bodies. Refer to the Management Case section for a description of the relationship between Programme Boards and PEC.

## Implementation Risk

Considerable effort has gone into assessing options that are able to be executed by the Ministry and industry partners.

The Treasury Risk Profile Assessment rates the programme at High, with the three sections assessments being Low, High, and Low. The programme approach is to address the significant risks identified early to improve the certainty of outcome. The implementation risk for each project is described in each sub case.

The feasibility of implementation has also been assessed. The details are contained in the Management Case.

# The Economic Case

*Exploring the Preferred Way Forward*

## Critical Success Factors

The following critical success factors were identified by stakeholders in conjunction with the Investment Objectives (in the Strategic Case), and reflect those objectives

**Table 9:** Critical Success Factors

| Generic Critical Success Factors | Broad Description | Proposal-Specific Critical Success Factors |
|---|---|---|
| **Strategic fit and business needs** | How well the option meets the agreed investment objectives, related business needs and service requirements, and integrates with other strategies, programmes and projects. | Contribution to the reduction of risk<br>Enduring value of the solution, measured by its alignment to the Technology Strategy |
| **Potential value for money** | How well the option optimises value for money (i.e., the optimal mix of potential benefits, costs and risks). | Use of Agile and PI planning to deliver Minimum Viable Products meeting the Investment Objectives. |
| **Supplier capacity and capability** | How well the option matches the ability of potential suppliers to deliver the required services, and is likely to result in a sustainable arrangement that optimises value for money. | Establish long term partnerships for new capabilities required by the Ministry. |
| **Potential affordability** | How well the option can be met from likely available funding, and matches other funding constraints. | Meet risk reduction targets within available funding. |
| **Potential achievability** | How well the option is likely to be delivered given the organisations ability to respond to the changes required, and matches the level of available skills required for successful delivery. | Inclusion of this programme into the Workforce Planning process. |



## Programme Options

This section includes the eight projects identified. Each is described as self-contained sub business cases. Because the case for change and the solutions are different in each case, elements of the Economic Case are included individually in each sub case. Specifically, the sections are:

- Case for Change
- Risks and Benefits
- Options Considered
- Commercial Case
- Financial Case

These sub-business cases cover the preferred and alternative options.

# 1. Identity and Access Management Replacement

## 1.1 The Case for Replacing our Identity and Access Management Platform

An Identity and Access Management (IdAM) platform is an essential part of any large business. The absence of an IdAM platform would mean that there would be unfettered access to computer systems, including private and sensitive data. For example, anybody with physical access to a Ministry computer could go into any system and view any data or make any changes they wished, ranging from client data to salary details.

MSD's current Identity and Access Management (IdAM) platform poses a serious risk to the Ministry. This platform authorises staff access to all of the Ministry's computer systems, data and information. If IdAM were to fail no staff member would be able to logon to any system; and no clients would be able to access digital systems. In essence the Ministry would not be able to process a single client transaction if IdAM failed.

The Ministry has made a number of attempts to remediate risk around the IdAM platform, but these projects have been under-estimated and not been allocated sufficient internal capital to make a material difference to the risk profile. These projects have, however, created a foundation for future efforts to replace IdAM. A team has been working for two years to define and agree the future state IdAM architecture and business governance model.

Within the limits of the internal budget, a target identity store has been established and work is underway to move applications to it. However, this is but one component of what is an extremely complex and multi-layered Identity system and at the current rate of investment it will take well over 5 years to finish the task.

In the meantime, the other components of the identity ecosystem are running on dated, tightly coupled platforms that have been underinvested in for over a decade. This means that they are difficult to change and keep up-to-date for the staff identities that they hold. For example, some of the underlying servers are 14 years old, and these cannot be upgraded to modern servers because the applications operate on obsolete operating systems and middleware that can only run on old hardware.

The platform also includes significant bespoke sub-applications such as AUM and CYFHub that are poorly understood and need to be replaced with standard 3rd party software.

Manual intervention and workarounds are now required to keep the platform running, creating significant risk of data breach or unauthorised access. Further on-boarding and off boarding new staff is so problematic that there is a high possibility of staff still having access to systems after they have left.

We have a very large external data store hardwired into MyMSD that was not initially designed to handle this number of users and transactions when it was built as part of the MSD Simplification programme. With the predicted uptake and transaction volume of this platform – this store needs to be re-platformed to a larger enterprise platform that will handle this load. Not replatforming significantly risks the continued service of our MyMSD online channel that now has over 650,000 beneficiary identities registered in it.

The Ministry's Technology Strategy has identified the future IdAM as being a strategic asset that underpins safe and easy access for staff, partners, and clients. This investment will ensure that the future asset is future proofed and able to accommodate future operating models.

## 1.2 Background

The Ministry's Identity and Access management capability is made up of a number of identity applications that together provide the means by which our staff access our applications and information. It is also how over 650,000 beneficiaries access their information through the MyMSD application, as well as how other cohorts of beneficiaries such as students use the Ministries online applications. These repositories of clients are growing at 1000 new clients per week – and now include over half our active clients.

The current Ministry identity capability has evolved over time and has been in existence for approximately 15 years. It is predominantly a bespoke solution and has been incrementally developed to meet changing business structures and needs since its inception.

Although the technology continues to function and support the basic needs of the business, it now does not have the ability to adapt to become a modern IdAM platform to support the increased desire for cloud based services, modern cyber security threat protection, seamless authentication capabilities, and improved process efficiency, This is because over the many years of development and enhancement, the existing Identity Management platform lost its foundational architecture. Many dependencies now exist with multiple peripheral systems and workarounds employed to manage capability deficiencies. This has resulted in an ever growing amount of technical debt and a high level of risk with running and managing the platform.

A number of attempts have been made to refactor parts of the existing identity management platform and modernise its capabilities. This has proved to be challenging, complex, and aspects of existing functionality have been replicated with no real overall benefit. These initiatives had significant financial investment but lacked business engagement and involvement, which may have contributed to the difficulties in achieving the targeted objectives.

At the technology layer, the existing Identity Management platform consists of a number of disparate applications, many of which are reliant on legacy, unsupported hardware and software and/or use software not designed for access management functions (e.g. payroll). This has made the overall platform very complex and difficult to maintain.

Various workarounds have been implemented to compensate for this cumbersome nature, and some security controls have not been fully utilised in an attempt to maintain stability of the system and interconnected components. This creates an ever present risk to MSD (and its shared services customers) of a major outage that affects not only the Identity Management processes but also the Corporate Identity Directory (LDAP) which could result in many of MSD's critical business applications being unavailable.

Adding to this complexity are manual business processes for on-boarding and off-boarding users, modifying access rights and terminating employment, which are also highly complex. Inconsistencies in these processes combined with delays caused by sequential batch driven processes, coupled with the lack of automated de-provisioning from applications (particularly cloud applications where user credentials are held in the application itself), present a high security risk of unauthorised access.

The age and lack of functionality in some of the existing Identity Management components limits MSD's ability to take advantage of newer technology which could reduce this risk. Consequently there is no central capability to manage identities or record what entitlements have been assigned to a worker. Instead, a disparate set of processes and record keeping exists that result in inefficiencies, accumulation of access rights and an inability to audit access rights across the organisation.

There are three main themes to the IDAM problem in the Ministry.

They are:

1. We require urgent remediation to keep this IDAM platform running for our key applications – They are running on dated, tightly coupled platforms that have been underinvested in for over a decade. This means that they are difficult to change and keep up-to-date for the staff identities that they hold.
2. There is so much manual intervention and workarounds are now employed to keep the platform running that there is significant risk of data breach or unauthorised access. Further on-boarding and off-boarding new staff is so problematic that there is a high possibility of staff still having access to systems after they have left or staff having access to resources they are not supposed to have access to.
3. We have a very large external data store with over 650,000 beneficiaries hardwired into MyMSD that was not initially designed to handle this number of users and transactions when it was built as part of the MSD simplification programme. With the predicted uptake and transaction volume of this platform – this store needs to be re-platformed to a larger enterprise platform that will handle this load and the number of users we now have. Not re-platforming significantly risks the continued service of our MyMSD online channel.

NOTE: The re-platforming in point 3 also makes this client identity store reusable for future online Ministry applications.

NOTE: The recommended options in this paper are also highly aligned to Te Pai Tawhiti – and all of the initiatives and work outlined here is reusable for the 2020 business case

## 1.3 Risks and Benefits

There are key themes running through the problems outlined in the above problem statement that present themselves as risk – as well as the opportunity to provide benefits to the Ministry.

The risks include:

- **Unauthorised access** – increases MSDs exposure to risks of privacy breaches, security breaches and internal fraud. Unauthorised access is the result of not removing access to applications and systems when people leave the organisation or move to a different role.
- **No view of user access** – it is currently virtually impossible to answer the question 'who has access to what?' in a reasonable timeframe today. MSD cannot protect its data if it does not know who has access to it.
- **Lack of security for user credentials** – by requiring users to maintain multiple passwords and by storing username and password in cloud applications user credentials are vulnerable to theft and misuse.
- **Failure of an IdAM component** – reliance on unsupported and legacy hardware and software make MSD vulnerable to a failure of a critical component which could affect access to critical business applications. Further, because of the tightly coupled nature of our identity stack, upstream failure of an identity system has 'flow on' downstream effects to our lower level identity provisioning systems.
- **Tight linkage to business process and criticality of applications** – Delivering MSDs services is becoming more reliant on technology and failure of IDAM services completely brings many of our critical platforms out of service.
- **Lack of reusable client and partner identity** capability that is simple to use and provides the strength of identity we need to offer services to our clients.
- **Identity will be at the forefront of the new security architecture** the Ministry will deploy that will allow staff to work from anywhere, anytime, on any device. The fundamental requirement for this strategy is that we have a high degree of confidence in the strength of our digital identity for staff. This work is also a fundamental prerequisite for this next phase of security work to continue.

The Benefits include:

- **Reduce the risk of unsupported critical identity infrastructure failure** through upgrading it or migrating it to a supported system.
- **Reduce the risk of inappropriate data access** through more secure authentication mechanisms.
- **Reduce the risk of passwords being compromised** by reducing the number of passwords and enforcing a consistent password standard across all our access systems.
- **Workflow enabled compliance and audit functions** for provisioning and application access that only gives the access that each user needs.
- **Consistent role based permissions** to applications and resources for all staff.
- **Single centralised record of assigned user permissions** and a central record of user permissions.
- **Prevent permissions creep** through automated provisioning and de-provisioning of users and access.
- **Better user management** of NGOs, contractors and service providers.
- **Workflow enabled provisioning and de-provisioning** (as opposed to manual currently).
- **Self service capability** for access requests and password resets.
- **Improved management of licencing costs** through accurate reporting on usage.
- **Improved user experience** and ease of use through single sign on.
- **Enable secure access for cloud applications** and platforms.
- **Provide a single view of who has access to which systems.** Currently there is none and this poses a high level of risk to the Ministry in operating these systems.
- **Improve the manual, slow on boarding process** that is prone to error and not auditable other than through time consuming manual means.
- **Lower operational costs** through being able to see who is using which systems – and therefore being able to save considerable licencing costs.
- **Remove the security and operational risk** of a number of identity related systems running on unsupported software.
- **Remove single points of failure** so that if one identity system fails, staff and clients are still able to log in and continue to use our systems.
- **Lower our security vulnerability** through better Identity lifecycle management and the full de-provisioning of users once they leave MSD.

Other objectives not directly related to risk of failure that lay the foundation for future identity capability:

- **Identity will be at the forefront of the new security architecture** the Ministry will deploy allowing staff to work from anywhere, anytime, on any device. The fundamental requirement for this strategy is that we have a high degree of confidence in the strength of our digital identity for staff to access information from anywhere.
- This work on **the external client store paves the way for simple access** to our information and resources where identity 'gets out of the way' so New Zealanders can access the services they need when they need them.

### *Initial risk analysis*

This section outlines the main risks that have been identified for this work stream. They are examined in terms of the seriousness of their consequence as well as their likelihood. Risk management and mitigation strategies are also outlined for each of these risks.

**Table 10:** Initial Risk

| Main Risks | Consequence (H/M/L) | Likelihood (H/M/L) | Comments and Risk Management Strategies |
|---|---|---|---|
| The risk that the organisation cannot meet its business imperatives. | H | H | IDAM platforms like AUM and Sun Systems (iPlanet - Directory Server) continues to be utilised despite being unsupported for a large number of applications, exposing the Ministry to risk of a large scale failure. |
| The risk that there will be an undermining of customer's/media's perception of the organisation's ability to fulfil its business requirements – for example, adverse publicity concerning an operational problem. | H | M | Risk of costs as a result of fraud, data leaks or privacy breaches - estimated costs of each incident. |
| The risk that design cannot deliver the services to the required quality standards. | H | M | Modern IdAM approaches/ methodologies/ solution options is a relatively emerging field and there is a risk the design of the IdAM solution will not meet the specific needs of MSD and additional design effort is required. |
| The risk that the construction of physical and/or virtual assets is not completed on time, to budget and to specification | H | M | The bespoke component of the IGA development for Option 2 is unknown. This in-turn could alter the high-level estimates provided to date and or deliver a product that does not meet the needs as desired requiring some re-work. |
| The risk that the quality of initial intelligence (for example, preliminary site investigation) will impact on the likelihood of unforeseen problems occurring. | M | L | An implementation of this kind will require specialist expertise (both internal and external) and retaining this expertise and/or having to replace key resources during delivery does pose some risk to the project. |
| The risk that can arise from the contractual arrangements between two parties – for example, the capabilities of the contractor/ when a dispute occurs. | L | M | Modern IdAM delivery may require multiple partners/vendors and associated agreements. There is potential with this project that there may be procurement issues. |
| The risk that operating costs vary from budget and that performance standards slip or that a service cannot be provided. | M | L | Risk that MSD is paying for licenses (annually) that are not required due to users identity access rights not being updated or removed when changes are made. |
| The risk that operating costs vary from budget and that performance standards slip or that a service cannot be provided | M | L | Risk of fraud or privacy breach incident as a result of unauthorised access occurring every year. |

| | | | |
|---|---|---|---|
| The risk that the costs of keeping the assets in good condition vary from budget. | M | M | There is an on-going risk of maintaining knowledgeable staff to support in house built applications. This risk applies to out years 3-5. There is an on-going risk of maintaining knowledgeable staff to support the current platform applications. |

A risk register has been developed and will be progressively updated as more detailed analysis is undertaken.

### *Risks from Change*

The tables below deal with the risks of the preferred investment option. Specifically it examines the execution risk which looks at risk associated with doing the work, the residual risks that will be leftover once the work is complete – and any introduced risk that would be created as part of doing this work. It also looks at any mitigation that may be implemented to lessen the effect or consequence of any of these risks becoming material issues that require remediation.

**Table 11:** Execution Risk

| Execution risk | Consequence (H/M/L) | Likelihood (H/M/L) | Assessment Rating | Mitigation |
|---|---|---|---|---|
| **Project Complexity** Due to the complexity and many touch points into MSD systems and applications implementing a fit for purpose IdAM solution will take time and will require a high-degree of expertise and knowledge from external parties. | H | M | M | The project proposes to build a partner relationship with a single vendor (service aggregator) who has experience in delivering IdAM solutions. The service component of the procurement will be as important as the technology. |
| **Market Capability** Modern IdAM principles and technologies are not widely established in New Zealand. Sourcing suitably qualified expertise/capability may be difficult. | M | M | M | The project is conducting market research to see what expertise is available both in New Zealand and overseas to assist where needed. |
| **Governance** Ownership and governance with responsibility and accountability is a key component of a successful IdAM solution. Currently MSD does not have appropriate governance arrangement in place which would be suitable for IdAM. | M | M | M | The project will develop a governance model which outlines the key roles and responsibilities which would need to be in place for IdAM to function correctly. |
| **Scope Creep** Scope creep due to the unknown state of the existing platform. | H | M | H | If there are technical issues that manifest in the later stages of the project which require a change of direction or the addition of scope then this would impact the projects baselined scope which would impact project timelines and costs. Management strategy is to ensure detailed and robust analysis and planning is carried |

| | | | | |
|---|---|---|---|---|
| | | | | out with the vendor in the design phase.<br>Use standard MSD project change control processes to manage any exceptions/charges of scope.<br>Use of a project variation register to track and manage all proposed changes of scope.<br>Allow sufficient contingency in schedules and budget to cover any unexpected scope. |
| **Integration Failure**<br>Technology components may fail to integrate with each other. | H | M | M | If there are unexpected issues identified due to the complexity of integration between LDAP and applications then this may require additional effort to analyse, design and implement a resolution. This would add unplanned effort to the project which would in turn impact project timelines and budgets.<br>The management strategy is to ensure comprehensive testing is carried out in pre-production environments before production deployment/cutover.<br>Ensure there is an effective and tested roll-back strategy in place in the event of identifying an issue that cannot be safely resolved during cut-over. IDAM platforms will be selected based on standards based technologies to minimise the chance of this happening<br>Use standard MSD project change control processes to manage any exceptions/charges of scope. |
| **Resource contention / re-prioritisation of work.**<br>If the project is unable to secure the required resources or there is contention for resources with other MSD work then this could cause delays and erode benefits realisation which would impact project timelines and costs. | M | M | M | Make sure resource plans are up to date and accurate and provided to resource managed with sufficient notice.<br>Ensure project resource requirements are clearly flagged at PI Planning. |
| **Financial Contention / re-prioritisation of work**<br>If financial constraints are imposed on the project work streams, then Identity and access management/ security risks may not be addressed which will result in the risk profile of MSD not being addressed. | M | M | M | Should there be financial constraints on the Project, then there will need to be stakeholder engagement to determine a revised scope, which will need to be based on risk mitigation / acceptance. |

| | | | | |
|---|---|---|---|---|
| **Interdependent Workstreams** The success of the IDAM project is a prerequisite for a number of other work streams. This means that IDAM must deliver a certain set of core capabilities for other work streams to be successful in their delivery. | H | H | H | Planning and upfront work will be emphasised to make sure we can deliver to milestones and the needs of the other work streams. |

**Table 12:** Residual Risk

| Residual risk | Consequence (H/M/L) | Likelihood (H/M/L) | Assessment Rating | Mitigation |
|---|---|---|---|---|
| The risk that parts of the existing IDAM project remain and become an impediment to other parts of the programme to slow down. | M | M | M | Plan for any eventuality of this happening and phase the project accordingly so that any parts remaining play a minor role and can more easily be removed in the near future. |
| Legacy platforms are unable to integrate to the new IDAM platforms and vulnerable as a result | L | M | M | Audit and identify these systems early and plan for how they will work in the new system – minimising any vulnerabilities in doing so. |
| The external client store would still have to mature further for it to become a reusable external store for another applications and it may be a bottleneck in the short term. | M | M | M | Build the external client store in a way that allows this functionality to be added to or easily enabled in future releases. |

**Table 13:** Introduced Risk

| Introduced risk | Consequence (H/M/L) | Likelihood (H/M/L) | Assessment Rating | Mitigation |
|---|---|---|---|---|
| Stopping this project before the full capability is delivered. | H | M | M | Because this project is about moving to a new modern IDAM platform, from an old obsolete one, if we stop this project half way through with half the applications and systems modernised and half not – we will have created an even more complicated IDAM system than we do now. Consequently, a number of the risks and benefits would not be mitigated or delivered on. |
| Introducing defects as we build the new system. | H | M | M | Rigorous testing will be conducted through the delivery lifecycle to minimise the chance of this happening. |

| | | | | |
|---|---|---|---|---|
| Running old and new systems concurrently through the migration project. | H | M | M | This will have to happen – however this will be minimised so we can retire technical debt and take advantage of the benefits the modern IDAM systems have to offer. |

## 1.4 Options considered (Economic case)

The options presented for comparison include two distinct and feasible implementation approaches which are options two and three, each with associated costs, benefits, and risks. The Do Nothing (status quo) option has also been included for baseline comparison; making four options in total for consideration.

The options have been assessed against their ability to fulfil key service requirements, investment objectives, critical success factors, and finally an economic assessment is provided to help represent an unbiased view for comparison. The following section highlights the key point for consideration in each of the potential options.

