



Te Tari Taiwhenua Internal Affairs

Facial Recognition Services Business Case

Prepared by:	Frances Skilton & Lisa Buchan
Prepared for:	Russell Burnard, Service Delivery and Operations
Date:	12 September 2018
Version:	1.1
Status:	FINAL
Security Classification:	IN CONFIDENCE

Released under the Official Information Act 1982

Facial Recognition Services Business Case

Document Control

Document Information

Position	
Document ID	FR Business Case v1.1
Document Owner	Russell Burnard, Service Delivery & Operations
Issue Date	12 September 2018
Last Saved Date	9 October 2018
File Name	FR Business Case v1.1 12 September 2018

Document History










Version	Issue Date	Changes
0.1	3 August 2018	Initial outline and draft of strategic, economic and commercial cases for review by project team.
0.2	9 August 2018	Updated investment objectives and economic case with the assumptions and targets from the benefit analysis, incorporated feedback from FR project team, incorporated management case, incorporated financial case, incorporated updated CBA with benefits included, updated ILM and BMP.
0.3	14 August 2018	Incorporated FR Project Team feedback, particularly on the Management Case, added passports forecast data, updated CBA information and updated figures.
0.41	21 August 2018	Updated with feedback from Project Executive and SDO executives; Russell Burnard, Jeff Montgomery, David Philp, John Crawford Smith, Darren Godden & Te Ara Manaaki team, Barbara McCallum, Greg Archer, Nick Athea. Key changes; clarify and update investment objectives, Exec summary; clarify consequences of not replacing system, clarify options considered and ongoing opex cost. Still pending opex/capex split options, decision by project exec on clash with TAM and Uruwhenua delivery times, updated aspirational option costs and approvals text.
0.51	5 September 2018	Updated with Corporate Centre Clinic feedback. Key changes; verified that the preferred supplier's proposed data centre is compliant with security and privacy requirements for NZ govt, explained current system value, consequences of failure and how risk is currently managed, updated risk mitigation for software vendor viability and multiple project management risk, updated financials with aspirational option and capex opex split adjustment.
1.0	7 September 2018	Updated with final approvals and next steps detail.
1.1	12 September 2018	Final correction of the Cost Benefit detail for Option 3 and Assessment Period description. Addendum 1 included.

Document Review




Role	Name	Review Status
Project Manager	Antonia Aloe	
Facial Recognition Project Team	Esther Williams Peter Campbell Gerard Harris Jenny Zhang Lee Cook Sirshen Naik Stephen Sanders Jessica Trang	

Released under the Official Information Act 1982

Document Approval

Submitted by	Signature	Date
<p>Antonia Aloe Senior Project Manager <i>I confirm that the project can be successfully delivered.</i></p>		12/09/2018
Recommended for authorisation by	Signature	Date
<p>Deanna Hughes Manager Project Delivery SDO <i>I confirm that the project can be successfully delivered.</i></p>		13/9/18
<p>Jenny Livschitz Manager Financial Planning and Performance <i>I confirm that the budget estimate is an accurate and reliable assessment of the funding needs for this project.</i></p>		13/9/18
<p>Sirshen Naik SDO Finance Business Partner <i>I confirm that the business group has the on-going operating expenditure to support the capital spend throughout the project and beyond.</i></p>		13/9/18
<p>Arun Patel Acting Chief Financial Officer <i>I confirm that the business group has the on-going operating expenditure to support the capital spend throughout the project and beyond.</i></p>	 subject to passport fee renew	13/9/18
<p>Nick Athea Chief Portfolio Manager <i>I confirm that the budget request is included in the current portfolio plan and that the proposed approach meets Departmental assurance requirements.</i></p>		13/9/18
<p>Barbara McCallum Manager Commercial Services <i>I confirm that the procurement approach is robust and achievable.</i></p>		13.09.18
<p>Murray Davey Acting CIO <i>I confirm that the preferred option is an appropriate technology solution to realise the business outcomes and suitably aligns to DIA's information technology strategy.</i></p>		14/09/18
<p>Russell Burnard Project Executive/ Senior Responsible Owner <i>I confirm that the project fits with Business Strategy, will deliver the defined benefits and that the business case has addressed all risks and issues associated with the</i></p>		12/9/18

project.

Authorisation by	Signature	Date
<p>Maria Robertson DCE, Service Delivery and Operations, Department of Internal Affairs</p> <p><i>I confirm the business case aligns to Branch and Departmental Strategies and that funding can be provided from within the Branch. I authorise the business case to proceed to IGC.</i></p>		14/9/18
<p>Marilyn Little Investment Governance Committee (Deputy Chair), Department of Internal Affairs</p> <p><i>I confirm the business case has fully addressed all risks and issues, financial viability and aligns with Departmental strategy.</i></p>		24/9/18
<p>Peter Murray Chief Executive, Department of Internal Affairs</p> <p><i>I confirm the business case has fully addressed all risks and issues, financial viability and aligns with Departmental strategy.</i></p>		28/9/18

Approval Request

This business case seeks formal approval to:

- **Approve** investment of one off capital of up to \$2.15 million in 2018/19 and up to \$3.85 million in 2019/20;
- **Approve** investment of one off operating expenditure of \$0.36m for 2018/19 and \$0.14m in 2019/20 to replace the current facial recognition software which is no longer supported;
- **Approve** investment of ongoing operating expenditure of \$3.92m (including Depreciation and Capital Charge of \$0.89m) per annum to ensure DIA can continue reliable and secure production of passports;
- **Endorse** the project finalising the contract for the syndicated procurement of Facial Recognition Services in line with the costs approved above;
- **Note** that in the event the scope or cost of the final contract changes materially, the project team will present the new contract and memo to the Investment Governance Committee for endorsement prior to being tabled with the Minister of Internal Affairs for approval; and
- **Note** that operating expenditure for this investment will be funded from the Passports Memorandum Account; and
- **Note** whole of life cost for the project is \$24.60m.

Contents

Approval Request	vi
Executive Summary	1
Introduction	8
Background	9
The Strategic Case – Making the Case for Change	10
Strategic context	10
Investment objectives, existing arrangements and business needs	14
The reasons for this investment	17
Potential business scope and key service requirements	17
Main benefits	19
Main risks	20
Key constraints, dependencies and related projects	23
The Economic Case – Exploring the Preferred Way Forward	24
Critical success factors	24
Long-list options and initial options assessment	25
The short-listed options	25
Economic assessment of the short-listed options	25
Commercial Case - Preparing for the Potential Deal	32
Background	32
Market summary	32
The New Zealand Government market for facial recognition technology	33
Procurement process	34
Business requirements	36
The preferred supplier	38
Commercial risks	39
Pricing and payment mechanisms	39
Contractual and other issues	40
Financial Case – Affordability and Funding Requirements	42
Financial Summary	42
Financial Modelling	42
Sensitivity Analysis	43
Management Case – Planning for Successful Delivery	44
Project management planning	44
Change management planning	52
Benefits management planning	56
Risk management planning	56
Project and business assurance arrangements	59
Post-project evaluation planning	60
Next Steps	61
Appendix A: Chief Executive’s Letter	62
Appendix B: Glossary of Terms and Abbreviations	64
Appendix C: High-level principles and requirements for the facial recognition service	66
Appendix D: Privacy Assessment	70

Appendix E: DIA outcomes framework	77
Appendix F: ILM and Benefit Management Plan	78
Appendix G: Facial Recognition Risks and Uncertainties	80
Appendix H: Presentation of the Long-list Options Assessment	83
Appendix I: Detailed Economic and Financial Data	90
Appendix J: Supplier overview	93
Appendix K: DIA and Other Agency Use of Facial Recognition Services	96
Appendix L: Commercial Case details	98
Appendix M: Facial Recognition Service Requirements	101
Appendix N: Project Team Bios	116
Appendix O: Best Practices derived from Lessons learned	118
Appendix P: Facial Recognition Replacement Project Stages	120
Appendix Q: List of Assurance Activities	124
Addendum 1: Responses to State Services Commission feedback	128