### *1.4.1 List of options considered*

**Table 14:** Description and status of options

| Option | Description | Status |
|---|---|---|
| **Option 1** Status Quo (Do Nothing) | MSD retains the existing identity and access management capability, applications and processes; and accepts the existing (and escalating) costs, technical debt and associated risks of retaining the status quo. | Discounted |
| **Option 2** In-house (Partial Solution) | MSD implements a bespoke (in-house developed) solution that focuses on reducing the risks and costs associated with technical debt. The scope of the solution will meet the key requirements but will not be as fully featured as a COTS IGA and AM solution. | Discounted |
| **Option 3** Full Vendor Managed Solution | MSD goes to market to procure the services and applications required to implement a full IdAM solution, based on COTS products and delivered as a service.<br><br>This option will involve using the expertise of a Service Aggregator and purchasing of fit-for-purpose COTS IdAM solution applications. Providing MSD with modern IdAM capability, reducing risk, eliminating technical debt, and optimising identity access management for future strategic initiatives. | Preferred solution |
| **Option 4** Defer Solution | MSD retains the existing identity and access management capability and defers starting the IdAM work for another year. | Discounted |

### 1.4.2 *Detailed Examination of the IdAM Options*

This section details the main features of each of the four options as well as showing the maturity of each of the capabilities that make up the IdAM platform:

#### *Option 1: Status Quo*

- No change management impact.
- Continuing lack of defined and enforced policy and process.
- Increasing risk profile of the IdAM function.
- Continued reliance on undocumented and unsupported processes and application to perform access provisioning.
- Continued dependency on sequential batch driven integration which enforces tight coupling of applications.
- No improvement to IdAM capability maturity.
- MSD will continue to be constrained in making security and user experience improvements due to the lack of support and flexibility within the current Identity Management solution.
- No external support for MSD's current Identity Management solution, MSD will need to maintain its own expertise in supporting and maintaining this platform which has not only financial implications but resource prioritisation and staff retention implications as well.
- Due to the bespoke nature of the existing Identity Management components it is likely that MSD's capability to support and maintain these will further decline over time.
- No strong control to mitigate security risks relating to unauthorised access, client information privacy or internal fraud.

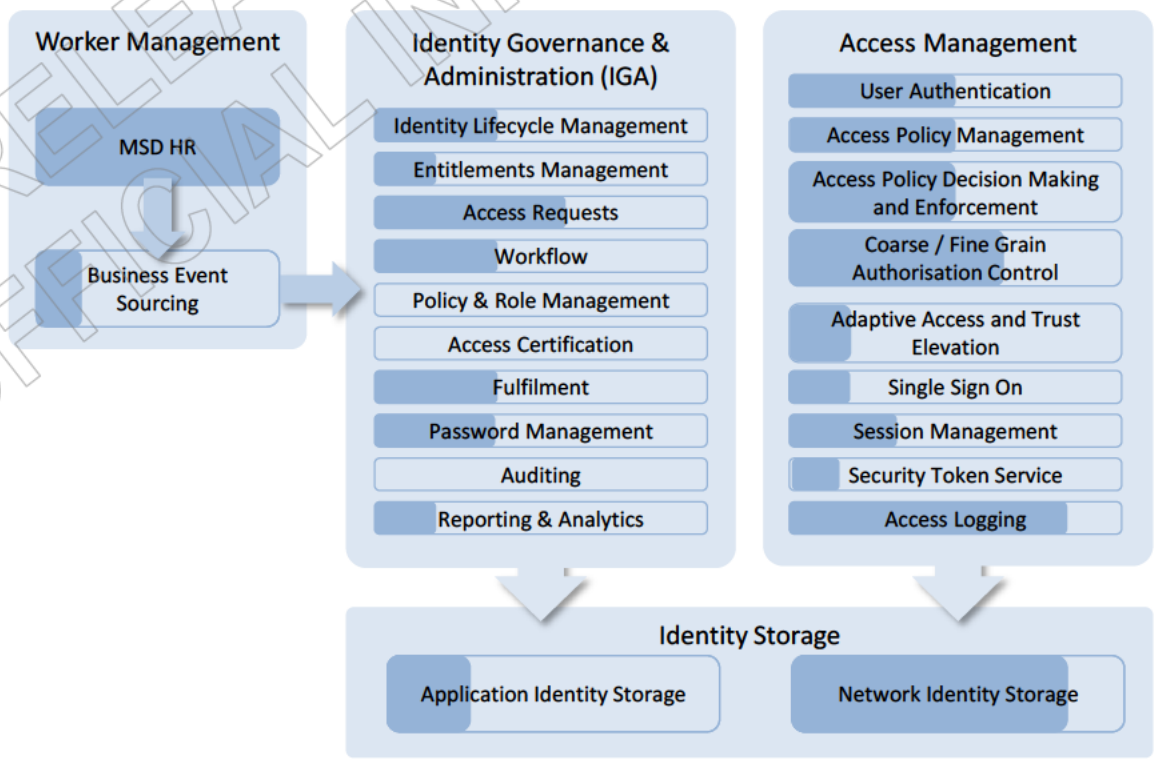



**Figure 1:** Current capability maturity

***Option 2:*** *In House Partial Solution*

- A modern supported identity store with a documented support roadmap will be implemented.
- IGA functionality delivered will be significantly less than a recognised IGA COTS product.
- Not investing in a strategic Access Management (AM) toolset will severely limit MSD's capability to support the strategic objectives of increased mobile device support and digital enablement in a secure way.
- By removing the dependency on CHRIS 21 information for new starters can be sent to IGA earlier in the HR process this will reduce the time new starters have to wait for application access to be established.
- Existing IdAM related applications which expose MSD to risk will be retired and replaced.
- Significant amount of in-house work required to define scope, design, build and test the solution.
- In-house development of an IGA platform carries a high level of risk. Risk of budget overspend, scope blowout and lack of the appropriate skills all need to be considered. MSD has made previous attempts to replace the existing core Identity Management applications with no success.
- No vendor supported roadmap for IGA components to ensure constant platform upgrades and avoid technical debt accumulation.
- MSD will need to maintain in-house skills to support the IdAM platform from both a technical and business perspective.
- Significant Organisational Change Management effort required.

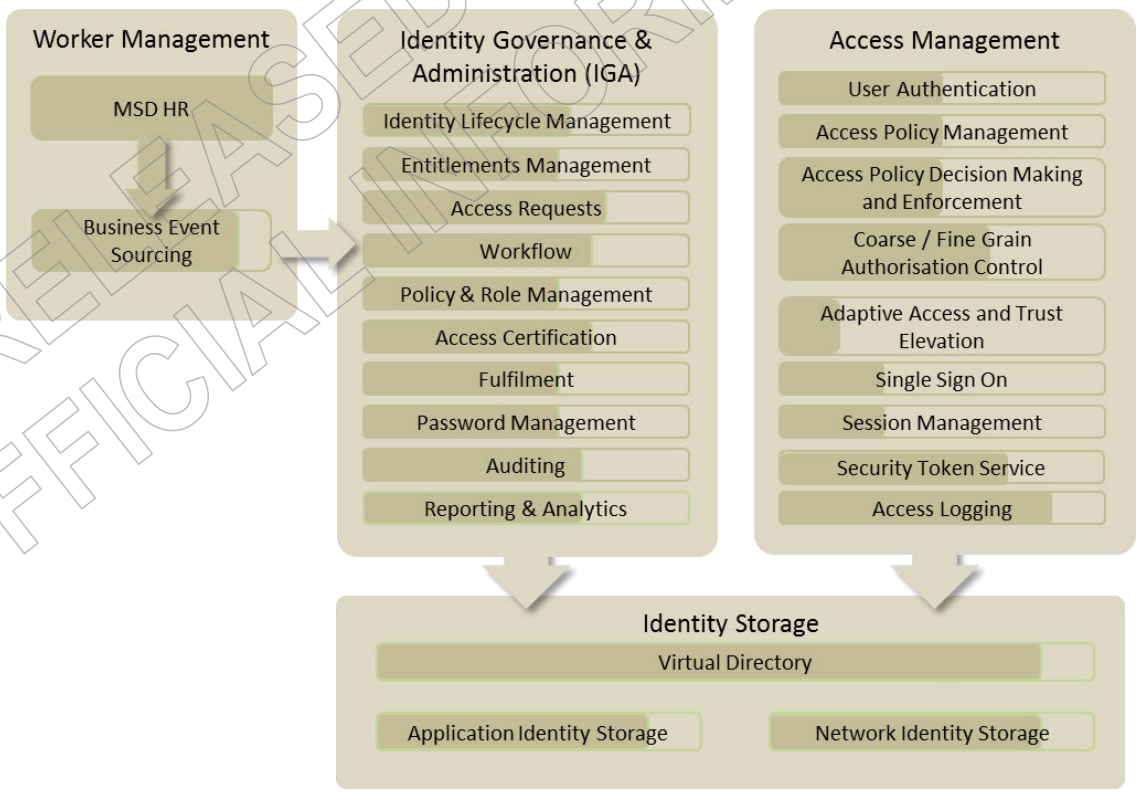



**Figure 2:** Option 2 capability maturity

***Option 3:*** *Full Vendor Managed Solution (Recommended Option)*

- MSD will have an IdAM platform that provides the capabilities required to securely provide support for increased mobile and digital channel access to systems and resources.
- MSD will benefit from the increased efficiency and improved security that centrally managed provisioning and de-provisioning from cloud and internal applications will provide.
- Functionality to perform access audits and certification will mean that IdAM can be used a robust control for operational risks.
- Existing IdAM related applications which expose MSD to risk will be retired and replaced.
- MSD will implement market leading products with a well-defined support and investment roadmap.
- Opportunity to expand the scope of Business Events that impact on identity.
- By removing the dependency on CHRIS 21 information for new starters can be sent to IGA earlier in the HR process this will reduce the time new starters have to wait for application access to be established.
- A strong control to mitigate security risks relating to unauthorised access, client information privacy or internal fraud will be in place.
- MSD will be able to adopt cloud services securely.
- Change management impact will be significant as it will require the establishment of new roles and responsibilities, as well as training for new applications and processes.
- The MSD client identity and authentication component will be extracted from MyMSD so that it can be migrated into the Ministry strategic identity platform.

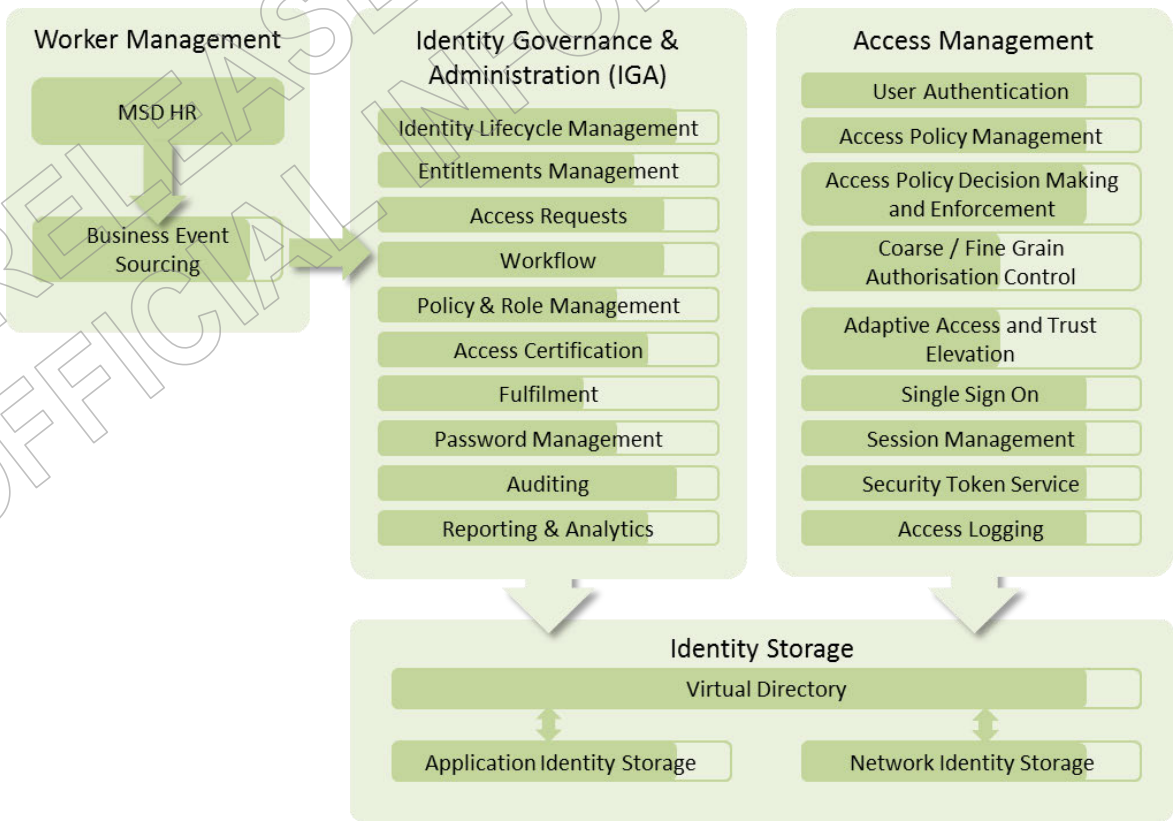



**Figure 3:** Option 3 capability maturity

***Option 4:** Defer the IdAM Solution another year*

This option is very similar to option 1 in terms of its features – with the risk of failure incrementing over this time.

Accordingly, for the year that the solution is delayed there is:

- No change management impact.
- Continuing lack of defined and enforced policy and process.
- Increasing risk profile of the IdAM function.
- Continued reliance on undocumented and unsupported processes and applications to perform access provisioning.
- Continued dependency on sequential batch driven integration which enforces tight coupling of applications.
- No improvement to IdAM capability maturity.
- MSD will continue to be constrained in making security and user experience improvements due to the lack of support and flexibility within the current Identity Management solution.
- No external support for MSD's current Identity Management solution, MSD will need to maintain its own expertise in supporting and maintaining this platform which has not only financial implications but resource prioritisation and staff retention implications as well.
- Due to the bespoke nature of the existing Identity Management components it is likely that MSD's capability to support and maintain these will further decline over time.
- No strong control to mitigate security risks relating to unauthorised access, client information privacy or internal fraud.

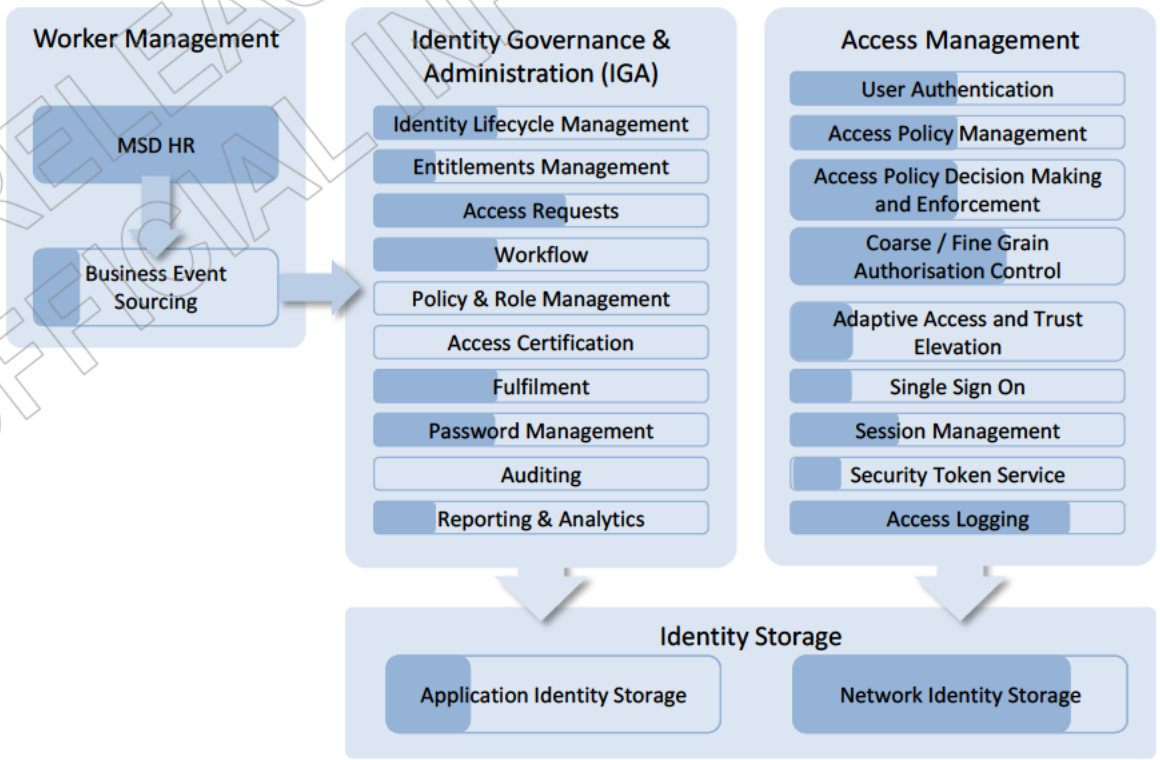



**Figure 4:** Current capability maturity

### *1.4.3 Assessment of Investment Objectives*

**Table 15:** Data Warehouse Options

| Investment Objective | Option 1<br>Do Nothing | Option 2<br>Partial Solution | Option 3<br>Full Solution |
|---|---|---|---|
| **Position MSD to take advantage of new technologies and delivery channels in a secure way** | No | No | Yes |
| **Modernise and improve the IdAM capability** | No | Partial | Yes |
| **Improve risk profile** | No | Partial | Yes |
| **Technical debt risk** | No change | Eliminated | Eliminated |
| **Resource risk** | No change | Reduced | Eliminated |
| **Unauthorised access** | No change | Reduced | Reduced |
| **Support the Shared Service business model** | No change | No change | Yes |
| **User Centric approach to designing and building IdAM solution** | N/A | N/A | Yes |
| **Manage Business Change** | N/A | Yes | Yes |

## 1.5 Delivery Plan and Procurement (Commercial Case) for the Preferred Option

### *1.5.1 Principles behind how we will deliver the IdAM capability for the Ministry*

- **Align with Government ICT strategy (Digital, IaaS/Cloud, COTS, AoG, as-a-service). But leverage existing assets.** The project will align with MSD IT Strategy and Action Plan (the ISAP) which in turn is aligned with Government ICT strategy. The programme will actively promote digital platforms; change MSD IT to use IaaS/Cloud and COTS offerings, and to move to as-a-service commercial arrangements. However this will need to be mindful of existing investments and/or commercial arrangements.
- **Grow our technology capability. Give our team career growth opportunities.** Where possible the project will seek to grow the capability of the internal IT team by giving the team growth opportunities. This will reward commitment to the organisation and reduce dependence on external contractors.
- **Minimise impact on IT customers' work programmes.** The IdAM project will implement its changes in a way that minimises any impacts on its customers. Ideally changes will be virtually transparent to them.
- **Governance framework is MSD PgMF. Delivery framework is SAFe.** From a governance and management perspective, the programme will align with MSD's Programme Management Framework which aligns with the MSP (Managing Successful Programmes) framework. Organisation of day-to-day delivery work will use SAFe (the Scaled Agile Framework).
- **Embed the customer in the heart of the delivery.** A key principle of SAFe/Agile is that the customer is involved in all discussions/decisions around scope/requirements definition and in reviewing/confirming deliverables to ensure they are fit for purpose. The project will achieve this by having BAU owners of deliverables involved throughout the delivery. There will be an overall business owner for the project (the Product Manager) with business owners who specialise in the main deliverables from specific work streams (Product Owners).
- **Chunk up the work. Use Tranches. Each Tranche delivers a business outcome.** The end of a Tranche is a major milestone that releases major business benefits. The programme will structure tranches so that an off-ramp can be invoked but business benefits can still be achieved (see below).
- **Allow for off-ramps. If an off-ramp is invoked, assets must be usable.** Where possible delivery will be structured to allow stakeholders to either stop the delivery or change direction if results indicate there are better ways to achieve outcomes. The 'off-ramp' will be structured to minimise any lost investment and to ensure that any assets at that point are usable (i.e. they are not partly completed and as a result cannot be used).
- **No big-bangs. Incremental implementations. Pilots and phased rollouts.** The project will take a risk-averse approach to implementations. There will be no big-bang implementations. Instead, changes will be implemented via small steps so that risk can be contained and widespread business impact can be avoided.
- **Front-load risk and attack it via POCs/trials.** Many areas of the project introduce new technology and involve process changes. Where a solution outcome cannot be predicted with near certainty, the programme will attempt to complete POCs and trials to prove a solution works, and to understand the implications for delivering, implementing and supporting that solution.
- **Focus. Limit Work in progress (WIP). Play 80:20.** Programme management will actively limit WIP to enable the team to focus its efforts. This reduces delivery risk, and also increases productivity. The Product Manager and Product Owners will assist in this goal by defining the MVP (minimum viable product) for each solution.
- **Use existing suppliers and AoG common capabilities.** In alignment with government guidelines and the Procurement Board guidelines, the Programme will use existing suppliers and AoG arrangements before going to the market.
- **Focus on outcomes and benefits.** Programme management will identify an approach and on-going measures that ensure there is constant focus on the outcomes and benefits the programme is aiming to achieve.