Index of Tables

Table 1. Cost Benefit Comparison of Options	4
Table 2. Project Cost Summary – preferred option & supplier	4
Table 3. Major risks for the Facial Recognition Replacement Project	7
Table 4. Facial Recognition Replacement Project alignment with government principles and goals	12
Table 5. Facial Recognition Replacement Project alignment with DIA priorities	13
Table 6. Scope of the Facial Recognition Replacement Project	18
Table 7. Analysis of potential benefits that can be expressed in monetary terms	19
Table 8. Analysis of potential benefits that cannot be reliably expressed in monetary terms	20
Table 9. Risks discussed in each section of the business case	21
Table 10. Uncertainty risks with potential impacts on the Facial Recognition Replacement Project	21
Table 11. Key constraints and related projects	23
Table 12. Facial Recognition Replacement critical success factors used to assess options	24
Table 13. Processing time for facial recognition exceptions	26
Table 14. Current and predicted rates of facial recognition exceptions for passport applications	27
Table 15. Facial recognition processing time improvements	27
Table 16. Facial Recognition short list analysis summary	28
Table 17. Facial Recognition options cost benefit analysis results	30
Table 18. Facial Recognition technology software vendors and system integration suppliers	33
Table 19. Suppliers that responded to the RFP	34
Table 20. The cross-functional team responsible for the RFP / BAFO evaluation panel	35
Table 21. Results of the supplier evaluation at the end of the Best and Final Offer (BAFO) stage	36
Table 22. Service Requirements	36
Table 23. Assets Acquired and Replaced	37
Table 24. Contract risk allocation	39
Table 25. Key terms of the Master Syndicated Agreement	41
Table 26. Financial summary of the Facial Recognition Replacement	42
Table 27. Total project cost breakdown	43
Table 28. Life Events and Identity Services Key Board members	47

Table 29. Facial Recognition Replacement Project roles and responsibilities	48
Table 30. Facial Recognition Replacement Project key milestones	51
Table 31. Facial Recognition Replacement Project change impacts	53
Table 32. Key risks to delivery for the Facial Recognition Replacement Project	57
Table 33. Facial Recognition Replacement Project issues	59
Table 34. Key Assurance Activities	59
Table 35. Facial recognition services included in scope long list options	84
Table 36. Summary of scope options	85
Table 37. Summary of Solution Options	86
Table 38. Summary of Delivery Options	88

Index of Figures

Figure 1. Automated verification of passport photo	1
Figure 2. Checking a face does not have a duplicate in the system	1
Figure 3. Facial Recognition Replacement Project implementation timeline	5
Figure 4. Automated verification of passport photo	14
Figure 5. Checking a face does not have a duplicate in the system	15
Figure 6. Facial Recognition Scope of Replacement	16
Figure 7. Facial Recognition Replacement Project benefits and KPIs	19
Figure 8. Life Events and Identity Services Board Scope	45
Figure 9. Project delivery, governance and quality assurance structure	46
Figure 10. Facial Recognition Replacement Project approach and timeline	50
Figure 11. Current facial recognition components	55
Figure 12. Proposed future state architecture for facial recognition in passports	55

Executive Summary

Background

The DIA facial recognition system is an essential step in the current passport processing system.

When an application is received to renew a passport, the facial recognition system automatically checks the submitted photo against the previous passport photo to ensure the person is the same. This **verification** capability has significantly reduced the amount of labour required, with only 25% of renewals requiring a manual check when the system cannot provide the required certainty level. Figure 1 shows a demonstration of this capability¹.

Figure 1. Automated verification of passport photo

9(2)(a)



When an application is received for a new adult passport, the facial recognition system checks the submitted photo against nearly four million existing passport photos to ensure that the application is not an attempt to create a duplicate identity (see Figure 2)

This identification capability has prevented criminals and terrorists from obtaining valid but fraudulent passports. Before this capability was introduced, up to forty duplicate passport applications were intercepted each year.

9(2)(a)

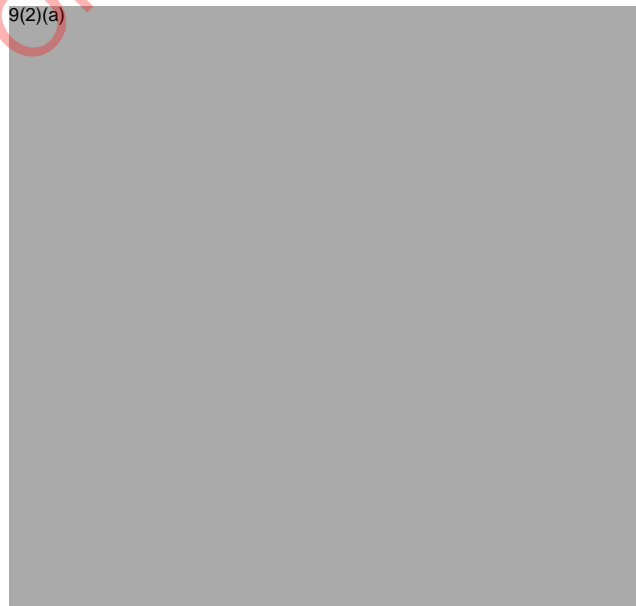


Figure 2. Checking a face does not have a duplicate in the system

¹ Note that the faces used for Figures 1 and 2 are examples provided by the system vendor.



If a suspicious passport application is received, DIA investigates further using a specialist team. This team also assists other agencies with their investigative activities by providing specialist knowledge around identity systems enabling the correct identification and confirmation of individual identities 9(2)(k)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Damian Christopher Gillard was caught by facial recognition technology used in data matching checks to ensure passport details match the identity of the person in the photograph².

Strategic Case

The global market for biometric solutions is growing rapidly, and has recently undergone a period of acquisition and rationalisation. As a result, the software vendor that provides the current facial recognition system was acquired and the software is no longer supported in New Zealand. The local integrator and provider of the software is doing their best to keep the system stable, but cannot commit to service levels, and they have no legal authority to update the facial recognition software if upgrades or expansion are required. The immediate consequences of a failure of the Facial Recognition system would be a growing backlog of adult passport renewals until the system is restored, or for longer term failure, until additional staff could be brought in to reduce the backlog. Another consequence would be that fraudulent passport applications could not be detected until facial recognition identification services were restored.

The current risk is being managed by having the current facial recognition system on a separate server to the main passports system. The facial recognition system server is under a change freeze to prevent upgrades that could cause failure of the facial recognition system.

The key problem to be addressed by the facial recognition replacement project is to reduce the risk of facial recognition system failure. A secondary issue that will be solved by the replacement programme is the inability to upgrade the current system to make improvements to accuracy and fraud detection, since the technology used by criminals is developing rapidly.

² https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11252563

Resolving these problems would result in the following benefits:

1. Maintain the Integrity of the passport system and meet the service levels required by the business
2. Improved efficiency as a result of more accurate algorithms for facial recognition
3. Maintain DIA's ability to contribute to public safety by detecting fraudulent passport applications.

The measurable investment objectives set for the project were:

1. Improve contracted service levels from 'best efforts' to 99.5% availability and 24-hour recovery time by April 2020
2. Reduce the hours spent on facial recognition tasks per 10,000 adult passports from 333 to 55 by April 2021, and reduce the hours spent on facial recognition tasks per 10,000 adult passport renewals from 78 to 56 by April 2021
3. Improve the ability to detect fraud as measured by audits of test samples from 96% completing as expected to 99% completing as expected by December 2020.

The overall productivity savings are expected to be between 2,000 – 4,000 hours per year, depending on the volume of passport applications.

Economic Case

Costing of a replacement service showed a significant investment would be required. A thorough review of options was undertaken to ensure all alternatives had been considered, including returning to manual operation and sharing other agencies current systems. These were discounted as not feasible. The shortlisted options were:

1. **Do nothing.** Continue the current system beyond 2021. This would jeopardise the whole passport process, creating a high risk of failure, and was discounted.
2. **Do Minimum, reduce scope** by eliminating the ability to check for a duplicate identity. This would halve the whole of life cost of the facial recognition service, but would create a fraud vulnerability that could harm NZ's passport reputation by creating an avenue for criminals to launder money and sell valid but fraudulent New Zealand passports.
3. **Preferred - Replacement** with a similar scope of service using modern software. This option meets the business requirements and fits with Te Ara Manaaki goals by creating a common capability. It was the best value for money option that reduces business risk to acceptable levels. This was the preferred option.
4. **Aspirational option** using artificial intelligence to enhance accuracy and further improve fraud detection. This option was unable to be supplied by the market in the timeframe required, and would be considerably more expensive, with unknown accuracy improvements.