#### *1.5.1.1 Financial Analysis*

The following section outlines the project planning and management arrangements.

##### *Programme Management Arrangements*

The IdAM project and the delivery of the services will be managed within the context of a wider programme management process.

The proposed project will be delivered out of the MSD Security programme, which comprises of a portfolio of projects for the delivery of work that lifts the security posture and maturity of MSD. The scope of the programme is set out in the Security Programme Business Case approved on 16th June 2016.

The relevant programme management arrangements are as follows:

- MSD's Programme Management Framework (PGMF) will be used for overall programme governance.
- MSD's Programme Management Framework (PgMF) is based on the Managing Successful Programmes (MSP) methodology.
- The PgMF will be used to provide the project with an overall governance framework. It provides guidance on the structure of governance groups and also identifies the key artefacts that need to be produced by the programme.
- The PgMF will be tailored to reflect the needs of the project and to reflect some of the deliverables that were completed during the development of the indicative IdAM Business Case.

##### *Project Delivery*

In the event that this investment proposal receives formal approval, a project will be established to deliver the required services. The project will be delivered from within MSD Security Programme, one of MSD's established standing teams.

The 'delivery methodology' to be used for this project is a **SAFe/Agile model** to plan and manage delivery work.

- SAFe breaks down scope and requirements into Epics, Features and Stories. The Product Manager and Product Owners for each project will be responsible for working with project teams to break down scope and then for prioritising work.
- Delivery is spread across 3 month periods known as Programme Increments (PIs). Delivery in each PI is broken into fortnightly Sprints. Changes are implemented incrementally.
- An MVP approach is used to minimise delivery complexity and risk. The Product Manager and Product Owners will identify the minimum solution required to meet requirements and achieve programme benefits. This approach maximises return on investment (ROI) and also significantly increases the likelihood of successful delivery.
- BAU owners of deliverables will be identified early in the delivery. They will be actively involved in construction and sign-off activities.
- The programme will ensure that projects have considered long-term ownership of deliverables in BAU. Wherever possible BAU owners will be directly involved in management and construction work (i.e. an Agile/DevOps model). BAU owners will also be involved in the sign-off of specific deliverables. This maximises the likelihood that deliverables are accepted and fit-for-purpose. It also assists in the transfer of IP.

*Implementation Approach*

- There will be no big-bangs. Each workstream will have incremental delivery stages with phased implementation in each stage. The project will take a risk-averse approach to implementation, changes will be implemented via small incremental steps so that risk can be contained and widespread business impact can be avoided.
- Changes will be delivered over a number of stages. Within each stage, after the completion of structured testing, there will be pilots and phased rollouts to reduce risk.
- The project team will implement the majority of solution components in advance of go-live in order to minimise the amount of change required on the go-live date. The nature of this project means that it is possible to pre-install many IT changes prior to go-live. This will reduce the effort and risk involved with the final implementation.
- Implementations/deployments will be planned in such a way that a 'roll-back' to the original state is achievable if required.

*Changes to Scope*

- Changes to project scope can be made by the leadership team/ governance group so long as these changes do not impact the overall spend or expected project benefits. These changes will be managed by the product and project manager for the project and included in governance reporting. Formal agreement to variations is not required for this level of change.
- If there is a need to vary scope from the baseline and this has an impact on spend or benefits, the project manager will highlight this to the Product Manager, Product Owners and the Programme Manager. If an alternative approach cannot be found to enable a project to achieve its targets, a variation will be raised with governance groups for a decision (e.g. increase overall budget available, reduce benefits targets).

*Key Deliverables*

- A modern and effective IdAM capability made up of new people, process, policy and Technology.
- Identity Governance and Administration (IGA) platform and capability.
- Access Management platform and capability.
- New modern Identity Directory and Virtual Directory.
- MSD will use Infrastructure as a service (IaaS) by default and only purchase its own infrastructure assets by exception.

## 1.6 Financial Case for IdAM Replacement

### *1.6.1 Plan*

This is detailed in the sections above, however the focus is on the internal workforce section of IDAM and extracting the external store from MyMSD, as these are the areas with the most critical need in MSD.

### *1.6.2 Cost*

**1.6.2.1 Detailed funding breakdown for the 'Do Nothing' Option for Workforce and External Client Store**

**Please provide a breakdown of the costs of this initiative**

**IdAM Replacement: Partial Solution**

| ($m) | 2019/20 | 2020/21 | 2021/22 | 2022/23 |
|---|---|---|---|---|
| **Capital**<br>Capitalised labour including vendor costs | - | - | - | - |
| **Capital**<br>Software acquisition and implementation | - | - | - | - |
| **Operating**<br>FTEs Minimum Platform upkeep | .58 | .87 | 2.9 | 1.9 |
| **Operating**<br>As-a-service fees vendor support fees<br>Software maintenance | - | - | - | - |

**1.6.2.2 Detailed funding breakdown for the Partial Solution for Workforce and External Client Store**

**Please provide a breakdown of the costs of this initiative**

**IdAM Replacement: Partial Solution**

| ($m) | 2019/20 | 2020/21 | 2021/22 | 2022/23 |
|---|---|---|---|---|
| **Capital**<br>Capitalised labour including vendor costs | 8.0m | 6.6m | 4.6m | 2.25m |
| **Capital**<br>Software acquisition and implementation | 2.1m | 1.0m | - | - |
| **Operating**<br>FTEs | - | - | - | - |
| **Operating**<br>As-a-service fees vendor support fees<br>Software maintenance | 0.7 | 1.0 | 2.4 | 2.4 |

| 1.6.2.3 Detailed funding breakdown for the Full Solution for Workforce and External Client Store | |
|---|---|
| **Please provide a breakdown of the costs of this initiative** | **IDAM Replacement: Full Solution** |

| ($m) | 2019/20 | 2020/21 | 2021/22 | 2022/23 |
|---|---|---|---|---|
| **Capital**<br>Capitalised labour including vendor costs | 8.9m | 6.3m | 1.6m | - |
| **Capital**<br>Software acquisition and implementation | 2.1m | 1.0m | - | - |
| **Operating**<br>FTEs | - | - | - | - |
| **Operating**<br>As-a-service fees vendor support fees<br>Software maintenance | 0.2 | 1.3 | 1.3 | 1.3 |

### *1.6.3 Assumptions*

For the purposes of the cost benefit analysis the following assumptions have been made:

- Implementation costs and fixed asset costs are represented as capital expenditure
- Existing hardware cannot be decommissioned (as it is shared by other systems/applications), or would be insignificant in monetary terms, therefore not included as a benefit.
- Financial benefits that relate to inefficiencies with the current Identity Management capability, end user efficiency improvements and reduction in the support of the old Identity Management components are an indication of resource waste rather than actual tangible monetary benefits and have therefore been classified as non-cash releasing. These have been conservatively estimated so as not to unfairly influence the appraisal.
- MSD's preference is for a Managed Service rather than an in-house supported solution.
- Resource costs have been estimated based on a 36 month implementation time frame.

### *1.6.4 Estimated Costs*

The following costs were estimated:

- Costs for existing MSD Identity Management components (Oracle DBX, AUM, LDAP, and FIM SYNC) have been based on figures sourced from the Infrastructure and Services Team.
- The cost of change for the status quo includes the estimated costs for that may be incurred due to the risks and deficiencies of the current state. These costs include potential failure of a critical IdAM component, increased cost of supporting technical debt and legacy applications, purchase of unnecessary licenses and cost of dealing with privacy breaches or internal fraud.
- The internal resource effort for delivery and integration (internal project team) has been estimated using standard project resource forecasting techniques.
- Option 2 build costs have been estimated using the cost of a similar Ruby on Rails development with uplift for added complexity and assumes the development will be done in-house.
- An estimate of cost to integrate existing MSD applications to the IdAM platform has been included for options 2 and 3. A high level estimate of $1m over 2 years has been used.

- Design and build risks of $7.1m (over 5 years) have been included for Option 2 as this option requires in-house bespoke development of some IGA components; the scope of which is unknown. This is represented as capital contingency.
- Procurement risk of $1.2m (over 3 years) has been included for Option 3 as the estimates provided are high-level only and based on very high level requirements. This is represented as capital contingency.
- Design risk of $1.8m (over 3 years) has been included for Option 3 due to the limited engagement with service providers and vendors to date. This is represented as capital contingency.
- An estimate of MSD resources required to participate in the Organisational Change Management has been included in the implementation costs for options 2 and 3.

### *1.6.5 Key Constraints and Dependencies*

The proposal is subject to the following constraints and dependencies. These dependencies will be carefully monitored during the programme.

**Table 16:** Key Constraints and Dependencies related to the risks identified for this workstream.

| Constraints | Notes |
|---|---|
| **Skills** | Within MSD there are a limited number of people who have the skills and knowledge to make changes to the current state environment.<br>Within New Zealand the availability of people with skills in the technologies required to implement a modern IdAM solution is severely limited. Use Service Providers rather than build an in-house capability. |
| **Existing arrangements** | MSD has existing contractual agreements with a number of vendors who provide products/applications which make up the current IM suite.<br>Commercially MSD may be constrained with regards to terminating or modifying these agreements. |
| **Financial** | The IdAM project has been funded by the IT Security Programme up the end of 17/18 financial year. If funding beyond that date is not approved then the project will not be able to continue. |
| **Dependencies** | **Notes and Management Strategies** |
| **Affordability** | The success of this proposal is largely dependent on its financial affordability for MSD. IdAM solutions and implementation projects are notoriously complex and expensive therefore implementation is likely to involve a significant investment from MSD. |
| **Service partner availability** | The success of this proposal is dependent on the availability of service providers/ partners to complete the implementation. Preferred IdAM vendors/partners may already be engaged with other customers. |
| **Alignment** | MSD has a number of strategic initiatives and programmes of work which the IdAM project may be dependent on or be a dependency of. IdAM will introduce changes to a number of MSD systems and alignment with other programmes of work will be required. |
| **Resources** | MSD does not have the in-house expertise and/or may not have the required internal resources to carry-out an IdAM implementation. An IdAM implementation will require internal expertise and the project will be dependent on the availability of those resources. |
| **Support and commitment** | Success of the implementation will be dependent on the support from all Business Units within MSD. The commitment of resources in line with the delivery plan will also be required |

### *1.6.6 Economic Risks*

**Table 17:** Key economic (non-monetary) risks used in the economic assessment

| | Option 1<br>Do Nothing | Option 2<br>Partial Solution | Option 3<br>Full Solution |
|---|---|---|---|
| **Strategic**<br>Relating to strategic objectives, customers, stakeholders and the environment in which MSD operates. | H | M | L |
| **Operational**<br>Relating to existing business processes, change management, project objectives, dependencies, and communication. | H | H | M |
| **Political**<br>Risks associated with compliance to Government objectives. | H | M | L |
| **Reputation**<br>Associated with public perception, relationship to the media or activities that could reflect negatively on MSD. | M | M | L |
| **Regulatory**<br>Associated with compliance to policies, standards and guidelines. | M | L | L |
| **Financial**<br>Associated with the availability of funding, budgets and accuracy of financial information. | M | H | H |
| **Infrastructure**<br>Relating to capability, acquisition, implementation, and on-going support of infrastructure components. | H | M | L |
| **Resourcing**<br>Relating to resource capability, retention, satisfaction and recognition. | M | H | M |
| | High | High | Medium |

# 2. Centralise Rules Processing

## 2.1 The case for retiring DREW

The DREW (Date Rate Entitlement Wizard) was first implemented in 1996. It is an essential 'tool of trade' for 2,800 front-line case manager and contact centre staff. It performs benefit and superannuation calculations to support the processing of Income Support applications. This includes 'what if' scenarios to discuss with clients. It also is used to help front line staff to perform calculations pursuant to backdated transactions.

Over the 22 years of its existence DREW has bloated to approximately 300 screens and 5,000 function points, as legislation has been changed on a regular basis and some statutory benefit rules have been 'grandfathered'.

Whilst DREW is an integral part of the benefit / pension business processes and has been a stable reliable tool since its inception it has had a steadily rising risk profile in recent years to the point where it now poses a serious risk to the Ministry at service centres and at call centres. These are:

- **Capability / Support risk** which stems from where it is supported from and who is supporting it. A small company with one developer (Venturi) that has moved its base to France, supporting an integral step in the benefit / pension business processes is a far from ideal situation for the Ministry to be in.
- **Technology risk**
    - DREW uses an old version (V5.4) of a proprietary rules engine XpertRule (up to v9.1 in 2012) and is the only application in the Ministry that is in that technology. Although XpertRule is still active in the market and is still being improved by the UK based company that owns it, local skills are not readily available.
    - DREW is one of the few remaining Personal Computer (PC) based front-line applications. It has been a challenge to make it work under Windows 10. So far it has worked with the Windows 10 pilot sites. However, Windows 10 (unlike Windows 7) is 'evergreen' software meaning that Microsoft releases updates to the operating system every 6 months and this will be largely beyond the Ministry's control. DREW is the significant front-line application most at risk of being rendered inoperable by an operating system change.
- **Complexity risk** - The Ministry currently supports multiple repositories of the statutory eligibility and entitlement rules which can potentially give slightly different answers. This is in addition to maintaining the statutory rules still embedded in legacy backend systems such as SWIFTT. All of these increase the complexity of the Ministry's application environment. This duplication of rules, impacts the time to market and poses multiple points of risk of failure. This risk will become even more significant with the expected recommendations that will come from the Welfare Expert Advisory Group (WEAG) due in early 2019, and also from the Ministry unpacking the requirements of the newly released Statement of Intent – Te Pae Tawhiti.

These factors increase the risk of failure in DREW. The inability to run DREW would have profound effects on the daily processes at service centres and call centres which will impact the Ministry's ability to process benefit applications and change in circumstance queries / actions. These in turn will have adverse effects to the Ministry's clients who have a large dependency on the Ministry's financial support. Clients and staff are already impacted by having multiple sources of truth for statutory rules.

Inability to change DREW due a lack of support would also severely impair the Ministry's ability to enact government policy. For example, any recommendations arising from WEAG.

As further discussed in the next section, it is important to note that the case for retiring DREW is driven by:

- Eliminating risk of failure due to the factors described above
- the strategic direction of leveraging investment in Cúram as the primary repository of entitlement rules

DREW retirement is not driven by cost reduction because the current support costs and development costs for modifying DREW are very minimal.

## 2.2 Background

DREW's existence was primarily driven by limitations of the benefit / pension system 'Social Welfare Information For Tomorrow Today' (SWIFTT) implemented in 1991, namely:

- SWIFTT was not designed to handle "what if" calculations
- Where SWIFTT does not have enough information to automatically complete back dated entitlement calculations, users have to manually work out the entitlement rates and then enter them into SWIFTT. These complex calculations were performed by expert users using spread sheets and calculators with an associated steep learning curve.

DREW filled these gaps satisfactorily. It started as a tactical solution and the outcomes from it were meant to be re-implemented in a more strategic solution, but that has not happened until now. Other higher business priorities and (for some time) the absence of an agreed strategic solution resulted in more functionality built into DREW including:

- 'screen scraping' data from SWIFTT to reduce double handling of data
- Automatically sending some results back to SWIFTT
- Functions that were deemed to be easier (and cheaper) to develop in DREW – but not necessarily the architecturally right place for those functions

Today DREW is able to provide some of the more complex calculations as part of the application process or change-in-circumstance process, particularly in processing backdated transactions. Despite this assistance from DREW, there remains a steep learning curve for staff and risks of getting incorrect calculations.

Currently, the eligibility and entitlement rules in the Ministry are spread across a number of rules engines / repositories on top of the rules embedded in the legacy systems. The rules repositories are:

- XpertRule – used by DREW
- IBM's ODM[11] – used by DART[12]
- Cúram – used by CMS, EOS, ODS

The legacy systems, particularly the larger ones own the bulk of the eligibility and entitlement rules, and given their age and the design / programming patterns of their time, are tightly coupled with some of the processing rules. Two systems of particular strategic interest in this initiative are SWIFTT and SAL[13], largely because the entitlement rules and the evidence involved in executing those rules are deemed to be suited to be implemented in CMS. The key reason for using CMS for these is Cúram was originally purchased to house most of the key functions of income maintenance systems (that include SWIFTT and SAL).

This direction has not changed because Cúram remains the industry leader for social services frameworks. Cúram has industry best practices that the Ministry can leverage from. The rules are the heart and soul of any social services organisation, and the rest of the processes are dependent on those rules (and accompanying evidence) being as easily accessible as possible. Using a straight out rules engine like Operational Decision Manager (ODM) may offer other functions (e.g., modelling and simulation) but the rest of the social services functions will have to be built around those rules.

[11] ODM - IBM® Operational Decision Manager is a comprehensive decision automation platform that helps to discover, capture, analyze, automate and govern rules-based business decisions.
[12] DART - The dynamic automatic review tool is an integrated web based application that has been developed to automate the calculation of back dated review assessments when assessing overseas pensions, and a client's and/or partners entitlement to benefit for a past pay period due to a change in earnings. DART access is available to Specialised Processing Services (SPS) and Integrity Intervention Centre (IIC) users – less than 300 users.
[13] SAL - The Student Allowance and Loans system enables Students applying for a Student Allowance, Student Loan and Scholarship to be assessed and paid. Work and Income NZ took over the responsibility for the assessment and payment of Student Allowances on 1 January 1999 from the Ministry of Education. 500 con-current users can access this system at any one time and 72,000 student allowance applications are administered.

If implemented properly in Cúram, the rules are in a form that is suitable for the Ministry to migrate the rules to another rules platform in the future should the Ministry decide to move away from Cúram, thereby preserving the investment that will be made in implementing the rules in Cúram.

### *2.2.1 Current day functions of DREW*

**Table 18:** The functions that currently exist in DREW:

| DREW Tab / Function | What does it do |
|---|---|
| Summary | Display of Current values, proposed & difference as a result of a 'what if' calculation. Proposed has the 'what if' values. |
| Income Assessment | Calculates the 'what if' main service rate based on the income amount that is entered. The 'what if' income amount is also kept for 'what if' supplementary assessments. |
| Commencement Date | Calculates the commencement date of a main service by working out the entitlement date, stand-down period, and applying the 28 day rule. |
| Working for Families (WfF) Tax Credits | Calculates a non-beneficiary's Working For Families Tax Credits payment to find out their income from that. It links to the IR web site calculator. |
| Family Tax Credit (TFC) | Estimates the client's (and partner's if any) total gross income for the current tax year, in order to see whether they are over the FTC income threshold or not. |
| Accommodation Supplement | Calculates 'what if' Accommodation Supplement supplementary assessment: entitlement and rate |
| Disability Allowance | Calculates 'what if' Disability Allowance supplementary assessment: entitlement and rate |
| Temporary Add Support | Calculates 'what if' Temporary Additional Support supplementary assessment: entitlement and rate |
| Childcare Assistance | See CCS Oscar / GCAP below |
| Employment Transition payment | Calculates both the average net specified income and the rate of Employment Transition Payment when a client successfully completes an SLP Employment trial. |
| Portability NZ Residence | Calculates the 20th year and 65th year dates for portability based on client's date of birth. |
| Winter Energy Payment | Allows opt-out of Winter Energy Payment, and also applies any additional children to the payment amount. |
| Independent Circumstances | Determines whether a young person is financially independent or not. This is for students. |
| Money Management | Calculates in-hand allowance, which SWIFTT also does, but there is more detail presented in DREW. Currently for Youth benefits, but can be calculated for any main service. |
| Multi Date | Calculates the Sustainable Employment, Medical Certificate, and pregnancy dates. The dates within DREW are different than SWIFTT by 1 day. |

| | |
|---|---|
| CCS Oscar | Calculates 'what if' Child Care Assistance and OSCAR assessment: entitlement and rate. differentiates between weekly provider charge and weekly provider flat fee, whereas SWIFTT only gathers weekly provider charge |
| GCAP | Calculates 'what if' Guaranteed Child Assistance Payment assessment: entitlement and rate. |
| Training Incentive Allowance | Calculates the amount and determines whether a course is the most effective means of improving client work skills. |
| Better Off Calculator | Calculates the amount of financial assistance a client could potentially be entitled to once they come off benefit and enter paid employment |
| Special Benefit | Calculates 'what if' Special Benefit supplementary assessment: entitlement and rate |
| Financial Means Assessment | RCS Functionality (a system within a system)<br>• used by the RSU unit in Whangarei and is the main application they use in order to carry out their work. They use DREW to determine eligibility / amounts for RCS/RSS. Their correspondence to their clients is via letter templates held in DREW.<br>o Approximately 20 users<br>o Used to establish eligibility and entitlement (where applicable) for Rest Home Subsidy / Residential Care Subsidy, RSS, and Rest Home Loan<br>o Also used to assess income for residential care purposes<br>o Approximately 14 letter types are produced<br>o 3 print assessments are produced<br>o Approximately 32 functions (counted as a 'use case" each) |

To support these functions, DREW gets the data from other systems – mostly from SWIFTT via screen scraping. DREW also has its own tables (e.g., Rate Tables) to assist in the calculations, which have to be maintained and have to be synchronised with the production equivalent tables.