Table 1 shows the cost benefit analysis for the options considered.

Table 1. Cost Benefit Comparison of Options

	Option 1: Do Nothing	Option 2: Do Minimum – reduce scope	Option 3: Preferred - replace	Option 4: Aspirational (AI)
Appraisal Period (years)	12.5 years	12.5 years	12.5 years	12.5 years
Capital Costs	-	\$6.6m	\$6.0m	\$11.2m
Whole of life costs	\$0.8m - \$1.0m	\$10.7m - \$13.8m	\$21.9m – \$27.4m	\$43.1m - \$53.8m
Present Value of monetary benefits	-	-	\$0.6m	-
Present Value of costs	(\$0.9m)	(\$12.2m)	(\$24.6m)	(\$48.5m)
Net present value (NPV)	(\$0.9m)	(\$12.2m)	(\$24.0m)	(\$47.8m)
NPV rank (out of 4)	1	2	3	4

Commercial Case

An initial approach to the market resulted in two vendors who could meet DIA’s passport process requirements. DXC was selected by the panel as representing the best value for money, since it delivers significant accuracy improvements over the other respondent for a similar whole of life cost, as well as representing the best organisational capability and capacity to deliver.

Within DIA, the new Facial Recognition Service can be used as a common capability for Citizenship applications and identity services. Outside DIA, other agencies such as NZ Police and the Immigration service of the Ministry of Business Innovation and Employment currently use facial recognition capability, but have contracts that prevent DIA accessing their services. There is interest in using a shared service once their contracts expire.

Financial Case

Table 2 shows a breakdown of capital and operating costs for the design and implementation project.

Table 2. Project Cost Summary – preferred option & supplier

\$'m	FY18/19	FY19/20	All Years
	Forecast	Forecast	Total Budget Required
Opex	0.358	0.142	0.500
Capex	2.147	3.853	6.000
Total	2.505	3.995	6.500

The \$2.147m of Capex for FY18/19 is already included in DIA capital forecasts for FY18/19 and is therefore funded out of the current DIA capital budget. The \$3.853m of additional Capex for FY19/20 is within what was signalled during the initial capital planning round and will be funded out of DIA’s

capital budget for FY19/20. The Capex forecasts in FY18/19 and FY19/20 include a contingency of \$1.074m.

The \$0.358m of Opex for FY18/19 and \$0.142m of Opex in FY19/20 will be funded from the Passports Memorandum account. The Opex forecasts in FY18/19 and FY19/20 include a contingency of \$0.068m.

Ongoing costs for the preferred option are an average of \$3.917m per annum post implementation (including Depreciation and Capital Charge of \$0.891m per annum). Offsetting this increase are expected benefits of \$0.094m in FY20/21 and an average of \$0.111m per year thereafter.

As these ongoing costs relate to the provision of the Passports service, they will be funded from the Passports Memorandum Account. Periodic fee reviews are conducted on the memorandum account to ensure that fees charged recover costs over the medium to longer term. The next fee review is due for Cabinet consideration in November 2018.

Whole of Life Costs for the Project are \$24.605m, and therefore outside of the Department's delegated authority to approve. Approval by the Minister is required.

A quantitative risk analysis was completed which showed that the project cost estimate of \$6.43m was \$0.07m short of the 85% percentile, so a contingency of \$0.070m has been added to make the project cost \$6.5m.

Management Case

The project will be governed by the existing Life Events and Identity Services governance board within the Service Delivery and Operations (SDO) branch of DIA. The scope of this board includes all inter-related projects and programmes within SDO.

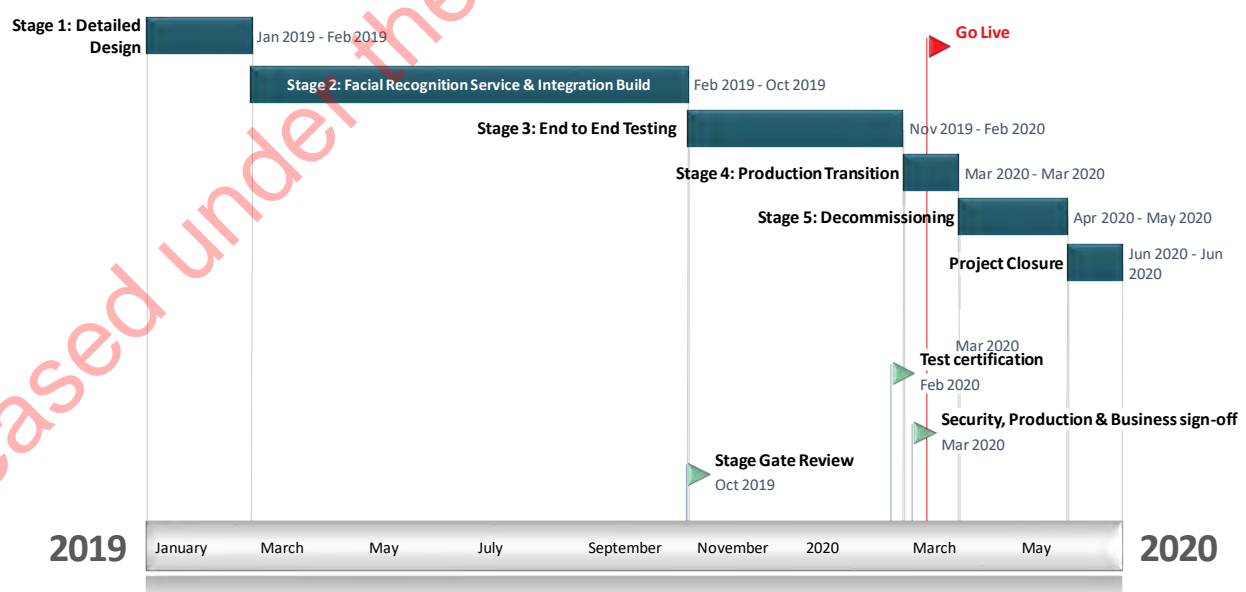


Figure 3. Facial Recognition Replacement Project implementation timeline

The timeline for delivery is shown in Figure 3.

The risk profile assessment showed a medium level of risk, due to the minimal change experienced by users, lack of external customer impact, and proven technology. No risks were identified that would exceed DIA risk thresholds. The major risks that remain are shown in Table 3.

Released under the Official Information Act 1982

Table 3. Major risks for the Facial Recognition Replacement Project

Type	Risk	Mitigation
Management	Te Ara Manaaki is a major transformation programme that will be delivering over a similar timeframe to the Facial Recognition Project and the Uruwhenua 2020 Passport Personalisation project, and the wider Identity Services Portfolio	The changes to be delivered by the projects will be planned, scheduled and coordinated. The SDO Capital Plan & Te Ara Manaaki Dependency Map will be reviewed and updated regularly through the course of the projects
Commercial	Software vendor viability - the current solution was retired after a competitor buyout. The market has been consolidating over the last few years.	Complete due diligence as a part of procurement process. Contract provision for insolvency or acquisition in contract including step-in rights, ability to terminate the contract and establishing an agreed succession plan ³ .

Next Steps

Upon approval of the business case the key next steps include:

- finalise contract negotiations
- commence project implementation (subject to approvals).

³ During contract negotiations, escrow rights will also be sought

Introduction

DIA is a world leader in identity verification and issuing secure passports. Facial Recognition (FR) software is a cornerstone of the automated rules processing in the Passports System. The current facial recognition system enables the:

- matching of first time passport applicants against the image database to ensure they do not have a passport under a different identity ('one-to-many' matching)⁴.
- streamlining of low risk passport renewal applications by verifying the old passport photo with the new one ('one-to-one' matching).
- matching of all passport applicants against the watch list database to provide a second level of assurance against a list of known high risk applicants in the watch list.
- undertaking of ad-hoc investigations for both DIA and other agencies.
- periodic review of photo databases to ensure no fraudulent identities have been created in the past ('many-to-many' matching).

The purpose of this Business Case is to:

- identify the investment objectives
- summarise the investment options that were reviewed and identify the preferred option that meets business needs
- summarise the market proposals for the preferred option and recommend the preferred vendor
- approve management arrangements and secure the necessary funding for implementation of the new facial recognition service.

⁴ Note that in the case of Smith-Traynor's escape abroad, his old photo was not digital, so the potential issue was not detected

Background

The DIA facial recognition system is an essential step in the current passport processing system. The current system was implemented in 2012.

Setting up the Facial Recognition Replacement Project

In November 2016, DIA approved a project mandate for the *Facial Recognition Replacement Project* to replace the existing facial recognition solution since it had been acquired by another company and would no longer be supported in New Zealand after 2017. A new facial recognition solution to be delivered as a managed service was proposed as the preferred option, with the option to expand the service to other government groups at a later date.

The project mandate was followed by an internal DIA Stage One Business Case in February 2017 that provided approval to start a Request for Proposal (RFP) process, and funding for the development of a Stage Two Business Case. The Stage One Business Case proposed a milestone of signing the contract on 31 July 2017.

An initial implementation date of October 2017 was approved in the project mandate. This has now been extended to March 2020 in the Project Initiation Document. This delay was driven by an extended negotiation with vendors to address the unaffordable prices received in the initial RFP responses.

No significant changes to project scope or strategic priorities supported by this investment have occurred since the mandate of November 2016.

The Strategic Case – Making the Case for Change

Strategic context

The DIA facial recognition system is an essential step in the current passport processing system. Its role is to automate the verification of old and new photos for passport renewals, check that the person does not have an alternate identity under another name, ^{9(2)(k)} [REDACTED]

[REDACTED] The system creates cost savings by reducing manual checks, improves turnaround time for passport renewals, and reduces errors and security risks for delivered passports.

The global market for biometric solutions is growing rapidly, and has recently undergone a period of acquisition and rationalisation. As a result, the software vendor that provides the current facial recognition system was acquired and the software is no longer supported in New Zealand. The local integrator and provider of the software is doing their best to keep the system stable, but cannot commit to service levels, and they have no legal authority to update the facial recognition software if upgrades or expansion are required.

The immediate consequences of a failure of the Facial Recognition system would be a growing backlog of adult passport renewals until the system is restored, or for longer term failure, until additional staff could be brought in to reduce the backlog. Another consequence would be that fraudulent passport applications could not be detected until facial recognition identification services were restored.

The current risk is being managed by having the current facial recognition system on a separate server to the main passports system. The facial recognition system server is under a change freeze to prevent upgrades that could cause failure of the facial recognition system.

Environmental context

Environmental trends impacting on this investment area

Technology: There has been rapid advancement in the field of biometric recognition techniques - from iris, fingerprint and voice, through to affordable DNA testing. The capabilities of artificial intelligence are growing and these can be used to improve fraud detection and recognition, but can equally be used by criminals to bypass security systems.

Privacy: Concerns are growing as the ability of corporations and government to identify people when they walk into an office or retail shop make it obvious that the person has been recognised. In response to this concern, the Cross Government Biometrics Group was created, which has established a set of guiding principles to reduce privacy concerns and assist with sharing of facial recognition technologies across government⁶.

Global Identity markets: The International Civil Aviation Organisation (ICAO) is working on advancing a mechanism for global passports, and the World Economic Forum is advocating the development of digital identity verification services that link state provided identities with commercial application of these identities.

⁹⁽²⁾
(k) [REDACTED]

⁶ https://www.dia.govt.nz/Web/diawebsite_historical.nsf/wpg_URL/Resource-material-Guiding-Principles-for-the-Use-of-Biometric-Technologies-Index?OpenDocument. See Appendix C for summary of the principles

Population growth and propensity to travel: The New Zealand population and New Zealanders international travel are both expected to grow, which will steadily increase the number of passports issued⁷.

Anti-money laundering legislation has increased the requirement for passport use as a primary form of identification.

Security threats are growing, since terrorists and criminals will pay large sums for valid passport identities and they have grown increasingly sophisticated in the technology and methods used to obtain them.

These trends are likely to increase New Zealand's reliance on facial recognition over the next five years. Beyond five years, the investment in facial recognition will enhance the NZ government's ability to leverage the benefit of these global trends, from electronic passports to global digital identity.

NZ Government Alignment

There are several NZ government policies and strategies that are relevant for the Facial Recognition Project:

Government Privacy Principles

[The Privacy Act and principles](#)⁸ must be complied with by any proposal to store personal data. These principles influence where data can be stored, and how it must be managed as well as how it can be used.

Government Biometric Principles

The [Guiding Principles for the Use of Biometric Technologies](#)⁹ were produced by the Cross Government Biometrics Group (CGBG), an inter-agency group chaired by the Department of Internal Affairs. They should be used by agencies to inform decision making when considering biometric technologies for identity-related business processes.

The NZ Government ICT Strategy and Action Plan

Part of the technology section of the [ICT Strategy and Action Plan](#)¹⁰ is a move towards adoption of common capabilities and shared services where possible.

All of government procurement

⁷ Although there will be a temporary dip over the next few years due to the change in passport period of validity from 5 years back to 10 years.

⁸ <https://www.privacy.org.nz/the-privacy-act-and-codes/privacy-principles/>

⁹ https://www.dia.govt.nz/Web/diawebsite_historical.nsf/wpg_URL/Resource-material-Guiding-Principles-for-the-Use-of-Biometric-Technologies-Index?OpenDocument See Appendix C for summary of the principles.

¹⁰ <https://www.ict.govt.nz/strategy-and-action-plan/strategy/technology/>

The [NZ Government Principles and Rules of Sourcing](#)¹¹ must be complied with for significant investments.

Table 4 shows how the Facial Recognition Project aligns to each of the NZ government principles and goals

Table 4. Facial Recognition Replacement Project alignment with government principles and goals

Legislation, Policy, Principles and Rules	How Facial Recognition Replacement Project supports
Privacy	The Facial Recognition Replacement Project has ensured privacy is designed into the service, with all aspects of delivery and hosting required to comply with NZ Privacy regulations and principles ¹² .
Biometric Principles	The Facial Recognition Replacement Project meets all of the principles agreed for the use of biometric technologies.
NZ Government ICT Strategy and Action Plan	The contract for the Facial Recognition Replacement project is an all of government syndicated contract that will allow shared use across other parts of DIA as well as other agencies ¹³ .
NZ Government procurement principles	The sourcing strategy and plan for the Facial Recognition Project was completed in partnership with the MBIE government procurement group and meets all procurement principles and rules.

About the Department of Internal Affairs

DIA is a diverse government agency with a broad range of responsibilities and functions that span ICT investment, information management, working with communities, and delivering a range of services to serve and connect people, communities and government to build a safe, prosperous, and respected nation.

Within DIA, a core responsibility of the Service Delivery and Operations branch (SDO) is to manage and protect the integrity of national identity information. This includes identity information for life events such as births, deaths and marriages, citizenships and passports.

Alignment to existing Department of Internal Affairs strategies

DIA's outcomes framework¹⁴ outlines the short, medium and long-term performance priorities and measures. The Facial Recognition Replacement Project supports three of DIA's strategic focus areas.

¹¹ <https://www.procurement.govt.nz/procurement/principles-and-rules/>

¹² See Appendix D for results of the Privacy Impact Assessment: Threshold check

¹³ See Appendix I for details of the other potential users

¹⁴ See Appendix E: DIA outcomes framework

Table 5. Facial Recognition Replacement Project alignment with DIA priorities

Strategic Alignment Area	How Facial Recognition Replacement Project aligns
Transforming Service Delivery – Te Ara Manaaki	SDO has a major service transformation programme, Te Ara Manaaki underway. The new Target Operating Model is working towards common processes and systems. Facial recognition could become a common service across SDO, with potential uses in Citizenship application and Identity Services ¹⁵ .
Trusted information - people will view DIA as trustworthy and secure	The high integrity of the NZ passport and low level of fraudulent use of passports (supported by a strong and secure document) are two key measures of success for the project. The service was designed to meet security requirements, and will be certified as meeting NZ government security standards ¹⁶ prior to launch of the new service.
DIA is fit for purpose - our tools and systems are reliable, fast and modern.	<p>We will understand the cost of delivering our services and we will invest in continuous improvement to ensure our services are efficient and effective</p> <p>The facial recognition replacement ensures DIA is fit for purpose by keeping the Passport Processing System operating effectively at the best value available in the market, and can keep up with the increasingly advanced technology used by criminals and terrorists to create fraudulent passports.</p>

Information Systems Architecture

The Facial Recognition Replacement Project is aligned to three of DIA Information Systems Strategic Plan (ISSP 2014) Future Themes and Architectures:

- **Privacy and Security:** The Facial Recognition service will support the passport system confidentiality, integrity, privacy and availability requirements.
- **As a service enabled:** The proposal recommended by this project is to deliver Facial Recognition as a Service.
- **Fit for purpose:** The Facial Recognition service will deliver a solution that supports the service levels and purposes of the business

¹⁵ See Appendix I for more information

¹⁶ See Appendix Q for the list of assurance steps. Relevant security standards include NZISM and PSR.