### *2.2.2 Future Strategy and Risk mitigation*

The Ministry has a wider strategy around rationalisation / consolidation of rules that will leverage the investment it has made in the Social Services framework Cúram (re-branded as SPM by IBM). However, in the meantime, the immediate need is to eliminate the risks posed by continuing to have DREW as a core component of the service delivery business process.

The recommended option is a two pronged approach that will:

- Ensure alternative support capability in case Venturi cannot provide support for DREW – either temporarily or permanently
- Eliminate dependency on Venturi and XpertRule by retiring DREW and achieving the business outcomes provided by DREW through other means another system.

The DREW application is built on a proprietary rules engine product called XpertRule and is supported by a small software company of one developer – Venturi – that used to be locally based but is now based in France.

It started in 1996 as a way of automating manual calculations that users had to do due to limitations of the SWIFTT benefit / pension system. Currently it is estimated that DREW has:

- More than 300 screens and reports
- Close to 2,000 "procedures"
- Approximately 5,000 – 6,000 function points (Note that SWIFTT is estimated at around 13,000 function points)

These statistics allude to the complexity and size of the DREW application.

The bulk of the rules that DREW started with are a duplicate of the SWIFTT rules, and are also aligned to the rules as documented in MAP.

Over time additional functions were added to DREW not because it was the right architectural decision but largely because it was expedient to do so. An example of this is the set of functions under the 'Financial Means Assessment' which focus on the Residential Care Subsidy (RCS) functionality. This is practically a 'small system' on its own that is used by the Residential Subsidy Unit (RSU) in Whangarei. Sometimes expediency was driven by tight timeframes associated with legislative driven projects such as Welfare Reform.

## 2.3 Risks and Benefits

### *2.3.1 Risks*

The primary risk for DREW is – **Support risk** which stems from where it is supported from and who is supporting it. A small company with one developer that has moved to France, supporting an integral step in the benefit / pension business processes is not the ideal situation for the Ministry to be in.

Another risk is that the application uses an old rules engine called XpertRule and is the only application in the Ministry that is in that **technology**. Although XpertRule is still active in the market and is still being improved by the UK based company that owns it, local skills are not readily available.

The Ministry cannot and should not maintain multiple rules engines in addition to maintaining the rules still embedded in legacy systems for a variety of reasons that can be attributed to increased **complexity** in the Ministry's IT environment. Some of the symptoms include unnecessary duplication of rules, impact to time to market, multiple points of risks of failure, etc.

***Initial risk analysis***

This section outlines the main risks that have been identified for this work stream. They are examined in terms of the seriousness of their consequence as well as their likelihood. Risk management and mitigation strategies are also outlined for each of these risks.

**Table 19:** Initial Risks

| Main Risks | Consequence (H/M/L) | Likelihood (H/M/L) | Comments and Risk Management Strategies |
|---|---|---|---|
| **If single person support is unavailable then there is no development and maintenance support for DREW.** | M | H | **Background**<br>Support for DREW is provided by a one developer company that is based in France.<br>(NB Other thing not explicitly discussed is that - internally testing is done by a specialist Business Analyst rather than by the testing team, and this also needs to be moved into standard processes.)<br>**Mitigation** |

| | | | |
|---|---|---|---|
| | | | Retire DREW (which is part of a strategic direction to rationalise / consolidate rules) which will completely remove reliance on this person.<br>In the meantime, while the rules migration project is being pursued, a support team will be set-up with an eye towards widening the intellectual property base and gaining the experience for supporting the strategic solution. |
| **If Windows 10 is upgraded then the desktop implementation may be adversely affected.** | H | L | **Background**<br>DREW uses a very old version (still a supported version) of the rules engine XpertRule and is deployed as a PC-based application. It was a challenge to implement DREW on the Windows 10 environment when the Ministry moved to Windows 10. The system could be adversely affected by a Windows 10 upgrade.<br>**Mitigation**<br>Apart from reacting if a problem happens as a result of an upgrade, DREW retirement is the only option.<br>DREW could be migrated to a later version of XpertRule but previous analysis showed that functionally, the newer XpertRule version does not offer anything of interest to MSD. The challenge with Windows 10 was not fully known until the upgrade happened. |
| **If WEAG recommendations and/or other high profile projects have tight deadlines then DREW functional changes may have to be completed as a solution response thereby further increasing technical debt.** | M | H | **Background**<br>WEAG recommendations, Te Pae Tawhiti changes, and/or legislative changes will likely have very tight deadlines. This typically forces IT to sometimes implement sub-optimal changes. DREW will typically be impacted by those changes. Ideally DREW as a legacy system is ring-fenced and new functions / modified functions are implemented in the strategic platform. If DREW is modified as a result of tight deadlines, technical debt against DREW will likely increase.<br>**Mitigation**<br>Negotiate where feasible for the proper solution to be implemented in the strategic platform. |
| **If there are multiple requirements that will impact DREW then the one person team may not be able to cope with the required changed resulting in unfulfilled requirements.** | H | L | **Background**<br>WEAG recommendations and Te Pae Tawhiti are both expected to impact DREW. The desire to open up 'rules and data' where appropriate will also likely hit DREW.<br>**Mitigation**<br>Moving the support in house to a proper support team will increase the Ministry's ability to respond. |
| **If DREW continues to exist as part of the service delivery process as one of a number of systems that implement policy rules then the different systems may come up with slightly** | H | M | **Background**<br>As MSD evolved over time and timeframe demands of previous projects were met, policy rules (particularly entitlement rules) are implemented in different systems – most notably SWIFTT, CMS, DART and DREW.<br>This opens up the risk of systems producing different results. Different results will undermine the public trust |

| | | | |
|---|---|---|---|
| **different results based on their implementation of the rules.** | | | on MSD systems, and will cause confusion amongst staff.<br>**Mitigation**<br>Rigorous testing on the systems involved. |
| **If DREW continues to exist as part of the service delivery process as one of a number of systems that implement policy rules then the development and testing costs will be higher compared to having rules implementation consolidated / rationalised..** | L | H | **Background**<br>As MSD evolved over time and timeframe demands of previous projects were met, policy rules (particularly entitlement rules) are implemented in different systems – most notably SWIFTT, CMS, DART and DREW.<br>Policy rules that are being modified that exist in multiple systems will result in more development and testing effort.<br>**Mitigation**<br>Unavoidable until systems are decommissioned and/or rules become 'service based' implemented in the strategic solution. |

Some of these risks are already in the risk register, which will be updated to ensure that all these risks are captured appropriately.

### *Risks from Change*

The tables below deal with the risks of the preferred investment option. Specifically it examines the execution risk which looks at risk associated with doing the work, the residual risks that will be leftover once the work is complete – and any introduced risk that would be created as part of doing this work. It also looks at any mitigation that may be implemented to lessen the effect or consequence of any of these risks becoming material issues that require remediation.

**Table 20:** Execution Risk

| Execution Risk | Consequence (H/M/L) | Likelihood (H/M/L) | Assessment Rating | Mitigation |
|---|---|---|---|---|
| **If projects are on tight timeframes then DREW may still have to be modified while the replacement is in flight resulting in increased technical debt.** | M | H | M | Negotiate delivery timeframes.<br>Analyse MVP for the replacement system that could reduce / eliminate duplicated code with DREW. |
| **If setting up internal support team cannot attract the required resources (support of a sunset system is not attractive to staff) then reliance on current vendor will continue.** | M | L | M | Provide pathway to support team as the support team of the new system.<br>Assess how remuneration can be attractive temporarily during the transition period from DREW to the new system. |
| **If business direction changes drastically then MSD may have to review its strategic direction / solution.** | L | L | L | Technology strategy has just been recently updated and trends have been assessed to validate strategic direction. |

| | | | | |
|---|---|---|---|---|
| **If there are DREW functions / requirements that are not a good fit for the strategic direction then MSD may have to customise the social services framework it is using for its strategic direction.** | M | M | M | Requirements that MSD IT may have doubts as to their fit with the strategic platform will be part of a 'proof of concept' / ' proof of technology'.<br>Any requirement that cannot be satisfied OOTB (out of the box) will be negotiated with IBM to be part of a 'sponsor user programme' initiative. |
| **If the requirements are not implemented correctly in the new system then trust on MSD and its systems will be undermined.** | H | M | H | Rigorous testing will be employed on the new system.<br>(this is a standard project risk) |

**Table 21:** Residual Risk

| Residual Risk | Consequence (H/M/L) | Likelihood (H/M/L) | Assessment Rating | Mitigation |
|---|---|---|---|---|
| **If there are a number of systems that implement policy rules then the different systems may come up with slightly different results based on their implementation of the rules.** | H | M | H | **Background**<br>DREW retirement is only a step towards the desired strategic outcome around rules consolidation / rationalisation. Policy rules (particularly entitlement rules) are still implemented in different systems – most notably SWIFTT, CMS, DART and DREW.<br>This risk of systems producing different results is reduced but still exists. Different results will undermine the public trust on MSD systems, and will cause confusion amongst staff.<br>**Mitigation**<br>Rigorous testing on the systems involved. |
| **If there are a number of systems that implement policy rules then the development and testing costs will be higher compared to having rules implementation consolidated / rationalised...** | L | H | M | **Background**<br>DREW retirement is only a step towards the desired strategic outcome around rules consolidation / rationalisation. Policy rules (particularly entitlement rules) are still implemented in different systems – most notably SWIFTT, CMS, DART and DREW.<br>Policy rules that are being modified that exist in multiple systems will result in more development and testing effort.<br>**Mitigation** |

| | | | | |
|---|---|---|---|---|
| | | | | Unavoidable until systems are decommissioned and/or rules become 'service based' implemented in the strategic solution. |

**Table 22:** Introduced Risk

| Introduced Risk | Consequence (H/M/L) | Likelihood (H/M/L) | Assessment Rating | Mitigation |
|---|---|---|---|---|
| **If system where DREW rules are migrated to are not tested appropriately then the system might produce erroneous results / inconsistent to other systems.** | H | L | M | Rigorous testing makes this risk 'very low' in terms of likelihood. |
| **If more functions are built into the strategic platform then that becomes the bottleneck application for development.** | M | L | L | Current SAFe and agile development processes have shown the development workload can be dealt with. |
| **If IBM withdraws support for the strategic platform or decides to move in a different direction then the Ministry will have an 'orphaned' legacy system with more functionality than it started with.** | H | L | L | The increasing penetration of the product in the worldwide social services market and the investment being made by IBM on the product shows that this is an unlikely situation.<br>However, from a solution perspective, the heart of any social services organisation is the 'policy rules'. POC includes an assessment of how best to map MSD rules in the IBM product that will allow the Ministry to export the rules out if the Ministry decides to change its solution direction. |



### *2.3.2 Benefits*

The benefits discussed in this section are based on the strategic direction of using the Cúram-based system – CMS, as the target system for migrating the DREW functions.

This project is about pursuing the strategic direction and eliminating the risk of failure for DREW. **It is not about cost reduction.** The support costs and project costs paid to Venturi lower than what is spent for other systems/applications in the Ministry's portfolio. In reality, once DREW functionality has been migrated to CMS, the support and project costs of having the functions in CMS will be higher than leaving the functions in DREW.

However, by moving the rules to the preferred strategic platform that offers other features, over time, the following are additional benefits:

- Better user experience not just from having less systems but having UI consistency
- With one less rules changes to analyse, develop and test, the Ministry can reap the following benefits:

- Future development effort will be less
- Faster speed to market
- Flexibility and adaptability
- Better positioned to continue rationalisation / consolidation of rules
- Transparency of how entitlement rules have been applied

- Enable to Ministry to share (externalise) the outcome of rules execution for external parties via APIs (could be other agencies or independent developers that may be able to offer innovative ideas)
- Move forward with retirement of other systems
- Leverage investment made in Cúram

### *2.3.3 Exclusions*

- Migration of SWIFTT entitlement rules (embedded in the application logic)
- Migration of DART entitlement rules (implemented in the ODM rules engine)
- Migration of SAL entitlement and eligibility rules (embedded in the application logic)

## 2.4 Options considered (Economic case)

### *2.4.1 Long list of options considered*

The following are the options considered before settling in on the plan & costs described in the subsequent sections.

**Table 23:** Options Analysis

| Option | Description | Status |
|---|---|---|
| **Option 1**<br>Do Nothing or<br>Do Later | No change from current state. 'Do Later' is not really buying the Ministry any time. The "likelihood" of the risks happening will progressively increase and given the consequence was previously rated as "major", the risks will move to "Severe". | Discounted |
| **Option 2**<br>Address support risks | An alternative support model is set up either internally or with a local company.<br><br>There will be an increase in operational costs with no other business value apart from removing the dependency on the current support arrangements. The system will still be running on an old version of XpertRule and with the projects in the horizon (WEAG and Te Pae Tawhiti), it is likely that there will be more changes made to DREW that will have to be re-implemented elsewhere. | Short Listed |

| Option | Description | Status |
|---|---|---|
| **Option 3**<br>Address support risks and upgrade to new version of XpertRule | In addition to an alternative support model as in Option 2, the DREW application will be upgraded to the newest feasible version of XpertRule. This will eliminate support risks and technology risks, but still does not position the Ministry strategically particularly with the expected changes from the projects in the pipeline.<br><br>The support costs will still be higher and the analysis will have to be completed to establish the XpertRule version that the Ministry can use given the constructs that are existing in the current version of DREW. Testing costs will be incurred and possibly re-training for a system estimated at 6,000 function points. | Discounted |
| **Option 4**<br>Partial DREW Retirement | Migrate DREW entitlement rules related functionality only to strategic platform (CMS).<br>Ensure consistency with MAP rules.<br><br>The non-entitlement rules related functions will stay in DREW (e.g., RCS functionality). Although there will be less users and clients affected, none of the risks have been eliminated.<br><br>Although there is some strategic value in moving the entitlement rules, the continued existence of the risks negate any value that can be derived from a partial retirement. | Discounted |
| **Option 4**<br>Full Drew Retirement | Migrate DREW rules to strategic platform (CMS), and re-implement other DREW business outcomes that are not necessarily entitlement rules based into an existing system.<br>Ensure consistency with MAP rules.<br><br>This option has sub-options given below.<br><br>This option eliminates all the identified risks and positions the Ministry strategically to deal with the expected changes from the projects in the horizon. | |
| **Option 4.1**<br>Full DREW Retirement / DART and SWIFTT continue to use their own rules | Vanilla version of Option 4.<br><br>The duplicate rules in SWIFTT and DART will not be amended to use the rules in CMS. This is the lower development risks and costs option, and allows the Ministry to learn from an involved use of the Cúram rules engine. These lessons include:<br>• Rules definition lessons<br>• Performance<br>• Maintainability | Preferred Option |
| **Option 4.2**<br>Full DREW Retirement and DART re-uses new entitlement rules | Option 4 with the addition that DART will be modified to use the same rules in the new solution where appropriate.<br><br>Sub-optimal version of Option 4.4 but with far less development risks and equally far less strategic value. | Discounted |

| Option | Description | Status |
|---|---|---|
| **Option 4.3**<br>Full DREW Retirement and SWIFTT re-uses new entitlement rules | Option 4 with the addition that SWIFTT will be modified to use the same rules in the new solution where appropriate.<br><br>Sub-optimal version of Option 4.4 with less development risks (higher than Option 4.2) but more strategic value than Option 4.2. | Discounted |
| **Option 4.4**<br>Full DREW retirement / SWIFTT and ODM re-uses new entitlement rules | Option 4 with the addition that SWIFTT and DART will be modified to use the same rules in the new solution where appropriate.<br><br>Apart from rules in the other systems (e.g., EOS, MyMSD, SAL) which for now have been excluded from this initiative but included in the larger programme of work for Rules Consolidation, this option will see full re-use of the DREW rules that have been re-implemented. This will take the Ministry far deeper into its preferred strategic position, but will have a lot of development risks. | Discounted |
| **Option 5**<br>Full DREW Retirement (non-Cúram option) | A similar set of options as in Option 4 can be developed for full DREW retirement by migrating the functions to another platform other than CMS. For example, rules can be moved to ODM, an IBM commercial rules engine. The Ministry owns licenses to ODM and is a potential target option but this option has been discounted at this point primarily for the following reasons:<br>• CMS is seen as the strategic direction for all client management functions and the product it is built on (Cúram) was purchased as the target platform for eventually running entitlement functions.<br>• Third tier assistance rules have already been moved to CMS.<br>• Social housing rules have also been built in CMS as part of the Housing project.<br>• ODM is purely a rules engine, which means the rest of functions (e.g., user interface, data access) will have to be developed along with the necessary integration services. | Discounted |

#### *2.4.1.1 Alternative Support Model*

For Options 2 - 4.4, an alternative support model will be implemented for DREW. This could be a skills transfer from Venturi to a local company (e.g., DXC) or to MSD internal staff. The arrangement could be in the form of parallel support or could be outright transfer. This alternative support arrangement will be needed to eliminate the identified support risks while pursuing the outcomes from the other options.

Note: Alternative support arrangements were previously looked at

- An internal staff was trained up in XpertRule but proper transition to internal support have to be well thought of and planned. The Ministry also currently do not have a direct product support relationship with XpertRule.
- Transfer of support to one of the Ministry's larger service provider partners was looked at, but the costs to transfer support and the on-going support costs were deemed to be quite high compared to current arrangements. However, it is the current support arrangement that is seen as one of the key risks.

The Ministry needs to seriously re-consider one of the two support arrangement options above to address the pressing support risks. Agreement to proceed with DREW retirement does not eliminate the identified risks until such time that the solution is implemented.

#### *2.4.1.2 Assumptions and Comments:*

The following assumptions and comments are common for Options 2 and 3 (and its sub-options):

- Entitlement rules as they currently exist in DREW will be implemented in the Cúram rules engine through the CMS application.
- Comment 1 is supported by the draft rules architecture principles previously presented to the Architecture Council.
- Implementing the rules in CMS will take into account as much of the known future requirements / plans for implementing benefits / pension processing in CMS – i.e., structure / hierarchy of product delivery cases, integrated case, rules and sub-rules, evidence, etc.
- DART entitlement rules will be included in the scope of what will be analysed and the approach will consider the future of DART.

### 2.4.2 Shortlisted Options

**Table 24:** Shortlisted Options

| Title | Description | Est. Costs | Risks | Pros | Cons |
|---|---|---|---|---|---|
| **Option 2** Address Support Risks | No change from current state except for support arrangements (see assumptions) | Capital: $1.9<br><br>On-going: $0.9m | High | Well understood position<br>Only cost / effort required is to have alternative support arrangements | Alternative support arrangements do not address the other risks / issues<br>Handicaps the Ministry in implementing its future plans / strategic platform to address future needs of Te Pae Tawhiti, WEAG and emerging trends. |
| **Option 4.1** Full DREW Retirement / DART and SWIFTT continue to use their own rules | Migrate DREW rules to strategic platform, and re-implement other DREW business outcomes that are not necessarily entitlement rules based.<br>Ensure consistency with MAP rules. | Capital: $17 - 25m<br><br>On-going: $1.5m | High | Risks eliminated<br>Ministry well forward with its strategic intent<br>Use lessons learned before embarking on other rules sets<br>(see benefits section) | High Risk<br>High Cost |
| **Option 4.4** Full DREW retirement / SWIFTT and ODM re-uses new entitlement rules | Option 3 with the addition that SWIFTT and DART will be modified to use the same rules in the new solution where appropriate. | Capital: $45 - 75m<br><br>On-going: $2.5m | Extremely High | See Option 3 above<br>More rules rationalised / consolidated<br>Leaves SAL rules to consider for later migration<br>Improve speed to market & development costs<br>Improve consistency | Costs and risks are higher |

#### 2.4.2.1 Notes on the Cost Estimates

The upper limit is estimated as a new development of a system using J2EE from the number of function points of DREW. From close to 5,000 Function points in 2007, a reasonable estimate given the nett changes made since then is the current size is around 6,000 function points.