Investment objectives, existing arrangements and business needs

Investment objectives

The investment objectives for the Facial Recognition Replacement Project have been derived from the ILM and benefits described later in this section.

The measurable investment objectives set for the project were:

1. Improve contracted service levels from 'best efforts' to 99.5% availability and 24-hour recovery time by April 2020
2. Reduce the hours spent on facial recognition tasks per 10,000 adult passports from 333 to 55 by April 2021, and reduce the hours spent on facial recognition tasks per 10,000 adult passport renewals from 78 to 56 by April 2021
3. Improve the ability to detect fraud as measured by audits of test samples from 96% completing as expected to 99% completing as expected by December 2020.

The overall productivity savings are expected to be between 2,000 – 4,000 hours per year, depending on the volume of applications.

Existing arrangements and business needs

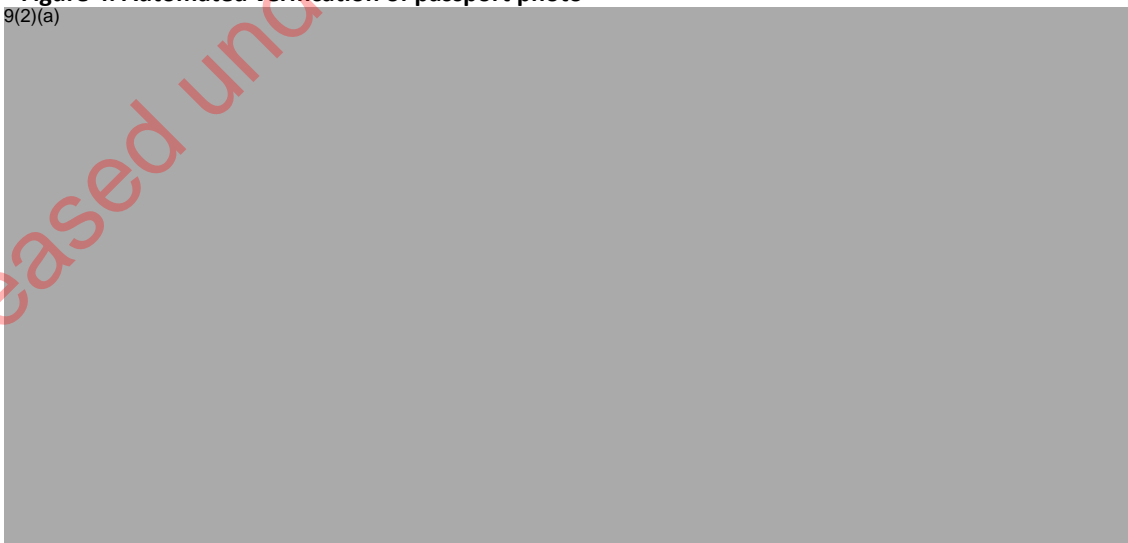
Current operations

In 2012 DIA implemented a facial recognition system that enabled the comparison of old photos with new photos for passport renewal applications. The system also allowed comparison of the new photo against the entire database of digital passport photos to check whether someone was already in the system under another name.

When an application is received to renew a passport, the facial recognition system automatically checks the submitted photo against the previous passport photo to ensure the person is the same. This **verification** capability has significantly reduced the amount of labour required, with only 25% of renewals requiring a manual check when the system cannot provide the required certainty level. Figure 6 shows a demonstration of this capability¹⁷.

Figure 4. Automated verification of passport photo

9(2)(a)



¹⁷ Note that the faces used for Figures 4 and 5 are examples provided by the system vendor.

When an application is received for a new adult passport, the facial recognition system checks the submitted photo against nearly four million existing passport photos to ensure that the application is not an attempt to create a duplicate identity (see Figure 7)^{9(2)(k)}

^{9(2)(k)}. This **identification** capability has prevented criminals and terrorists from obtaining valid but fraudulent passports. Before this capability was introduced, up to forty duplicate passport applications were intercepted each year.



Figure 5. Checking a face does not have a duplicate in the system

¹⁸ ^{9(2)(k)}



If a suspicious passport application is received, DIA investigates further using a specialist team. This team also assists other agencies with their investigative activities by providing specialist knowledge around identity systems enabling the correct identification and confirmation of individual identities ^{9(2)(k)}



Damian Christopher Gillard was caught by facial recognition technology used in data matching checks to ensure passport details match the identity of the person in the photograph¹⁹.

The facial recognition system is used by the passport processing system (known as KIWI). Figure 6 shows where the facial recognition process fits within the overall passport processing system.

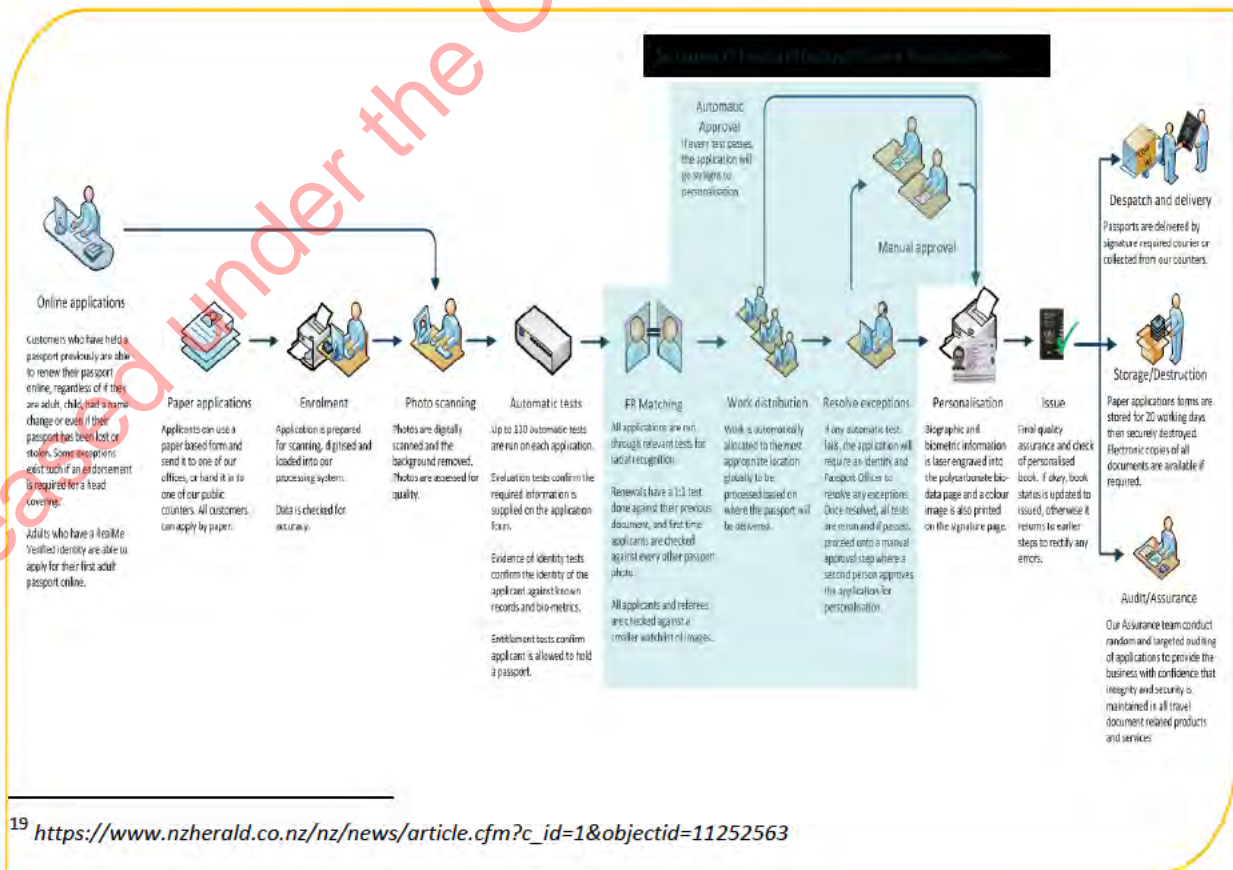


Figure 6. Facial Recognition Scope of Replacement

The reasons for this investment

The global market for biometric solutions is growing rapidly, and has recently undergone a period of acquisition and rationalisation. As a result, the software vendor that provides the current facial recognition system was acquired and the software is no longer supported in New Zealand. The local integrator and provider of the software is doing their best to keep the system stable, but cannot commit to service levels, and they have no legal authority to update the facial recognition software if upgrades or expansion²⁰ are required, creating an increasing risk of system failure.