*Worst case estimate (Re-build using Java)*

Assumptions:

- Java development productivity rate = 30 hours per function point
- Development Hourly rate of $100/hour
- Development costs = 40% of project costs

Calculations:

- Total Hours = 6,000 FP x 30 hr/FP = 180,000 hours
- Total Development costs = $18 m

- Total Project Costs = ($18m / 0.4) = $45 m

The lower limit was arrived at based on the recorded actual productivity statistics from the first CMS project by using the number of 'use cases' as the size of the project scope. A raw count from the table of functions of DREW would have resulted in around 60 use cases.

However given the nature of more than half of the "use cases" as straight calculations from entitlement rules (admittedly some are complex entitlement rules), a revised count of 35 "use cases" was used and the resulting estimate is close to $17m.

### *2.4.3 Recommended Option*

Option 4.1 is the recommended option for the following reasons:

- Eliminates the support risks by retiring DREW
- Eliminates the technology by removing XpertRule
- Positions the Ministry in its strategic direction
- Lesser development costs and risks while allowing for lessons to be learned from the implementation of the DREW entitlement rules

## 2.5 Delivery Plan and Procurement (Commercial Case)

### *2.5.1 Preferred Strategic Option*

The approach will be finalised as part of the project implementation. However, given the strategic intent for rules and the strategic value of the Cúram product, the approach used for the estimated costs is based on using the Cúram -based system – CMS as the home for all existing DREW functions.

There are a number of "what if" calculations that DREW does. These types of calculations are not completely out of the box (OOTB) functionality for Cúram. Although there are ways of addressing this requirement within the available OOTB functionality, the preferred approach is to work with IBM under the official "sponsored user" to come up with an approach which will later on be part of the official release of the product. Preliminary discussions with IBM are already underway, and these discussions are focused on analysing the implementation options and commissioning a Proof of Concept to test the preferred target architecture.

### *2.5.2 Key Constraints and Dependencies*

The proposal is subject to the following constraints and dependencies.....These dependencies will be carefully monitored during the programme.

**Table 25:** Key constraints and dependencies related to the risks identified for this workstream.

| Constraints | Notes |
|---|---|
| **Legislative driven implementation dates** | This will affect delivery dates and to some degree force a review of the MVP to reduce impact and reduce creation of technical debt. |
| **Resources** | Limited MSD resources to draw from. Ideally, support team and the development team are mostly in-house staff. |
| **Product features** | MSD solution will always be constrained by available functions in the strategic platform. Current assessment shows that the product can deal with MSD's required |

| | |
|---|---|
| | features and the debate will most likely be on 'how' the features are implemented. (NB MSD's position is to implement 'out of the box' rather than 'customise'.) |
| **Product roadmap** | MSD is tied in to when new features are going to be implemented in the product. However MSD has a close relationship with IBM and allows MSD to have an early view of the product roadmap, and to work with new features for the product via the 'sponsor user programme'. |
| **Dependencies** | **Notes and Management Strategies** |
| **Dependencies on other initiatives** | WEAG recommendations and unpacking of the Te Pae Tawhiti. |
| **The right resource availability** | Transfer of knowledge will be dependent on current support vendor (Venturi) and new development is dependent on other specialist resources (including DXC, IBM, and internal experts on CMS, SWIFTT and DART.) |

## 2.6 Financial Case for DREW Replacement

### 2.6.1 Detailed funding breakdown

**Please provide a breakdown of the costs of this initiative**

**DREW Replacement: Strategic Option**

| ($m) | 2019/20 | 2020/21 | 2021/22 | 2022/23 |
|---|---|---|---|---|
| **Capital**<br>Capitalised labour including vendor costs | 12 | 5 | - | - |
| **Capital**<br>Software acquisition and implementation | 0 | 0 | - | - |
| **Operating**<br>FTEs | 1.5 | 1.5 | 1.5 | 1.5 |
| **Operating**<br>As-a-service fees vendor support fees<br>Software maintenance | 0 | 0 | 0 | 0 |

Notes: Depending on the nature of the knowledge solution (e.g. SaaS vs. hosted IaaS) there may be capital amounts associated with software acquisition that will move to operating.

Notes:

- No software acquisition required as the Ministry already hold licenses for Cúram.
- The capital cost is all labour costs for the functional replacement of DREW. This includes "sponsored user" product co-development performed by IBM.
- The Ministry already has support costs for supporting CMS. Additional functionality being built into CMS will require additional resources and is currently estimated at 2-4 additional FTEs per annum. This is more than the current one developer support costs for DREW but note that the re-implemented DREW functions in CMS are more strategic and some rule sets will be re-used not just by internal systems but potentially by external parties as well.

# 3. Foundation Knowledge Management (Hindin)

## 3.1 The case for replacing Hindin

The Hindin platform has been in place at MSD since 2001. It is a knowledge base and workflow tool. It was originally procured to house numerous knowledge bases across the Ministry. These knowledge bases help inform staff about business processes and some legislative details.

Over time it has also been used as a workflow tool for core business processes such as managing Complaints, Review of Decision (RoD) and Education Provider Issue Management.

Applications resident on the Hindin platform constitute key tools for over 2,800 front line staff in service centres and contact centres. These tools are used by approximately 600 Work and Income staff per day and 500 StudyLink staff per day, which results in over 400,000 page views per month. Work and Income process approximately 4,500 Review of Decisions per year and 7,500 complaints per year in the Hindin platform. StudyLink providers raise 10,500 escalations per year to StudyLink and StudyLink staff record 15,600 interactions per year.

Strategically these applications need to be replaced with contemporary tools that are far more tightly integrated with the client context.

In the short term, the level of extreme technical debt associated with the Hindin platform is now at a level where it is not viable to continue to let the components age out another year. Currently the technology components underpinning Hindin include hardware that is 9 years old and software that is 10 years out of support. The probability of failure is trending from 'likely' towards 'almost certain'. The consequences of such a failure would be serious disruption to the critical business processes and functions supported by applications on the Hindin platform.

Contact centre and service centre staff are dependent on the information contained in the knowledge bases to support client calls. The 'review of decision' process is also fundamental to delivering on our clients' rights, as is the ability to record and deal with broader client complaints.



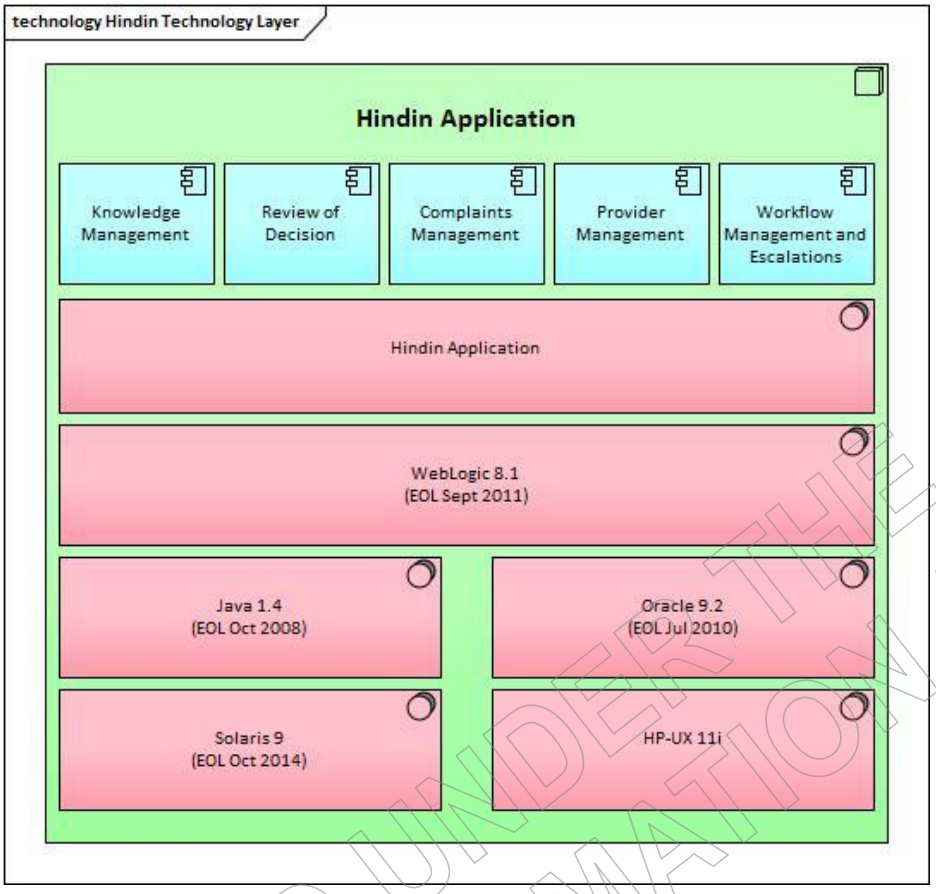
## 3.2 Background

The Hindin platform is third party software sold by Hindin Solutions, now Assura of Christchurch New Zealand. At the time that MSD purchased the product, it was exclusively a Microsoft based product, but MSD requested that a Java version of the application be developed and deployed at MSD.

Since then MSD has been the only customer for the Java version and the vendor has not invested in the code branch. It is an orphan branch of the application and has not been materially upgraded in the last 15 years.

The Hindin platform is now in a state where there are a number of serious problems that pose significant risk for the Ministry including the following out-of-support components:

- The application runs on a **9 year old** Sun (Oracle) M4000 server
- The database runs on an **8 year old** HP Superdome type server
- The application runs on the Solaris version 9 operating system **end of life since 2014 (first released May 2002)**
- Java 1.4 end of life since 2008 (first released February 2002)
- The database is Oracle version 9.2, end of life since 2010 (first released May 2002)
- Oracle WebLogic 8.1 end of life since October 2011 (first released July 2003)




It is not sustainable to continue to operate the Hindin platform under these conditions. There is a high risk of failure in which a single faulty component could render all of the applications that operate on it to be unavailable for a period of days or weeks. This is not confined to hardware and software components, the consequences of very old hardware and software includes significant risk of security vulnerabilities that cannot be fixed.

The level of extreme technical debt associated with the Hindin platform is now at a level where it is not viable to continue to let the components age out another year. The probability of failure is trending from 'likely' towards 'almost certain'.

The consequences of such a failure would be serious disruption to the critical business processes and functions supported by applications on the Hindin platform.

Over successive years small-scale projects have been initiated to reduce the number of knowledge bases still resident on the Hindin platform. These small scale projects have been intended to reduce the size of the problem without spending too much of the available balance sheet cash. The large expense of ($25 million) of retiring Hindin would have used up too much of the available capital, which was required to fund other important software, hardware, and security upgrades.

## 3.3 Risks and Benefits

The current risks include:

| Risk | Classification |
|---|---|
| The level of extreme technical debt associated with the Hindin platform is now at a level where it is not viable to continue to let the components age out another year. The probability of failure is trending from 'likely' towards 'almost certain'. | Reputation Risk<br>Operational Risk |
| System failure will lead to longer time frames to serve clients and partners. | Reputation Risk<br>Operational Risk |
| Knowledge is spread in existing knowledge management applications which are cumbersome and not consistently used by staff. This can lead to an inconsistent service experience for our clients. | Reputation Risk |
| The current implementation of the Hindin applications offer limited or no opportunity for integration to core MSD systems. | Strategic Risk |
| Multiple knowledge base applications have been added to Hindin making the discovery of content difficult for Service Delivery staff across business units. | Operational Risk |



### *Initial risk analysis*

This section outlines the main risks that have been identified for this work stream. They are examined in terms of the seriousness of their consequence as well as their likelihood. Risk management and mitigation strategies are also outlined for each of these risks.

**Table 26:** Initial Risks

| Main Risks | Consequence (H/M/L) | Likelihood (H/M/L) | Comments and Risk Management Strategies |
|---|---|---|---|
| **The level of extreme technical debt associated with the Hindin platform is now at a level where it is not viable to continue to let the components age out another year. The probability of failure is trending from 'likely' towards 'almost certain'.** | H | H | Once all functionality within the Hindin applications are migrated to modern supported platforms, the Hindin applications can be retired. |
| **System failure will lead to longer time frames to serve clients and partners.** | H | H | Once all functionality within the Hindin applications are migrated to modern supported platforms, the Hindin applications can be retired. |
| **Knowledge is spread in existing knowledge management applications which are cumbersome and not consistently used by staff. This can lead to an inconsistent service experience for our clients.** | M | M | The future Knowledge Management solution will be built to align with business practice and process, providing consistency for staff. |

A risk register has been developed and will be progressively updated as more detailed analysis is undertaken.

### *Risks from Change*

The tables below deal with the risks of the preferred investment option. Specifically it examines the execution risk which looks at risk associated with doing the work, the residual risks that will be leftover once the work is complete – and any introduced risk that would be created as part of doing this work. It also looks at any mitigations that may be implemented to lessen the effect or consequence of any of these risks becoming material issues that require remediation.

**Table 27:** Execution Risk

| Execution risk | Consequence (H/M/L) | Likelihood (H/M/L) | Assessment Rating | Mitigation |
|---|---|---|---|---|
| **The ability to integrate a new cloud (SaaS) platform for Knowledge Management with MSD identity management systems** | M | H | M | The identity management integration may initially be a tactical solution that does not completely meet the needs of the business. Once the new identity management solution is in place, the integration method can be upgraded. |
| **Complexity of data migration** | L | M | M | Early analysis into the complexity of the data migration. This migration task will need to start as soon as possible. |
| **Unacceptable Knowledge Management RFP responses** | M | L | M | Implement the tactical solution of Confluence as described in the second option. |
| **Knowledge Management RFP takes longer than expected** | M | M | M | Adjust the resource plan to increase the amount of concurrent activities or extend the timeline into the third year. |
| **Unable to resource enough Cúram Social Program Management (SPM) developers because of resource contention** | M | L | M | Adjust the resource plan to decrease the amount of concurrent activities resulting in an extended timeline into the third year. |



**Table 28:** Residual Risk

| Residual risk | Consequence (H/M/L) | Likelihood (H/M/L) | Assessment Rating |
|---|---|---|---|
| **Knowledge continues to be spread across multiple knowledge silos within the new Knowledge Management tool, resulting in a cumbersome experience for staff.** | M | L | M |

**Table 29:** Introduced Risk

| Introduced risk | Consequence (H/M/L) | Likelihood (H/M/L) | Assessment Rating |
|---|---|---|---|
| **Potential for a new implementation partner to be introduced as part of the RFP process, increasing the complexity of the operating environment.** | L | L | L |
| **A new skill set will need to be developed within MSD to support the new Knowledge Management tool, increasing the complexity of application support.** | L | L | L |

***Benefits***

The benefits of moving off the Hindin platform include:

- Remove severe operational risk of the Hindin platform becoming unavailable.
- Increase staff engagement and confidence, through a single source of truth in a new knowledge management solution.
- Decrease time and cost to service clients by improved access to information that is contextual and relevant to the client through the use of artificial intelligence.
- Decrease cost to train staff with the reduction of systems and the improved integration of systems.
- New modern solutions will provide flexibility for new requirements and process improvement (improved ability to respond to change).
- Introduction of a feedback mechanism for staff to evaluate where content is not fit for purpose and ensure content remains updated and relevant.
- Provide client and partner self-service options.

Residual Risk:
Through implementing the proposed changes the risk to MSD is greatly reduced. The functionality used by MSD staff will be running on modern, supported software with a roadmap for application support into the future. Unlike the current Hindin platform.

## 3.4 Options considered (Economic case)

### *3.4.1 Long list of options considered*

| Option | Description | Status |
|---|---|---|
| **Option 1**<br>Strategic option | The strategic option is to move the Hindin knowledge bases to an intuitive repository where artificial intelligence technologies such as cognitive computing can be applied in order to surface required information to client facing staff members in the right place right time. In addition to providing static information in the correct context, this option provides future opportunities to implement augmented intelligence to complement human intelligence by performing repetitive tasks, analysing large data sets and providing suggested outcomes. This will leave staff to exercise judgment and deal with more complex issues. This kind of technology will make staff more efficient and provide a smarter way of working.<br><br>The knowledge repository will be integrated with the core case management system so that knowledge can be provided automatically in the context of where a staff member is working.<br><br>The Review of Decision functionality currently resident on the Hindin platform will be moved to the Appeals component built into the Cúram SPM system. Initial analysis shows a high level fit with the high level requirements.<br><br>The Complaints functionality currently resident on the Hindin platform will be moved to the Cúram SPM system.<br><br>The Provider Management functionality currently resident on the Hindin platform will be moved to the Cúram SPM Provider Management Component.<br><br>After the client based Hindin functions have been migrated to the MSD client management system Cúram SPM, staff experience will be improved through consolidation of client information into a single system. | Short list option<br>Preferred solution. |
| **Option 2**<br>Do nothing | The do nothing option would result in **certain failure** of all of the Hindin based applications. As the platform components continued to age and be further out of vendor support. This is not a viable option because key business processes in the Ministry would no longer be supported. | Discounted |
| **Option 3**<br>Defer for 12 months | This option would result in some of the hardware clicking over to10 years old with the probability of failure continuing to escalate. This is not preferred as the risk of failure to key MSD business functions continues to be intolerably high. | Discounted |
| **Option 4**<br>Upgrade servers, operating systems, database, and Java to supported versions | This option would include the migration of all component parts of the Hindin platform to supported versions. This option would entail a significant overhaul of the15 year old Hindin Java application code as it is unlikely to be able to run on target architecture of the latest versions of Java and Oracle database server. The net result would be an expensive re-platform of capability that is 15 years out of date, and no longer meets MSD business needs. | Discounted |

| | | |
|---|---|---|
| **Option 5**<br>Move to the Microsoft based version of Hindin. | This option will involve moving all of the content and workflows to the version of Hindin that is currently supported. (i.e. the version of Hindin that is supported for all customers except MSD). This is not seen as a strategic option because it will not be integrated with the Cúram case management system and will be a stranded investment, not aligned with where MSD wants to move.<br><br>Furthermore, the Review of Decision and Complaints processes need to be effectively integrated with the client case management system. In line with the MSD technology strategy, the preferred target environment for this functionality is the Cúram appeals and Complaints processing.<br><br>A study was done into the viability of moving to the Microsoft version but it was found that there had been a divergence in the product relative to MSD business needs and that it was no longer a good match. | Discounted |
| **Option 6**<br>Move Review of Decision, Complaints and Partners to Cúram CMS and knowledge bases to Confluence | This option is partly strategic and partly tactical. It differs from the preferred option in that the knowledge sharing and collaboration system Confluence will be the target environment for knowledge bases.<br><br>Confluence has been the stop-gap tactical solution employed to date for transferring the knowledge bases to lessen the impact of a Hindin failure. It is considerably less expensive than the preferred strategic option which uses intelligent systems to consistently pass the right information to staff members. Confluence offers a supported platform for the knowledge content but it only offers very basic search capabilities. Longer term the content will need to be moved again to the strategic solution. This option will include the move of Review of Decision and Complaints to the Cúram CMS, so that the complaints and review of decision are attached to the client record.<br><br>This option will include moving the Provider Management component to Cúram Provider Management. | Short list option |

### *3.4.2 Shortlisted Options*

#### *3.4.2.1 Strategic Option*

The Te Pae Tawhiti Technology Strategy indicates the Ministry will progress to implementing one source of truth for client data and simplify systems to greatly improve the staff experience. This starts to deal with two of the main pain points for staff and clients in "there is no single client view" and MSD has "disparate business processes and lack of automation". MSD's preferred system of record for client related data and events is the IBM's Cúram Social Program Management (SPM).

With the procurement of a purpose built knowledge management system, information can be gathered, mapped and interrelated in a central location that can be searched and referenced by staff and other systems. Other systems include Cúram SPM, smart agents, and artificial intelligence platforms. These integrated systems can be configured to provide the right information, in the right place at the right time to staff and clients. Unlike the existing system that is not integrated with Cúram SPM and requires staff to manually search for the information they require across multiple knowledge management applications.

With the addition of augmented intelligence (from a future integrated artificial intelligence platform), MSD can make use of information from both the knowledge management system and Cúram SPM, to improve staff capability while making efficiency gains.

The knowledge management system will provide a feedback mechanism for staff and clients to evaluate content to ensure its effectiveness and conversion to business as usual.

The knowledge management system will have a content lifecycle framework that defines how content will be managed along with a standard taxonomy schema (developed together with Information Services) to create a model which can be reusable across all MSD information.

This option will allow MSD to continue to gain value from knowledge management over time as understanding and learning enables future actions relative to a client's context.

Cúram SPM has an off-the-shelf module for Review of Decision type processing called Appeals. Utilising Appeals processing for Review of Decision, and using the Cúram SPM framework for client complaints in general, means staff will have fewer systems to use and that complaints, and reviews of decision will be integrated with the client record. Both Review of Decision and complaints naturally fit with Cúram SPM, because this is the system where the bulk of the decisions for client provision of service are made. This will help alleviate two of the significant pain points with the Ministry's existing technology. Unlike the existing process implemented in an Hindin application where Review of Decision and complaints are managed outside of Cúram SPM with no integration.

Cúram SPM has an off-the-shelf module for Partners that can be extended to accommodate the provider functionality currently being provided by the Hindin platform. This will extend the current strategic use of Provider Management in Cúram SPM, further consolidating provider management functions in a single system. Unlike the existing component within the Hindin platform that is separate from other partner management components at the Ministry.

The Te Pae Tawhiti Strategy indicates the Ministry will help people be aware of all the support available to them and provide confidence they will receive it. Moving the multiple Hindin knowledge bases to a single intuitive repository, with integration to the core case management system will surface client information to staff in the right place at the right time.

#### *3.4.2.2 Partly Tactical Solution*

The partly tactical solution differs from the strategic option in that the knowledge sharing and collaboration system is Confluence. Some Ministry knowledge bases have already been transferred to Confluence to lessen the impact of Hindin failure. Confluence is considerably less expensive than the strategic option with no use of intelligent systems and no integration with the core case management system. This lack of integration will require staff to manually search for the information they require.

Confluence does however provide a single knowledge sharing and collaboration system where Ministry knowledge can be gathered, mapped and interrelated. The information can be searched and referenced by staff and Confluence provides features that allow staff to provide feedback on content as well as monitor content for changes.

With no integration with the core case management system, this solution does not deliver a single client view to staff. Also with no smart agent or artificial intelligence features, this is only an interim solution providing limited long term benefit.

## 3.5 Delivery Plan and Procurement (Commercial Case)

### *3.5.1 Preferred Strategic Option*

#### *3.5.1.1 Cúram Appeals, Complaints and Partners*

The components of the Cúram software required are already owned by the Ministry, and there is an existing in-house team that oversees configuration, testing, and implementation of Cúram modules and features.

The in-house Cúram team will be augmented with suitably skilled external labour using existing panel arrangements and external professional services contracts with IBM. It is not envisaged that any Procurement activity will be required for the Cúram components of the solution.

The in-house capability utilises the Scaled Agile Framework (SAFe) and DevOps as key parts of the Technology operating model to break the delivery up into smaller more consumable increments, and thereby avoid the risk of a 'Big bang" implementation.

It is a tried and true delivery pattern for the Ministry that has successfully delivered a number of large scale projects, and is viable in this case.

Among the first steps will be seek to eliminate the risk that this solution will not meet the business need or have considerable technical hurdles to implementation. This will be achieved by validating business fit of functionality in the solution, and that the high level design is feasible including any required integration points. This will be followed by a technical Proof of Concept PoC which will validate that the solution will work in the Ministry's environment. The technical PoC also allows the eventual end users to visualise the system early.

Development of a Minimum Viable Product (MVP) will then be pursued that will enable end users access to the system as soon as possible so their feedback can be incorporated into subsequent development iterations.

#### *3.5.1.2 Knowledge Base*

There will be a procurement exercise, abiding by the government rules of procurement, to determine the Knowledge Base software that will be required to meet the Ministry's strategic needs. The initial scope for the project is a target repository for the knowledge bases currently in Hindin.

Whilst only the current Hindin content is in scope, the solution will need to be highly scalable in volume of data, functionality, and access methods. For example, some of the knowledge/content types will need to be simultaneously available to staff, partners, and clients, via different channels. The knowledge repository will need to be amenable to natural language enquiry and speech interfaces. It is also possible that this will be a cloud based service.

Given that this will be a new capability, the Ministry will create a joint implementation plan with the vendor to ensure successful delivery. This delivery plan will splice in with the Ministry's Agile delivery method to ensure successful integration. Again, this is a tried and true delivery pattern.

### *3.5.2 Move ROD, Complaints and Partners to Cúram CMS and Knowledge Bases to Confluence*

#### *3.5.2.1 Cúram SPMbased Appeals, Complaints and Partners*

See 3.5.1.1 above.

#### *3.5.2.2 Confluence Based Knowledge Bases*

To partially mitigate the risk to the Ministry, a tactical solution has already moved a number of legacy Hindin knowledge bases to Confluence. This solution will build on the existing Confluence deployment to allow the decommissioning of the knowledge bases stored in the Hindin platform. Moving the information over is largely a business function and can be done incrementally to incrementally reduce risk of the information becoming unavailable.

This is supported software, but has limited knowledge management functionality and no integration with other Ministry systems. This option does not include any potential deployment of smart agents or artificial intelligence.

This option will complete the tactical solution of moving all of the knowledge content out of Hindin and into Confluence as an interim stage.

This approach would recognise the move to Confluence will be a stranded asset and further investment (some of it duplicated) will be required to move to the eventual strategic solution. This approach will not require any procurement plan or new commercial model because the Ministry already has rights to use the Confluence systems and has sufficient licenses.

### *3.5.3 Key Constraints and Dependencies*

The proposal is subject to the following constraints and dependencies. These dependencies will be carefully monitored during the programme.

**Table 30:** Key constraints and dependencies related to the risks identified for this work stream.

| Constraints | Notes |
|---|---|
| **Access to business Subject Matter Experts** | Building out a new Knowledge Management Tool that meets the needs of the business now and into the future will require time from subject matter experts. |
| **Limited number of Cúram Social Program Management (SPM) developers** | Cúram Social Program Management (SPM) developers are a speciality resource. |
| **Dependencies** | **Notes and Management Strategies** |
| **IDAM Replacement** | Ideally the new Knowledge Management tool will integrate with the IDAM replacement and be hosted in the cloud. |

## 3.6 Financial Case for Hindin Replacement

### 3.6.1 Detailed funding breakdown

**Please provide a breakdown of the costs of this initiative**

**Hindin Replacement: Strategic Option**

| ($m) | | 2019/20 | 2020/21 | 2021/22 | 2022/23 |
|---|---|---|---|---|---|
| **Capital** Capitalised labour including vendor costs | Product RFP | 0.3 | - | - | - |
| | Staff Knowledge Base Implementation | 2.0 | 1.6 | - | - |
| | Client and Partner Knowledge Base Implementation | - | 1.0 | - | - |
| | Complaints | 2.3 | | | |
| | Review of Decision | 0.4 | 2.5 | | |
| | Provider Management | - | 0.9 | | |
| **Capital** Software acquisition and implementation | | 5.0 | - | - | - |
| **Operating** FTEs | | 0.7 | 0.7 | 0.7 | 0.7 |
| **Operating** As-a-service fees vendor support fees Software maintenance | | 1.8 | 1.8 | 1.8 | 1.8 |

Notes: Depending on the nature of the knowledge solution (e.g. SaaS vs. hosted IaaS) there may be capital amounts associated with software acquisition that will move to operating.

### 3.6.2 Detailed funding breakdown

**Please provide a breakdown of the costs of this initiative**

**Hindin Replacement: ROD and Complaints to Cúram SPM and knowledge content to Confluence**

| ($m) | | 2019/20 | 2020/21 | 2021/22 | 2022/23 |
|---|---|---|---|---|---|
| **Capital** Capitalised labour including vendor costs | Knowledge Base | 2.0 | 1.4 | - | - |
| | Complaints | 2.3 | | - | - |
| | Review of Decision | 0.4 | 2.5 | - | - |
| | Provider Management | | 0.9 | - | - |
| **Capital** Software acquisition | | - | - | - | - |
| **Operating** FTEs | | 0.3 | 0.3 | 0.3 | 0.3 |
| **Operating** As-a-service fees vendor support fees Software maintenance | | 0.2 | 0.2 | 0.2 | 0.2 |

Notes:

## 3.6.3 Detailed funding breakdown

**Please provide a breakdown of the costs of this initiative**

**Partial Hindin Replacement: Knowledge content to Confluence only**

| ($m) | | 2019/20 | 2020/21 | 2021/22 | 2022/23 |
|---|---|---|---|---|---|
| **Capital** Capitalised labour including vendor costs | Knowledge Base | 2.0 | 1.4 | - | - |
| **Capital** Software acquisition | | - | - | - | - |
| **Operating** FTEs | | 0.3 | 0.3 | 0.3 | 0.3 |
| **Operating** As-a-service fees vendor support fees Software maintenance | | - | - | - | - |

Notes: This option will not allow the complete Hindin platform to be retired, but will reduce the overall risk.

# 4. Data Warehouse Replacement

## 4.1 The case for replacing the Data Warehouse

The data warehouse is an integral part of MSD and Oranga Tamariki's (OT) operation. The warehouse stores and integrates complex administrative data from over one million New Zealanders and enables MSD and OT to perform a wide range of, in some cases critical, functions, including frontline case management, advanced analytics, reporting and business intelligence. The Ministry of Housing and Urban Development (HUD) also depend on the data warehouse for the latter two functions using MSD data.

However, the demands placed on this system now far exceed what the platform was originally designed to deliver. The combination of increasing service demands and poor governance has meant the system has evolved in an ad-hoc way, requiring short term, quick-fixes, the consequences of which have built up over time and led to an increasingly complex, brittle, and ultimately unsustainable platform for delivering core functions. This accumulation of "technical debt" has reached a tipping point. The system is now in a state that not only limits our ability to develop new insights for supporting MSD's key strategic shifts but also presents a critical and imminent risk to performing MSD's most basic, business-as-usual activities. The system is now prone to regular outages that directly impact front line staff and the services clients receive; creates risks to client privacy; lacks the resilience needed to respond to inevitable disruptions and new service demands; and is no longer cost-effective to maintain. If unaddressed, these problems will get worse.

There is an opportunity now to establish a new data warehouse that delivers enduring value by providing a more stable, scalable, secure, flexible and cost-effective platform. This will allow MSD, OT, and HUD to deliver core functions, address emerging business priorities and respond more sustainably to longer term and future changes and demands on the system. In addition MSD and OT Chief Executives agreed in September 2018 to separate the provision of some shared services between the two agencies, with other services continuing to be provided until there is a natural investment point that requires a decision. This bid provides such an opportunity and in a way that maintains cross sector partnership.

## 4.2 Background

MSD's data warehouse is a critical asset that supports diverse functions, ranging from frontline operations and routine business reporting through to advanced analytics. The scale and complexity of this data asset, and the systems needed to support it, is substantial and growing. For example, the current system:

- Provides data management and reporting services for OT and HUD as a shared service.
- Now contains over 7 million lines of code that must be manually created and maintained.
- Stores information from over 50 different source applications that needs to be replicated daily.
- Incorporates multiple regular data updates from eight different agencies.
- Generates over 270,000 case manager reports each month.
- Provides weekly service matching information for MSD's 280,000 main benefit clients.
- Delivers data feeds for Statistics New Zealand's Integrated Data Infrastructure.
- Provides data for performance and accountability reporting.
- Supports a range of advanced analytics capabilities, including research, evaluation and business intelligence.

MSD recently commissioned Accenture to, in part, review the state of the data warehouse. This review identified that the current system is under severe strain caused by the cumulative effects of multiple factors, including:

- The platform architecture is not designed to meet increasing government and wider public demands for flexibility, service innovation and data transparency.

- Poor data governance and the lack of a cohesive vision. This has meant that system changes are often undertaken in an ad hoc way with little to no oversight and coordination to ensure these changes are sustainable.
- Lack of codified standards and practices. System changes are often poorly or inconsistently documented which creates significant risks when the few staff with deep institutional knowledge leave the organisation.
- The compounding effects of technical debt. Over time, the accumulation of ad hoc fixes and poor processes has meant the system is becoming increasingly prone to outages. Often the only option to address these issues is to create new artefacts, rather than fix the underlying, systemic issues – leading to yet more complexity and system vulnerability.

There is now clear evidence the system has grown unsustainably and that technical debt has reached a point where it is having critical and imminent, if not immediate, impacts across MSD's business including:

- **Significant adverse impacts on MSD clients and frontline staff**. Over the course of 2018 there have been regular outages and operational failures caused by the complexity and inflexibility of the system. In one recent example, medical certificate matches (needed to process payments to clients with disability) had to be processed manually at an overhead of 44 FTE per day at front line. Vendor experts and MSD technicians took nearly two weeks of investigation to diagnose and take measures to address the problem.
- The probability of outages having potentially very severe impacts on clients is becoming increasingly likely, if not inevitable. For example, the Accenture report notes that more complex errors are believed to exist, but have not been identified, and that outages could have widespread impacts on highly vulnerable clients, for example, urgent housing grants may be delayed, urgent at-risk children may not be flagged for attention, MSD may continue to contact deceased clients or initiate debt recovery because DIA data is unavailable. The risks to client wellbeing and the wider reputational risks to MSD and the Government are therefore substantial.
- **Risks to client data security, public trust and meeting obligations pursuant to the Privacy Act 1993**. The Privacy Act, as well as new guidance from Stats New Zealand, and MSD's Privacy Human Rights and Ethics framework, include principles that agencies must follow to demonstrate how personal information is used with the aim of ensuring that only authorised users can access personal data and for a legitimate purpose. However, the historical lack of a coherent data governance system, and unclear processes, makes it increasingly challenging, if not impossible, to meet these obligations because it is difficult to understand MSD's data assets, their relationships, who has access to them and how and where they are used. These privacy risks are compounded whenever system changes occur. It is further noted that OT is concerned that only authorised staff should be able to access their agency's data, but the current system does support the level of agency control and oversight required.
- **Increasing resources needed to maintain even basic functionality.** Because of the growing complexities and interdependencies within the system, implementing even minor system changes and correcting errors is becoming increasingly costly and time-consuming. A simple legislative change to a descriptive text, for example, requires manually modifying and testing 150 reports. In one instance, a data error affecting 200 clients over a three month period required approximately one month of processing time to resolve. Over all work occurring in the warehouse, it has been estimated that 75-80% of developer resource is spent maintaining the over 7 million lines of production code (this includes responding to up-stream system changes), with only the remainder available to support new initiatives, growth, or transformation.
- **Risks to the accuracy and timeliness of delivery.** The reputation of MSD and the wider integrity of the benefits system depend on accurate and timely reporting. The lack of controlled and consistent reporting rules, means that it is becoming increasingly challenging to provide assurance that key data is being reported accurately and consistently. The manual work and complexity often means customers need to wait too long for information.
- **Risk of not meeting future need, growth or innovation.** The current system is an impediment to realising the expected value of advances in analytics.

## 4.3 Risks and Benefits

### *4.3.1 Risks*

There are major risks associated with the status quo are:

- Data privacy - failure would result in potentially significant breaches of the Privacy Act.
- Business disruption - failure leads to slowed/stopped operations resulting in failure to meet critical client needs and potentially for extended periods of time.
- Inability to deliver insights across channels – making it harder for frontline staff to provide a tailored and responsive service to clients.
- Slow delivery of new products and system changes, including delays to implementing legislative or operational policy changes.

In addition, there are significant secondary issues associated with the status quo:

- Poor client experience.
- Reputational risks to MSD, OT, HUD and the Government.
- Reduced ability to partner with external organisations.
- Low or unknown data quality.
- Less innovation to drive long term improvements in service efficiency and client experience (e.g. self-service, real time options).
- Lock-in that may constrain the option set for the target operating model, and reduce our ability to respond and adapt to demands for service innovation.
- Increasing long term costs.

The two preceding lists inform the main objectives that options are tested against in the appendices.

***Initial risk analysis***

This section outlines the main risks that have been identified for this work stream. They are examined in terms of the seriousness of their consequence as well as their likelihood. Risk management and mitigation strategies are also outlined for each of these risks.

**Table 31:** Initial Risks

| Main Risks | Consequence (H/M/L) | Likelihood (H/M/L) | Comments and Risk Management Strategies |
|---|---|---|---|
| **System failure and business disruption** | H | M | **Background**<br>Due to the age and complexity of the system there multiple layers of outages ranking from whole system down, to failure to process and interface issues. Each layer has a different outage time and risk profile. However it all impacts the staff day to day work, due to the way data warehouse is used in MSD at the moment (application layer, operational intelligence, Single and integrated data sourcing, etc.). Such outages can lead to risks to client wellbeing and the wider reputational risks to MSD and the Government. |

| | | | |
|---|---|---|---|
| | | | **Mitigation**<br>The new design will consider the decoupling of different capabilities and will build a platform fit for all required capabilities (rather than added organically). The new platform will be selected based on scalability and required functions. |
| **Failing to deliver a tailored and responsive service to clients** | H | M | **Background**<br>Inability to deliver insights across channels due to complicated code and coupled functions and models.<br>**Mitigation**<br>In the new platform all new and migrated code will be simplifies, decoupled and structured in a way that allows re-use of components rather than the current complex coding standards (or lack of it). Auditing processes and governance will be introduced to ensure an on-going compliance. |
| **Resources and skills to maintain and support the current platform** | H | H | **Background**<br>Because of the growing complexities and interdependencies within the system, implementing even minor system changes and correcting errors is becoming increasingly costly and time-consuming. A simple legislative change to a descriptive text, for example, requires manually modifying and testing 150 reports. In one instance, a data error affecting 200 clients over a three month period required approximately one month of processing time to resolve. Over all work occurring in the warehouse, it has been estimated that 75-80% of developer resource is spent maintaining the over 7 million lines of production code (this includes responding to up-stream system changes), with only the remainder available to support new initiatives, growth, or transformation.<br>**Mitigation**<br>Selecting the up-to-date technologies and decoupling the complexity in the platform will help to reduce this risk as it will be easier to train or hire staff with today's standard data technologies. |
| **Old Technologies that cannot cope with new data concepts, solutions and paradigms** | M | H | **Background**<br>The platform architecture is not designed to meet increasing government and wider public demands for flexibility, service innovation and data transparency.<br>**Mitigation**<br>The design will include platforms and technology asset management standards to ensure up-to-date upgrades and on-going flexibility. |
| **Infrastructure scalability is not coping with rapid data growth** | M | H | **Background**<br>The platform architecture is not designed to meet increasing government and wider public demands for flexibility, service innovation and data transparency.<br>**Mitigation**<br>Selecting new platforms and possibly cloud services will enable a cost effective and agile scalability of the platform, only when is needed. |
| **Low or unknown data quality** | H | H | **Background**<br>Lack of data management at Data Warehouse or source systems levels for many years now, led to a problematic |

| | | | |
|---|---|---|---|
| | | | data quality. In addition, many solutions are built over the years to duplicate data (to mitigate integration cost). The result, however, is unmanaged data with no clear source of truth.<br>**Mitigation**<br>Data management and discovery tools and new processes will be included in the design of the new platform, as well as updated data policies, standards and governance to ensure an on-going data quality. |
| **Risks to the accuracy and timeliness of delivery** | H | H | **Background**<br>Because of the growing complexities and interdependencies within the system, implementing even minor system changes and correcting errors is becoming increasingly costly and time-consuming. A simple legislative change to a descriptive text, for example, requires manually modifying and testing 150 reports. In one instance, a data error affecting 200 clients over a three month period required approximately one month of processing time to resolve. Over all work occurring in the warehouse, it has been estimated that 75-80% of developer resource is spent maintaining the over 7 million lines of production code (this includes responding to up-stream system changes), with only the remainder available to support new initiatives, growth, or transformation.<br>**Mitigation**<br>Data management tools and policies will be introduced to manage the data quality at source as well as at storage level. Similarly data lineage and catalogue tools will be introduced.<br>Similarly the re-designed models will allow for a more agile delivery. |
| **Data privacy - failure would result in potentially significant breaches of the Privacy Act.** | H | M | **Background**<br>The Privacy Act, as well as new guidance from Stats New Zealand, and MSD's Privacy Human Rights and Ethics framework, include principles that agencies must follow to demonstrate how personal information is used with the aim of ensuring that only authorised users can access personal data and for a legitimate purpose. However, the historical lack of a coherent data governance system, and unclear processes, makes it increasingly challenging, if not impossible, to meet these obligations because it is difficult to understand MSD's data assets, their relationships, who has access to them and how and where they are used. These privacy risks are compounded whenever system changes occur.<br>**Mitigation**<br>The new design will consider all such aspects. Data governance and lineage needs to be enforced across all data storages (including source systems). The client consent should carry through the data asset life-cycle. |

A risk register has been developed and will be progressively updated as more detailed analysis is undertaken.