The immediate consequences of a failure of the Facial Recognition system would be a growing backlog of adult passport renewals until the system is restored, or for longer term failure, until additional staff could be brought in to reduce the backlog. Another consequence would be that fraudulent passport applications could not be detected until facial recognition identification services were restored.

The current risk is being managed by having the current facial recognition system on a separate server to the main passports system. This server is held under a change freeze to prevent upgrades causing a software failure.

The key problems to be addressed by the Facial Recognition Replacement project were defined as:

1. Unsupported systems have increased the risk of passport system failure to unacceptable levels
2. Ageing and inflexible systems prevent realisation of benefits from advancing technology.

Potential business scope and key service requirements

A number of scope options were considered as part of the long list option evaluation, however, the best scope to meet business requirements was to replace the current system capability.

The detailed scope is shown in Table 6.

²⁰ The current database is restricted to 4.5 million templates and this limit will be reached in mid-2020

Table 6. Scope of the Facial Recognition Replacement Project

In scope (we will do this)	Out of Scope (we won't do this)
<ul style="list-style-type: none"> • Replace the current facial recognition system application and platform (production, DR, QA, development and test environments) with facial recognition service on new infrastructure/ data centre • Deploy Facial Recognition as a Service infrastructure to the two DIA/ Datacom Data Centres • Installation and configuration of new facial recognition service • Enrolment of images (Dev, Test, QA, Production environments) • Run many to many deduplication • Facial Recognition Service Performance testing • Configuration of thresholds and service tuning • Integration of the new Facial Recognition Service with KIWI (Keeping Our Information with Integrity, DIA core Passport System) • Replace the Investigation Workstation (FEW – Facial Examination Workstation) with the Facial Recognition Service – Investigations Service • Update Blaze Rules to reflect the thresholds for the new Facial Recognition service • Updates to FRAP to integrate to the new Facial Recognition system • Updates to KIWI Biometrics Service to integrate to the new Facial Recognition system • Updates to Deletion tool to integrate to new Facial Recognition system. • Replace IPLS with new facial recognition service • Privacy assessments and security assurance activities • Decommission ABIS application and infrastructure • Decommission FRAP • Any applicable business process changes • Business change management and training • Design and implement support model and Service Support Design Package for the new Facial Recognition service. • Finalise the Master Syndicated Agreement for the procurement of Facial Recognition Services 	<ul style="list-style-type: none"> • Enhancements or changes to PPTS – Passports Processing Transformation System • Discovery or documentation of other government agency requirements

See the Change management planning section of the Management Case for how the architecture will change as a result of the project.

Main benefits

Since the key reason for change is the withdrawal of support for the current facial recognition software, the key benefit sought from the process of re-evaluating facial recognition is to ensure that passport delivery is not compromised, with appropriate support contracts in place.

Updating the current system allows for some accuracy improvements which lead to productivity as well as fraud detection benefits. The overall productivity savings from these improvements are expected to be between 2,000 – 4,000 hours per year, depending on the volume of applications.

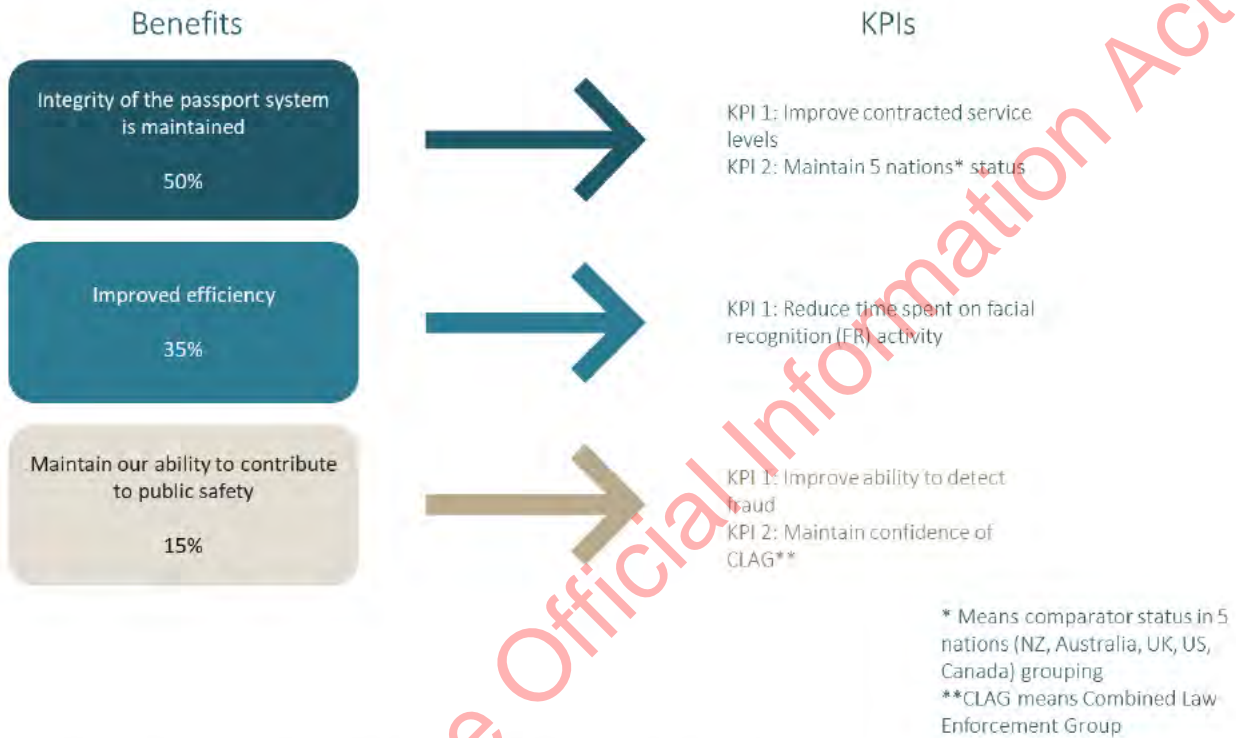


Figure 7. Facial Recognition Replacement Project benefits and KPIs

Continuous improvement in facial recognition algorithms is expected over the length of the service agreement, and will deliver new productivity and fraud detection benefits over time. These future benefits could not be estimated, but will help to ensure that DIA remains efficient and can keep up with attempts to obtain fraudulent passports.

Table 7. Analysis of potential benefits that can be expressed in monetary terms

Main Benefits	Who Benefits?	Direct or Indirect?	Description
Improved efficiency KPIs: Cost of staff for processing	Government and DIA	Direct	The new service will increase the accuracy of the facial recognition system, thereby reducing the time spent to manually review photos.

Table 8. Analysis of potential benefits that cannot be reliably expressed in monetary terms

Main Benefits	Who Benefits?	Direct or Indirect?	Quantitative or Qualitative?	Description and Possible Measures
Integrity of the passport system is maintained KPIs: Improve contracted service levels Maintain 5 nations status	New Zealanders and the NZ economy, NZ government	Indirect	Qualitative	Contracted recovery time objective and availability of the service. % of baseline sample that completes as expected during audit test
Maintain our ability to contribute to public safety KPIs: Improve our ability to detect fraud Maintain the confidence of CLAG	New Zealanders and the NZ economy	Indirect	Qualitative	% of baseline sample that completes as expected during audit test % of requests for investigation able to be responded to

The detailed benefit management map can be seen in [Appendix F: ILM and Benefit Management Plan](#).

Optimism bias

Optimism bias has been corrected by reducing the benefits to allow for real life obstacles to realisation of benefits, such as photo quality, user adaptation, process streamlining and integration and response time under load. The time to achievement of productivity benefits has also been extended due to previous experience with the complex interplay between the passport processing system and the people performing the processes.

Main risks

A Risk Profile Assessment was completed and reviewed by NZ Treasury and the overall project risk was assessed as Medium, despite the relatively high 'whole of life' cost. The key reasons for this rating include:

- **The low degree of change.** The current system runs in the background of the main passport processing system, and there will be little or no change observable by the passport system users. The only users who will notice the change are the Investigations Team who use a specialised interface. This team has seven staff.
- **No external impact.** No external customers are affected by the change.

- **Tried and proven technology.** The system will replace the current system with tried and tested modern technology²¹.

Different types of risk are discussed in detail in the different sections of the business case as is appropriate.

Table 9. Risks discussed in each section of the business case

Business Case section	Focus
Strategic case	Uncertainty risks due to environmental factors
Economic case	Risks associated with each option used in the options analysis
Commercial case	Risk allocation and mitigation with the supplier for the preferred option
Financial case	Financial risks of the preferred option and the associated contingency set aside
Management case	Risks to the delivery of the project and how they will be mitigated

Uncertainty risks for facial recognition technology

Uncertainties are the environmental factors that may change in unexpected directions or change more rapidly than anticipated.

Table 10. Uncertainty risks with potential impacts on the Facial Recognition Replacement Project

Main uncertainty	Consequence	Likelihood	Comments and Uncertainty Management Strategies
<p>Rate of technological advancement and change</p> <p>The impacts of technology and expectations around its use in facial recognition is broad. This includes:</p> <ul style="list-style-type: none"> • arrival of different Biometric techniques (eg DNA, hand vein patterns, palm geometry, iris, gait) • Growth in AI allowing continuous improvement by learning • Changes in accuracy expectations from global standards 	<p>Significant (cost to break and/or change a contract that is no longer fit for purpose, lower productivity from false rejects)</p>	<p>Improbable</p>	<p>Monitoring of tech development with regular reviews by DIA.</p> <p>Supplier to provide innovation report annually and roadmap for consideration.</p> <p>Contract provision for continuous improvement by the supplier to allow for improvements in technology</p> <p>Contract provision for DIA to exit the contract early if service standards are not maintained.</p>
<p>Changes in methods of fraud</p> <p>As technology becomes available, some individuals use these new capabilities to commit fraud. To maintain confidence in the passports system, DIA will need to remain current.</p>	<p>Significant</p>	<p>Improbable</p>	<p>DIA have requested a roadmap from the supplier to indicate how technology changes can be addressed. Up to two algorithm updates also accounted for.</p>

²¹ A local reference site for the preferred vendor was visited as part of the due diligence process

Main uncertainty	Consequence	Likelihood	Comments and Uncertainty Management Strategies
<p>Facial Recognition market (and software vendors business) growing quickly</p> <p>Facial recognition market growing with wider interest and new uses, eg “Face on the Move” technologies for video surveillance in supermarkets, airport arrival halls etc.</p> <p>The preferred supplier’s subcontractor (NEC) may not have the capacity to deliver if committed to wide range of projects, or this contract could be a lower priority.</p>	<p>Significant (supplier not able to meet SLA’s and support DIA)</p>	<p>Improbable</p>	<p>Complete due diligence as a part of procurement process.</p> <p>Supplier/s likely to see value in this contract – syndicated contract provides a wider customer pool within government and NZ market and Passports in particular is a strong reference internationally</p> <p>Primary supplier will be responsible for ensuring the services are performed.</p>
<p>Software vendor sustainability</p> <p>The current software is no longer supported in New Zealand after the software vendor providing the current facial recognition system was acquired. The market has been consolidating over the last few years.</p>	<p>Significant (new vendor/subcontractor may be forced onto DIA, or current vendor/subcontractor may close business)</p>	<p>Improbable</p>	<p>Complete due diligence as a part of procurement process.</p> <p>Contract provision for insolvency in contract including step-in rights, ability to terminate the contract and establishing an agreed succession plan²².</p>
<p>Variability in facial recognition demand and volumes</p> <p>This is driven by the demand for passports which, in turn is driven by a range of factors including:</p> <ul style="list-style-type: none"> • length of passport validity • changes in the international environment – for example terrorism, pandemic (eg SARS), immigration levels, lower flight costs • changes in the geopolitical environment including immigration factors • use of passports as unique identifier for other purposes eg criminal screening, AML compliance. 	<p>Moderate (Overall contract costs)</p>	<p>Improbable</p>	<p>Monitoring of throughput with forecasts with regular reviews.</p> <p>Payment will be based on actual throughput bands, rather than as a fixed monthly cost / rate.</p>

²² During contract negotiations, escrow rights will also be sought

A risk register has been developed and will be progressively updated as part of the project management assurance plans. See [Appendix G: Facial Recognition Risks and Uncertainties](#) for the full outline of risks.

No risks were identified that would exceed DIA risk thresholds. The risk profile assessment showed a medium level of risk, due to the minimal change experienced by users, lack of external customer impact, and proven technology.

Key constraints, dependencies and related projects

The proposal is subject to the following constraints. There were no dependencies identified. There are related projects that will be regularly monitored during the project as outlined in the table below.

Table 11. Key constraints and related projects

Constraints	Notes
Te Ara Manaaki and Uruwhenua 2020 Change windows	The Ara Manaaki programme is a large programme of change, which will require significant involvement by staff. Uruwhenua (passport personalisation) will also be implementing a new solution over a similar time period. Change and training windows are likely to be constrained for passport processing staff
Related projects	Notes and Management Strategies
RealMe Now App	Currently using manual one to one photo matching. Will consider the Facial Recognition service as part of possible future improvements
Te Ara Manaaki	<p>Te Ara Manaaki will be potentially be designing and implementing changes to the KIWI passport processing system where Facial Recognition is used, but the Citizenship area could use the Facial Recognition service over the next few years.</p> <p>Te Ara Manaaki and Facial Recognition services will be conducting detailed design and process in the same timeframe. However, Te Ara Manaaki will be delivering Passports co-apply changes which use a separate system to KIWI, and other Passport roadmap items which have yet to be defined.</p> <p>The Life Events and Identity Services Board will manage the change underway across DIA.</p>
Uruwhenua 2020 and Identity Services Portfolio	The changes to be delivered by the projects will be planned, scheduled and coordinated.

The Economic Case – Exploring the Preferred Way Forward

A review of all investment options was undertaken to ensure the best value for money and lowest risk option was selected.

Critical success factors

The following critical success factors were utilised by stakeholders²³ to assess options at the facilitated long list and short list options workshops.

Table 12. Facial Recognition Replacement critical success factors used to assess options

Generic Critical Success Factors	Broad Description	Application of Critical Success Factors for Facial Recognition
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.	As well as the investment objectives, how well the options align with DIA strategies including Te Ara Manaaki (service delivery transformation) and NZ government objectives including those for procurement and ICT.
Potential value for money	How well the option optimises value for money (ie, the optimal mix of potential benefits, costs and risks).	Value for money is assessed separately to risk, to ensure that the key differences between options were well understood.
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.	This was based on an assessment of the market and the suppliers in it. In-house provision was considered based on DIA's ability to deliver.
Potential affordability	How well the option can be met from likely available funding, and matches other funding constraints.	
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.	The supplier was the most important factor in achievability, since the number of people affected and the nature of the impact is small.

²³ The project team, project executive, finance and commercial representatives and business subject matter expert

Long-list options and initial options assessment

A wide range of options was generated by stakeholders. The long-list options considered elements of:

- A. scope
- B. nature of the service (solution)
- C. service delivery
- D. timing of the implementation
- E. funding source.

A larger number of alternatives were considered for the first three elements, while timing and funding had no alternative options. [Appendix H](#) summarises the long-list options and the associated advantages and disadvantages for each.

Long-list assessment

The potential long-list options in each of the five dimensions were assessed against the investment objectives and critical success factors. The full analysis, along with which options were taken forward for shortlist consideration is included in [Appendix H: Presentation of the Long-list Options Assessment](#).