### *Risks from Change*

The tables below deal with the risks of the preferred investment option. Specifically it examines the execution risk which looks at risk associated with doing the work, the residual risks that will be leftover once the work is complete – and any introduced risk that would be created as part of doing this work. It also looks at any mitigation that may be implemented to lessen the effect or consequence of any of these risks becoming material issues that require remediation.

**Table 32:** Execution Risk

| Execution risk | Consequence (H/M/L) | Likelihood (H/M/L) | Assessment Rating | Mitigation |
|---|---|---|---|---|
| **The scale of work required to move to a different platform** | H | L | M | The size of the current Data warehouse and its products is significantly big. To build a new platform that can serve similar outcome will take long time, lots of resources, and a good care of the massive amount of data that needs to be cleaned and/or migrated.<br><br>This risk can be **mitigated** by proper analysis and planning of the work required. There will be a gradual migration to the new platform based on risk and dependency analysis. The old platform will not be decommissioned before the full migration. |
| **The cost and effort of supporting old platform with new** | L | H | M | There will be time where both platforms are in Production.<br>The **new work** should budget for both platforms for the first 2 years. |
| **Business disruption** | H | L | M | This can be mitigated by properly analysing and planning the work to eliminate dependencies or business disruptions. Product owners and different business units must be involved in such planning.<br>Also to consider what needs to migrate or piloted first based on dependencies, complexity and minimal impact to relevant business units. |
| **Compatibility of new platform with current technologies (integration wise)** | H | L | M | The analysis of the solution components, including replication technologies, will consider all relevant source systems and integration.<br>In general, new replication technologies offer a wide range of integration solutions and adapters. |
| **Dependencies on other projects (including other BC initiatives).** | H | M | M | There will be lots of initiatives, as a result of this BC as well as the on-going BAU projects that can be impacted by the new platform work or the other way around.<br>Dependency and impact **management** will be managed at program and project levels across all initiatives in the organisation. |

| | | | | |
|---|---|---|---|---|
| **Source system changes might be required** | H | L | M | Data replication from source system to the new platform might be impacted by new infrastructure (cloud platforms, network capacity, etc.), or the frequency of pulling data (realtime replication, etc.).<br>**The integration** design will consider minimal impact of the source systems and the capacity of required infrastructure without impacting other systems. The Integration strategy should be based on replicating raw data rather than curated or transformed data on the source. |

**Table 33:** Residual Risk

| Residual risk | Consequence (H/M/L) | Likelihood (H/M/L) | Assessment Rating | Mitigation |
|---|---|---|---|---|
| **The continuous behaviour of cloning and duplicating data for current and ongoing data** | H | L | M | Training, governances and principles will help keep an on-going process that promotes best practices and monitor progress and behaviours. |
| **Data management, sourcing and Replication solutions** | M | L | L | Data and integration principles will consider following the best standards.<br>There is an assumption that some replication technologies, to be selected, which can enable multiple consumption of data while on-the-move (being replicated), resulting in the reduction of data storage and duplications.<br>Also, the new platform will include a significant allowance for data quality and management tools, which can progressively and gradually extends to all source data. |
| **Data privacy** | H | M | M | In addition to the design mitigations of the privacy risk mentioned in initial risk assessment section, link, there is a high level of dependency on other initiatives (e.g. IDAM, Client consent, etc.). All dependencies will be managed at program and project levels.<br>The new platform design, on the other hand, will be flexible and adaptable if such changes happened later rather than earlier. |

**Table 34:** Introduced Risk

| Introduced risk | Consequence (H/M/L) | Likelihood (H/M/L) | Assessment Rating | Mitigation |
|---|---|---|---|---|
| **Some current business outcomes (reports, etc.), are missed for some reason** | M | L | M | The likelihood of this is very low due to the planned assessment and analysis work as well as the involvement of all impacted business units in the organisation, in the business requirement gathering phase. |

| | | | | |
|---|---|---|---|---|
| | | | | The old platform will not be commissioned until all required jobs are migrated or replaced in the new platform. |
| **Compatibility of current or new technologies with the new analytics platform** | M | L | L | All processes of selecting new technologies will consider the compatibility of technologies.<br>In general, new replication technologies offer a wide variety of integration solutions and adapters. |
| **New technology and process to learn** | M | L | L | The users of the new platform, whether staff or developers, will be trained to be able to use the new technologies and processes properly. There will be knowledge database and best practice materials. |
| **Adaptation of AI, Open data and other new concept** | M | L | M | Open data, AI and other new aspect will suddenly be enabled. The uptake of such technologies will be higher over the few next year. Leading to few risks including:<br>Number and skills of resources, allowance for best designs and practices in that area, etc.<br>On the other hand the open data will require a significant data privacy consideration.<br>The progress of such new technologies needs to be compatible with the government AI strategies, policies and code of ethics. |

### *4.3.2 Benefits*

The benefits of replacing the MSD data warehouse and establishing more robust data governance and oversight include:

- Trusted and transparent use of data.
- Known and monitored data quality, providing greater confidence in the evidence being produced to support good decision making.
- Greater system reliability and resilience.
- Smarter decision making across channels - at speed and scale.
- Flexibility to support MSD's strategic shifts and meet future demands for service innovation.
- Higher percentage of work dedicated towards value generation.
- Single client view is robust and usable for policy and operations.

## 4.4 Options considered (Economic case)

### *4.4.1 Long list of options considered*

| Option | Description | Status |
|---|---|---|
| **Option 1**<br>Rebuild<br>(Recommended) | This option, as recommended by the recent Accenture analysis, is to rebuild the data warehouse in a modern, modular, extensible, scalable way. This allows for a re-examination of capabilities against current and future requirements that will ensure the emerging platform is future proofed.<br><br>This also leads to a very clear way for the programme to decommission the older components. Across a broad range of options this represents the best value.<br><br>Key points:<br>• This option is the only one that allows MSD, OT and HUD to deliver on data warehousing requirements.<br>• This option is fully aligned with the principles outlined in MSD's Data and Analytics Strategy, IT Strategy and can provide the system requirements needed to support Te Pae Tawhiti, regardless of the target operating model. | Short listed option (Preferred) |
| **Option 2**<br>Do nothing | For this option there is near certain occurrence of at least one of the major risk identified in the immediate future:<br>• Breaches of Privacy Act and risks to public trust.<br>• Increased severity and frequency of disruptions to business operations.<br>• Failure to support digital channels.<br>• Failure to deliver products and change within reasonable timeframes within specifications.<br>Key Points:<br>• This will lead to the need for increased and significant future investment.<br>• Key failures will occur if this option is taken.<br>• This will put at risk delivery of future strategic initiatives. | Discounted |

| | | |
|---|---|---|
| **Option 3**<br>Remediate in Parallel | This approach would involve taking the current system and maintaining it, while building new functionality in parallel to replace the existing products and decommission the old ones. We would use our existing human and technical resource (including hardware and software licences) to 'build beside'.<br><br>This approach does not involve a procurement phase because it makes the assumption that current resource and capabilities are sufficient. However, there is evidence to suggest this assumption is not true as there are current practices, such as storage and automated testing, and information management that are poorly supported, or not implemented in the current architecture, and so there is a risk that many of the same problems with the current system will transfer to the parallel solution.<br><br>Key Points:<br>• Current platform software will require a major upgrade in 3 years anyway and so this solution will need further future investment to migrate.<br>• This cannot fundamentally address system design issues.<br>• This is not optimal for MSD, OT and HUD partnering to deliver.<br>• Locks in capabilities that limit future operating model and options.<br>• This does not align with the principles of flexibility and modularity in MSD Data and Analytics and IT Strategies. | Discounted |
| **Option 4**<br>Remediate in place | In this approach we take the current system 'as is' and invest in transforming it while still using it. This essentially represents an accelerated version of our current 'Do nothing' approach that is constrained by resource availability.<br><br>The observed shortcomings of this approach are: the extreme interconnectedness of the over 7 million lines of largely undocumented code means extricating particular features is time consuming and involves costly impact analysis; the inability to know the exact usage demand of many products and datasets, and we have no ability to know how they might be re-combined and used further once they leave the warehouse. The conclusion is that this is a very costly and slow approach.<br><br>**Key Points:**<br>• Has same limitations as remediating in parallel<br>• Is very costly and slow because it requires unwinding 20 years of technical debt. | Discounted |
| **Option 5**<br>Targeted Partial Remediation | This option chooses the highest risk functionality to address in a narrow scope:<br><br>• Adding data lineage to the entire existing warehouse to address some privacy concerns.<br>• Rebuild single view of client, case manager reports, and legacy tools.<br>• Rebuild task management reports.<br><br>**Key Points:**<br><br>• This partial remediation addresses no individual risk very well.<br>• Adds to technical debt and will need future investment for a long term solution. | Short listed option |

**Appendices 1 and 2 provide a more detailed analysis of these options against the risks outlined in section 4.3.**

### 4.4.2 *Shortlisted options*

To explore the options for full remediation, we conducted interviews with over 50 MSD stakeholders as well as a series of workshops both within Insights MSD and with the wider MSD business to identify and test key business outcomes for data and analytics, ensuring alignment to our various strategies. The outcomes are summarised in Figure 1:

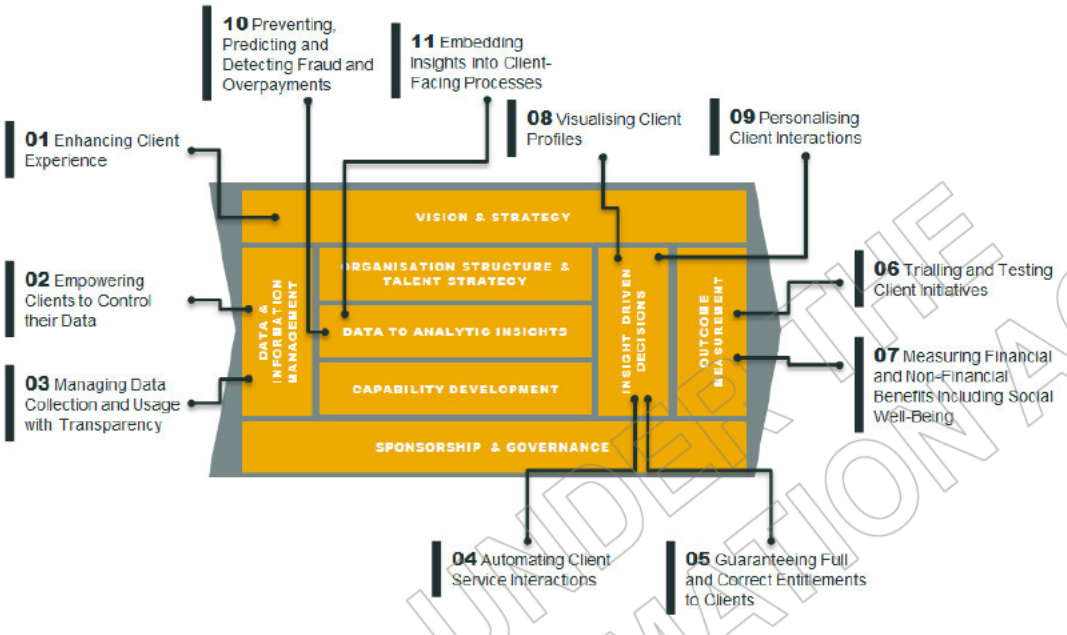



**Figure 1: Target state architecture, the outline shows components that are in scope for this bid. Note that advanced analytics products will be delivered on the platform; however these will be developed with existing teams.**

With these business outcomes as requirements Accenture developed a detailed view of a future state platform that would best deliver on MSD's objectives. This architecture is shown in Figure 2:

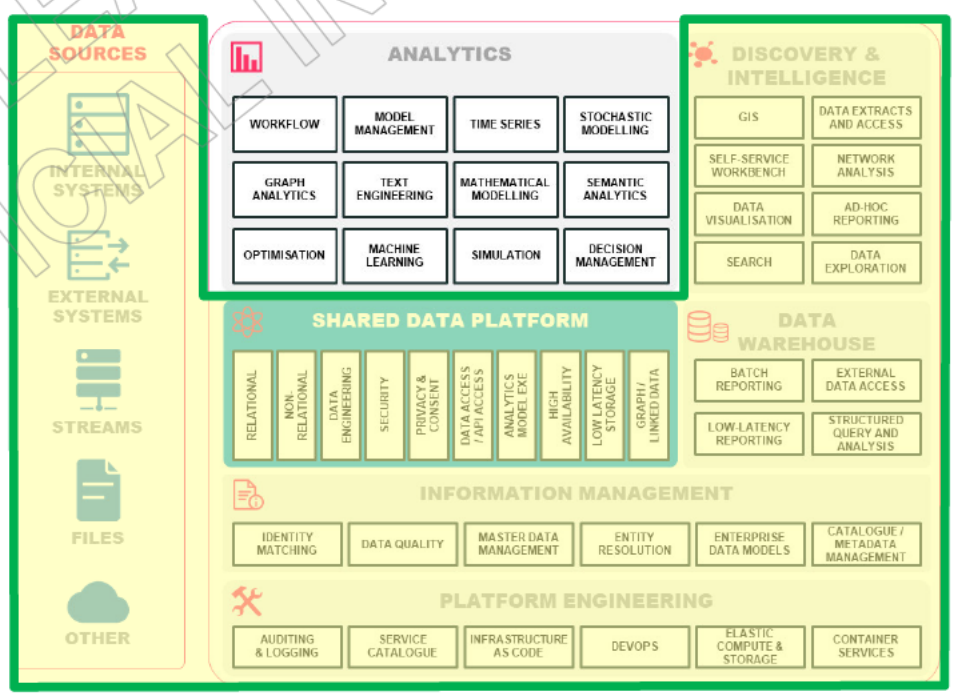



**Figure 2:** Target state architecture, the outline shows components that are in scope for this bid.

The key required components are: capturing data sources, information management, platform engineering, data warehouse, discovery and intelligence and analytics. These foundational capabilities enable a broad range of staff, client and partner outcomes to be delivered. This bid covers all the parts of the architecture except the analytics

components. It is focussed on addressing risk in a way that is consistent with modern practices and enables delivery of new value as well as existing products and services. Appendix 8 elaborates on this target state.

The preferred remediation option is rebuilding the data warehouse (See Appendix 7 for a full options analysis). The other options do not achieve all of the objectives, and, importantly, they cannot be delivered in a way that will support Te Pae Tawhiti or provide the flexibility to respond to longer term demands for system change and innovation. In every implementation of our strategic shifts and transformation, data and analytics provide key pillars of capability that are predicated on fast, accurate access and analysis of historical data that only emerge from the preferred option.

## 4.5 Delivery Plan and Procurement (Commercial Case)

### *4.5.1 Governance*

It should be noted that MSD has, in the last two years, re-organised our governance structure to include an Investment Strategy Governance committee (ISGC) responsible for endorsing high level investment decisions, and has delegated authority directly from MSD LT.

This is underpinned by a Portfolio Executive committee (PEC) that makes prioritisation decisions.

Underneath these governance groups are a more operationally focussed Data Design Authority (DDA) and a Data Management Reference Group (DMRG). The DDA and the DMRG, established in mid-2018, are specifically responsible for guiding decisions about design and implementation of data and analytics solutions, and it is these committees that will oversee the architecture and design decisions to ensure alignment to our Data and Analytics Strategy principles.

### *4.5.2 Platform Rebuild*

In addition to the mitigation options considered above in section 4.4.4, we also considered options along three other dimensions as part of the delivery plan:

- Service solution (how we partner with OT and HUD to develop the -services needed),
- Service delivery (cloud versus on-premises delivery) and,
- Implementation & Funding (how we phase and fund the delivery).

The detailed analysis of each option is in included in Appendices 3-5.

This analysis leads to the preferred set of options:

- **Mitigation Options**: Rebuild the data warehouse.
- **Service Solution**: Co-design the solution with OT and HUD, and as a further option decide on the operation and management towards the end of the 1st year of design and build.
- **Service Delivery**: Provision using Infrastructure as a Service (IAAS), Platform as a Service (PAAS) and managed services in a public cloud environment.
- **Implementation & Funding**: Using programme funding model to redesign and provision over 4 years using an "MVP and scale" approach.

The preferred scope and service delivery options will involve a formal procurement, as there are several vendors in the Market that can address these options and we do not take a view on the optimal detailed solution, preferring to let that emerge.

In the Service Solution case, however, OT and HUD are in agreement that this overall approach is agreeable.

The implementation plan revolves around designing a small minimum viable product and iterating by progressively building out data products involving design, migrate data, build phases, as shown in Figure 3:

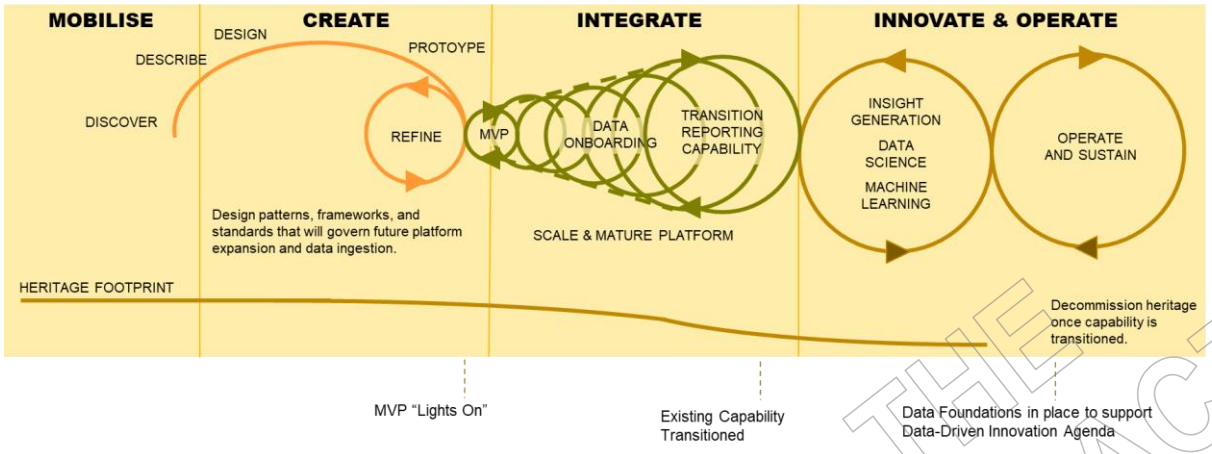



**Figure 3:** Delivery assumes developing an MVP and scaling.

This involves progressively building new products as we decommission heritage functionality. Further details of the work streams necessary to accomplish this rebuild are discussed in Appendix 7.

### *4.5.3 Partial Target Remediation*

We recently held a four day workshop with SAS in part to consider options for a partial remediation of the existing platform. In this approach we recommend selecting the top three highest risk components: an expanded data lineage across all current data assets, having a focused and dedicated work stream to decommission several key high risk products, and re-building some functionality generated by the warehouse for case management (Appendix 8 details these options).

This solution uses all our existing platform components to implement remediation, and this has consequences for delivery:

- We would **use the existing SAS based data warehouse**, noting that the current platform software will require a major upgrade in 3 years anyway and so this solution will need further future investment to migrate.
- The service delivery is **on-premises using current infrastructure** and there is a limited ability to remediate operational failures.
- This also **limits the options for partnering with OT and HUD** because the current warehouse was not designed to support the security and data access models now required. All of the options presented leave the status quo in place with respect to OT and HUD.
- **This is a "no procurement" option** and so there is a prior assumption that existing capability is fit for purpose, even though we know in some areas this is not true.

There are significant implications, principally that only some risks can be addressed, and then only in part. Additionally as we would be building onto an already complicated system, there would need significant future investment.

### 4.5.4 *Key Constraints and Dependencies*

The proposal is subject to the following constraints and dependencies.....These dependencies will be carefully monitored during the programme....

**Table 35:** Key constraints and dependencies related to the risks identified for this workstream.

| Constraints | Notes |
|---|---|
| **Client data privacy** | To untangle some of the data privacy issues, especially with old data, will add to the complexity of work. |
| **Data retention and archive policies** | At the moment there are no obvious or consistent retention or archive policies at both big data storage as well as source systems ends. |
| **Vendor lock-in** | When selecting new platforms, software and data products, it will be hard to not lock-in MSD to a vendor, especially in case of clouds or data management services. Exiting service terms need to be considered thoroughly in the contracts. |
| **Dependencies** | **Notes and Management Strategies** |
| **Dependencies on other initiatives** | There is a level of dependency on some of the initiative like IDAM, Cloud, and Privacy. |
| **The right resource availability** | To design and implement the new Analytics platform, a much specialised resources will be required. Local vendors will be more appealing, although qualification and degree of experience is very essential. |
| | |

## 4.6 Financial Case for Data Warehouse

**4.6.1 Detailed funding breakdown**

**Please provide a breakdown of the costs of this initiative**

**Data warehouse: Preferred Rebuild Option**

| ($m) | 2019/20 | 2020/21 | 2021/22 | 2022/23 |
|---|---|---|---|---|
| **Capital**<br>Capitalised labour including vendor costs | 7.0 | 8.0 | 5.5 | 1.0 |
| **Operating**<br>Software subscription | 1.5 | 1.5 | 1.5 | 1.5 |
| **Operating**<br>IaaS | 0.5 | 0.5 | 1.0 | 1.5 |

Appendix 7 gives a more detailed breakdown of the rebuild costs.

#### 4.6.1.2 *Notes for preferred option*

- **Comparison to similar efforts:** We have been in contact with data warehouse work currently in progress at IRD and ACC to assess these numbers relative to the work they are undertaking. Those data warehouses are dissimilar in nature because MSD has a very large legacy component to be

considered and has significant operational capability. Nevertheless, accounting for the differences the relative efforts involved are broadly consistent.

- **Ongoing operating expenses:** The 2022/23 numbers for software subscription and Infrastructure as a Service (IaaS) are assumed to be on-going.
- **OT and HUD:** In the preferred option OT &HUD would keep their contribution to the current data warehouse software and hardware, and shared services and this would allow those agencies to cover their cloud usage and resourcing for data and analytics. Financial arrangements could be for any shared components would have to be negotiated closer to the conclusion of the project when the exact nature of shared cloud resources would be known.
- **More details:** of the costing can be found in Appendix 7.

#### *4.6.1.2 Assumptions for Rebuild*

The assumptions in this costing for the rebuild option are:

- There are four work teams and resource profile shown in Figure 4. Note that Appendix 7 gives more details of the team structure and rates.
- The work would start November 2019. From July to October there is project preparation with a lower FTE footprint. Project establishment activities such as procurement, acquiring office space, and on-boarding would run during this time.
- Building analytics products is outside the scope of this bid and that existing baseline teams will do that work. This bid just sets up the platform and the data infrastructure to support the data products.
- The training costs for existing staff onto the new platform are not included
- The costs for running the procurement process are supported by the staff on-boarded in the July-Sep time period e.g. the Project Manager, Architects and Leads.
- The costs needed for changing MSD systems to allow any integration are not included
- The initial use of the cloud resources and software subscription (2019) costs is currently provided by Accenture as a best estimate based on available information, with the caveat that they have not done a usage review of our systems. Work is on-going to validate these numbers by refining a needs analysis of current deliverables, and by validating externally.
- Cloud usage grows over the project life as data is migrated, and thereafter at 10% per year.
- That MSD is “cloud ready” i.e. the capability exists to consume cloud services during the development, and that we develop capability to monitor and manage these services long term
- That MSD decommissions the existing data warehouse at the conclusion of the rebuild

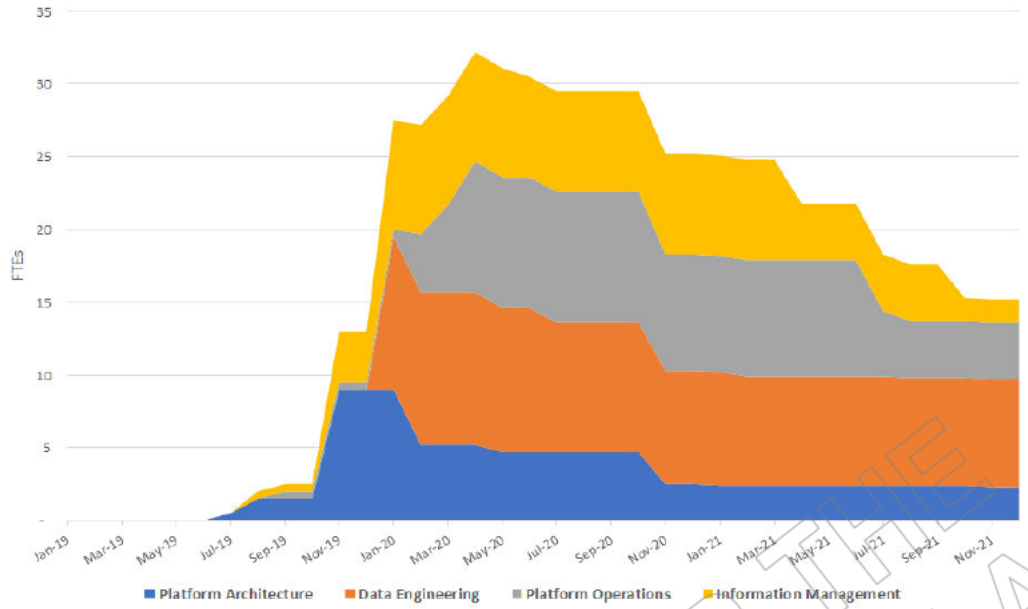



**Figure 4:** Resource profile for work teams to implement the rebuild option.

| 4.6.2 Detailed funding breakdown | |
|---|---|
| **Please provide a breakdown of the costs of this initiative** | **Data warehouse: Partial Targeted Remediation Option** |

| ($m) | 2019/20 | 2020/21 | 2021/22 | 2022/23 |
|---|---|---|---|---|
| **Capital**<br>Capitalised labour including vendor costs | 3.5 | 5 | 5 | 1.5 |
| **Capital**<br>Software subscription | | | | |
| **Operating**<br>IaaS | | | | |

#### *4.6.2.1 Notes for partial targeted remediation*

- **Scope:** The cost here assumes we implement the top 3 remediation priorities.
- **OT & HUD:** In this option OT & HUD current funding arrangements would stay in place

#### *4.6.2.2 Assumptions for Partial Remediation*

- No change in technology capability – continue to use current on-premises SAS analytics platform

# 5. Digital Capability

## 5.1 The case for scaling the Ministry's Digital Architecture

Client demand for MSD's digital services is set to double over the next two years. We know the number of clients who connect with us online is increasing significantly (currently growing at up to 1,000 new MyMSD users per day), and we know the frequency of client online interactions with us is also increasing. In other words, more clients are demanding to use our online services, and they are demanding to use these services more and more regularly.

We know that our digital platforms were not built to cope with this new load, and they will not be able to support the complexity of transactions we need to provide our clients with at these new demand levels. All of these factors mean that the current MSD online platform is not sized or architected correctly to deliver services at this new level, and is likely to fail under these steadily increasing loads.

Given we already have 650,000 clients registered in our digital channels, we know the effects of failure and disruption in our online channel would be major and widespread, with severe implications for both the Ministry and for all of our clients who use this channel.

The Ministry's digital architecture is in this position because it has emerged over a number of years from a series of short-term tactical decisions. These decisions were constrained each time by technology limitations, time, and cost, which have resulted in a now complex architecture.

The piecemeal build of the Ministry's straight-through processing has meant that there are high volumes of manual tasks being generated from client online applications. It has already resulted in high volumes of laborious and repetitive manual work for staff, and it has meant long delays for client applications to be processed. These problems and wait times will increase to critical levels under the predicted future loads. The straight-through processing implementation, and the Ministry staff impacted by it, will be unable to cope with these higher levels.

Because of all of these factors, urgent investment is required now; to increase the scalability of the digital architecture to handle the demand we know is coming, as well as to remediate the straight-through processing issues we already have and we know will fail with an increased transaction load.



## 5.2 Background

The Ministry's client-facing digital architecture has emerged over a number of years from a series of short-term decisions. These decisions were constrained each time by technology limitations, time, and cost; resulting in a now complex architecture.

Significant decision points which led to today's digital channel architecture are described below:

- 2013 - When Cúram UA (Universal Access) was originally deployed as part of the Enhanced Online Services (EOS) project, our Client Management System (CMS) was not yet the master of client records (prior to the Single CMS project completing), and CMS had not been upgraded to a compatible software version. EOS was consequently deployed as a stand-alone Cúram instance, requiring additional effort and complexity, and bespoke integration between EOS and CMS. The on-going cost of change of the Cúram platform is significant, and introduced client experience constraints which resulted in low client uptake.
- 2015 - Under the Simplification programme, significant improvements were made to the digital channel with the introduction of MyMSD. MyMSD was delivered as a solution to enable mobile-friendly self-service for clients (which was not possible at the time with Cúram Universal Access). Tactical decisions were made as to sub-software components which prevent the MyMSD application to scale. It was initially an agile and light-weight application, but over time it has grown to become a larger and increasingly complex application.

- 2015 - Tactical process management technology was delivered to enable partial automation and straight through processing of client online applications. As a consequence, Ministry staff are required to interact with 3 separate workflow tools; Straight to Processing (S2P), IBM Business Process Manager (BPM), and IBM Cúram.
- 2018 – The availability of a number of critical functions in MyMSD was increased through the introduction of the Connect360 Operational Data Store, delivered by the Availability programme.
- 2018 – The Ministry's current "MyMSD" digital experience is built on the integration between the MyMSD and Cúram UA applications.

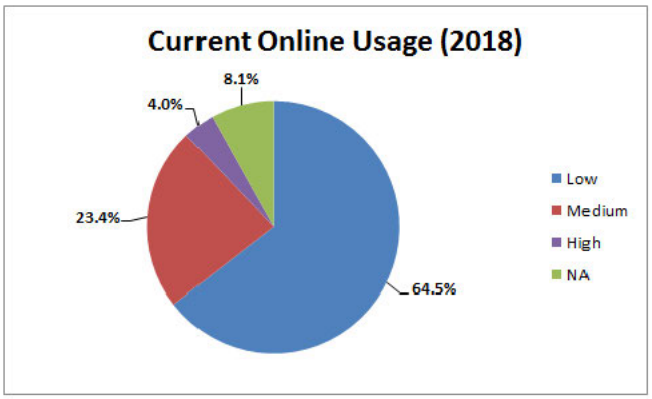
The Ministry's implementation of straight-through processing has been piecemeal over the years and suffers from a number of inefficiencies. This creates barriers to the Ministry automating the straight-through processing of client online applications and leads to delays and a poor experience for clients. As an example, 50% of the Ministry's top 10 Seniors online applications were not completed within timeliness standards in 2017.

Client online applications intended for automated straight-through processing frequently generate a high number of exceptions. These exceptions generate manual tasks which require staff to take action before the application can continue in its submission. Because staff struggle to keep up with the high workload, this commonly results in manual tasks sitting in queues for long wait times before they are seen by staff. The task management solution also allows tasks to be frequently re-queued, and worked on by different staff members, causing a significant amount context switching and rework to take place.

The Ministry forecasts client demand for medium usage of digital services to grow significantly over the next two years. Without including the growth of additional clients using the Ministry's digital channels, medium usage is expected to double over the next two years. The majority of this growth is expected to be driven through a high conversion rate of low users (less than 20% done online) to medium users (more than 20% but less than 60% done online).

**Table 36:** MSD Current and Forecasted Client Online Usage

| Client Online Usage | Client Online Usage Description | 2018 Actuals | | 2020 Forecast | |
|---|---|---|---|---|---|
| | | Volumes | % | Volumes | % |
| **Low** | Less than 20% done online | 183,672 | 64.5% | 128,178 | 45% |
| **Medium** | More than 20% but less than 60% done online | 66,576 | 23.4% | **113,936** | **40%** |
| **High** | More than 60% done online | 11,401 | 4.0% | **28,484** | **10%** |
| **N/A** | No engagements that could have been done online | 23,190 | 8.1% | 14,242 | 5% |
| | | 284,839 | 100% | 284,839 | 100% |



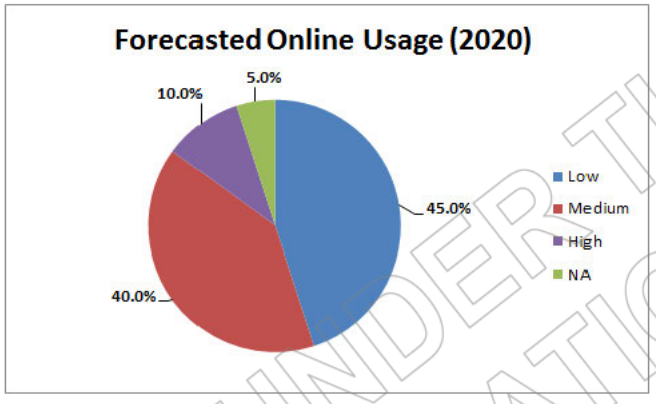




**Figure 5:** MSD Current and Forecasted Client Online Usage

## 5.3 Risks and Benefits

### *5.3.1 Risks*

The current complexity of the digital channel and straight-through processing architecture means there is:

- A significant risk that the Ministry's client-facing digital channels and straight-though processing will not be able to meet increasing client online demand over the next two years
- An increasing risk of failure of the Ministry's client-facing digital channels
- A high cost to maintain and support the Ministry's client-facing digital channels
- A high cost to introduce business changes to the Ministry's client-facing digital channels

***Initial risk analysis***

This section outlines the main risks that have been identified for this work stream. They are examined in terms of the seriousness of their consequence as well as their likelihood. Risk management and mitigation strategies are also outlined for each of these risks.

**Table 37:** Main Risks

| Main Risks | Consequence (H/M/L) | Likelihood (H/M/L) | Comments and Risk Management Strategies |
|---|---|---|---|
| **The Ministry's digital architecture may not scale to meet future client online demand** | H | H | Will be mitigated through increasing scalability of:<br>• Digital channel architecture, and;<br>• Straight-through processing architecture |

A risk register has been developed and will be progressively updated as more detailed analysis is undertaken.

### *Risks from Change*

The tables below deal with the risks of the preferred investment option. Specifically it examines the execution risk which looks at risk associated with doing the work, the residual risks that will be leftover once the work is complete – and any introduced risk that would be created as part of doing this work. It also looks at any mitigations that may be implemented to lessen the effect or consequence of any of these risks becoming material issues that require remediation.

**Table 38:** Execution Risk

| Execution risk | Consequence (H/M/L) | Likelihood (H/M/L) | Assessment Rating | Mitigation |
|---|---|---|---|---|
| **There may be insufficient skilled resources available to meet delivery needs resulting in a longer delivery timeline.** | M | M | M | Early program resourcing strategy and planning |
| **There may be competing Ministry priorities, resulting in delays to access key delivery resources (people, technical environments, etc.), resulting in a longer delivery timeline.** | M | M | M | Portfolio governance to manage escalations of constrained resources |

**Table 39:** Residual Risk

| Residual risk | Consequence (H/M/L) | Likelihood (H/M/L) | Assessment Rating | Mitigation |
|---|---|---|---|---|
| **The Ministry's digital architecture may not scale to meet future client online demand.** | H | L | M | Will need to maintain continued investment in digital architecture to ensure on-going ability to keep pace with future client online demand. |

**Table 40:** Introduced Risk

| Introduced risk | Consequence (H/M/L) | Likelihood (H/M/L) | Assessment Rating | Mitigation |
|---|---|---|---|---|
| **System defects and/or failures may be introduced to the Ministry's digital architecture from programme system changes, resulting in partial or complete loss of client online services.** | H | L | M | Will be managed throughout program delivery by project / risk management and test management practices. |

### 5.3.2 *Benefits*

The benefits of increasing the scalability of the Ministry's digital channel and straight-through processing architecture are:

- The Ministry's digital channels will be able to scale to meet the increasing client online demand over the next two years:
    - Channel choice is a critical enabler to improving service culture; continued investment in our digital channels will mean more and more clients will be able to get support through the channel that works best for them
    - Moving high volume transactions to digital channels enables Ministry staff to further concentrate resources on active case management, and other interventions to help clients achieve sustainable employment and positive social outcomes
- The Ministry's digital channels will be architected to accommodate further growth in client online demand in the future
- Reduced risk of failure of the Ministry's client-facing digital channels
- Reduced costs to introduce future business changes to the Ministry's client-facing digital channels
- Reduced bottlenecks and delays in straight-through processing of client online applications
- Increased alignment with vendor best-practice / reference architecture for architecture deployment

## 5.4 Options considered (Economic case)

### 5.4.1 *Long list of options considered*

| Option | Description | Status |
|---|---|---|
| **Option 1**<br>Do nothing | This option would require the Ministry's digital channel architecture to cope with twice the volume of client online usage it was architected for. This would lead to certain degraded performance and **probable failure of the Ministry's digital channels**.<br><br>This option is not viable because of the severe impact this would have on clients and the fact that the Ministry is committed to making more transactions available online through digital channels. | Discounted |
| **Option 2**<br>Defer for 12 months | This option would require the Ministry's digital channel architecture to cope with a greater volume of client online usage than it was architected for. This would lead to probable degraded performance and **an increasing probability of failure of the Ministry's digital channels**.<br><br>This option is not preferred because the risk of failure is increasing and continues to be high. | Discounted |
| **Option 3**<br>Increase Scalability of Digital Channels | This option concentrates on increasing the scalability of the digital channel architecture which provides the MyMSD digital experience to clients. This will allow the digital channel architecture to cope with the increased usage.<br><br>This option is not preferred because it would not resolve key bottlenecks in the Ministry's straight-through processing implementation, causing **certain delays and probable failure in straight-through processing of client online applications.** | Short-listed Option |

| | | |
|---|---|---|
| **Option 4**<br>Increase Scalability of Digital Channels and Straight-through Processing | This option includes all of the initiatives described in the **Increase Scalability of Digital Channels** short listed option. In addition, this option also includes resolving key bottlenecks in the Ministry's straight-through processing architecture.<br><br>This option is preferred because it will enable the Ministry to scale to twice the number of online usage over the next two years and be better positioned for continued growth of digital clients. | Short-listed Option (Preferred) |

### *5.4.2 Shortlisted options*

***Option 3:** Increase Scalability of Digital Channels*

This option concentrates on increasing the scalability of the channel architecture which provides the MyMSD digital experience to clients. It consists of two key components which are described in more detail in this section.

*Scalable MyMSD Architecture*

The complexity of MyMSD system will be reduced to enable it to become sufficiently scalable and agile enough to cope with the increasing client demand over the next two years.

This will be accomplished by making the following architecture changes to MyMSD:

- Transforming MyMSD to become Cloud Native; to remove barriers to scalability and increase flexibility and portability to any Cloud Service Provider
- Transforming the MyMSD application to become stateless; to enable horizontal scaling of the application
- Replatforming the MyMSD database to a high performance database; to enable scaling to a higher throughput of read and write database transactions
- Moving MyMSD to the New Zealand Government Container-as-a-Service offering
- Enabling Continuous Integration / Continuous Delivery (CI/CD) software development tooling to enable faster delivery of business change

*Scalable Cúram Universal Access Architecture*

The complexity of the IBM Cúram Universal Access (UA) architecture deployment will be reduced by aligning it with IBM's recommended reference architecture and best-practices. This will result in a simplified and more scalable architecture which will enable a lower cost of change.

The Ministry's client-facing Cúram architecture currently consists of a client-facing UA component connected to a heavy-weight Enhanced Online Service (EOS) instance of Cúram. The EOS Cúram instance requires bespoke integration with the Ministry's staff-facing Client Management System (CMS) instance of Cúram in order to synchronise client data.

This work will enable UA application to be connected directly to the CMS instance of Cúram. The heavy-weight EOS instance of Cúram will be decommissioned, and the existing bespoke integration between EOS and CMS will be decommissioned.