The short-listed options

On the basis of the long-list analysis, the recommended short-list for further assessment was:

- **Option 1: Status quo** – continue with the current unsupported facial recognition system. This option is retained as a baseline comparator
- **Option 2: Do minimum** – reduce current capability to detect fraud by eliminating the ability to check photos against the current identity photos (one to many)
- **Option 3: Preferred** – replace current capability with a sustainable, supported service using the latest algorithms for increased accuracy
- **Option 4: Aspirational** – use artificial intelligence to extend the current capability and enable constant improvements through self-learning.

Economic assessment of the short-listed options

An economic cost benefit analysis has been carried out to support assessment of the options.

Assumptions

See [Appendix I: Detailed Economic and Financial Data](#) for further detail on the financial assumptions.

Assessment period

Costs have been assessed over a 12.5-year period (project duration and 10-year supplier contract), and benefits are assumed to be realised progressively over the 12 months after the new service is in operation in 2020.

Estimated costs

The costs were estimated by:

- Applying the forecast passport demand estimates (see Appendix I: Detailed Economic and Financial Data) to the pricing matrix for the preferred provider.
- Creating a DIA resource plan for the implementation project, and adding the supplier implementation costs to estimate capital costs.

Estimated benefits

Only the preferred option had any economic benefit that could be measured. The basis of the benefit was from a reduction in the number of exceptions generated by the facial recognition system that require manual intervention. The aspirational option including artificial intelligence had uncertain costs and uncertain benefits. It is likely that the aspirational option would improve productivity more than the preferred option, however until such a system is available for government use in New Zealand, this cannot be tested.

There are three types of check that the facial recognition system performs. The first is a verification check for passport renewals to ensure that the old photo shows the same person as the new photo. The second is an identification check – this ensures that new passport applicants do not already have a photo in the passport system to prevent duplicate identities being created. 9(2)(k)

Each time the facial recognition system cannot meet the threshold parameters required for a check, it raises an exception that needs to be manually reviewed by the passport officer, and then peer reviewed by a second passport officer. A certain proportion of cases are referred for review by the investigations team. The time taken for these exceptions is shown in Table 13 below.

Table 13. Processing time for facial recognition exceptions

9(2)(k)

The preferred replacement facial recognition system creates savings by reducing the number of exceptions that need to be manually reviewed. It does this by having a more accurate algorithm than the current system.

Table 14 shows the expected reduction in exceptions for each class of passport application. Note that the current facial recognition system cannot automate child or youth passport applications. One of the potential benefits of the new algorithm is that it may allow some youth passport applications to be processed automatically. This will be tested before the new system is put into production to see whether additional benefits could be gained by automating youth renewals.

Table 14. Current and predicted rates of facial recognition exceptions for passport applications

9(2)(k)



There are up to 250 passport officers employed by DIA in five locations; Wellington, Auckland, Christchurch, Sydney and London. The estimated time spent by these officers on the facial recognition process is around 5,000 hours per annum, projected to decline slightly over the next 2 years and then increase by 50% per annum to 8,000 hours by 2027 in line with the passport renewal cycle, population growth, and a greater reliance on passport-level identification in the finance sector.

The new system is expected to reduce these hours by approximately 50%. The addition of youth automation and improvement of the algorithms over time may lead to further reductions, but once available, these need to be weighed against the risks and additional costs before decisions can be made. Full details of the model are shown in Appendix I: Detailed Economic and Financial Data.

The specific measures used for the investment objectives were:

Table 15. Facial recognition processing time improvements

Passport application type:	Adult new	Adult renewal
Hours per 10,000 passport applications spent on facial recognition manual processing today	333	78
Hours per 10,000 passport applications spent with predicted exceptions for preferred option	55	56

Past experience with facial recognition automation shows that realising these benefits takes time, with refining of the risk models used by the KIWI passport processing system required, as well as focusing on other process steps for staff. For this reason, full realisation of the productivity savings is not expected until one year after the system is fully in production, and a 17% “optimism bias reduction” was applied to the model.

Fully burdened staff costs were used to estimate the productivity saving from the reduced hours on exception checking.

In 2020, the latest forecast demand will be assessed to determine how these benefits (between 2,000 to 4,000 hours) will be reflected in staffing numbers – either through avoidance of staff increases or staff reductions.

There are also quality improvements from improved accuracy of the facial recognition system. This is because automated systems do not get tired or suffer de-sensitisation from overexposure to many images. The benefit of this quality improvement is reflected by the value of improved ability to detect fraud, rather than as a monetary benefit for economic comparison.

Identifying the preferred option

Table 16 shows the options analysis conducted by key stakeholders in a workshop on 30 July 2018. The detailed economic cost benefit analysis, using core assumptions outlined above, and the assessment of each options alignment to the investment objectives and critical success factors is presented in Table 17.

Table 16. Facial Recognition short list analysis summary

Option 1: Do Nothing	Option 2: Do Minimum – Reduce capability	Option 3: Preferred Replacement	Option 4: Aspirational Artificial Intelligence
Advantages			
	<p>Lower cost than option three and four.</p>	<p>More modern and accurate system will support delivery of all benefits including fraud detection and security.</p> <p>Shifting to ‘as a service’ aligns with DIA priorities, limits capital investment, and allows DIA to adapt to more easily adapt to change.</p> <p>Allows common capability to be utilised across SDO for Citizenship and Identity Services in line with the target operating model. Potential for other agencies to be involved aligns with AOG Shared Services Strategy.</p> <p>This option can be upgraded to Option 4 in the future.</p>	<p>Potential for on-going accuracy improvements from AI system learning providing additional efficiency gains compared to option 3.</p> <p>Better support for DIA to keep up with terrorist and fraud threats.</p> <p>May make system more attractive for other NZ government agencies to adopt.</p>
Disadvantages			

Option 1: Do Nothing	Option 2: Do Minimum – Reduce capability	Option 3: Preferred Replacement	Option 4: Aspirational Artificial Intelligence
<p>There is no vendor support. Prime vendor cannot commit to keeping the system running, and is unable to implement changes if required for integrations with other DIA systems</p> <p>Increasing risk of service failure.</p> <p>Will exceed licensing volumes by mid-2020.</p>	<p>DIA would be less likely to detect fraud from duplicate identities.</p> <p>Does not support Te Ara Manaaki objectives of a single customer view and increased automation.</p> <p>At risk of losing 5 Nations status and Visa waiver to countries.</p> <p>Cannot respond to CLAG requests.</p>		<p>Is still unproven, leading edge technology – meaning costs (and subsequent value for money) are unclear.</p> <p>Investment in facial recognition AI would be of potential benefit across the passport process, including Te Ara Manaaki and RealMe, so investment would need to be considered in a wider context.</p>
Risks comparison			
<p>Unacceptable (and increasing) level of risk to passport delivery services</p>	<p>Increased risk of fraud due to duplicate identities being established.</p>	<p>Lowest risk option, with proven technology and a current supplier.</p> <p>Low future risk because it can be upgraded to Option 4</p>	<p>Actual costs likely to be higher than estimated as technology will be new.</p>

Table 17. Facial Recognition options cost benefit analysis results

	Option 1: Do Nothing	Option 2: Do Minimum – reduce scope	Option 3: Preferred - replace	Option 4: Aspirational (AI)
Appraisal Period (years)	12.5 years	12.5 years	12.5 years	12.5 years
Capital Costs	-	\$6.6m	\$6.0m	\$11.2m
Whole of life costs	\$0.8m - \$1.0m	\$10.7m - \$13.8m	\$21.9m - \$27.4m	\$43.1m - \$53.8m
Present Value of monetary benefits	-	-	\$0.6m	-
Present Value of costs	(\$0.9m)	(\$12.2m)	(\$24.6m)	(\$48.5m)
Net present value (NPV)	(\$0.9m)	(\$12.2m)	(\$24.0m)	(\$47.8m)
NPV rank (out of 4)	1	2	3	4
Alignment with Facial Recognition Investment Objectives				
Maintain integrity – maintain SLAs	No	Yes	Yes	Yes
Maintain integrity – maintain 5 nation status	No	Yes	Yes	Yes
Improve efficiency – reduced per unit cost processing	No	Yes	Yes	Yes
Maintain public safety – maintain fraud detection	No	Partial	Yes	Yes
Alignment with Critical Success Factors				
Strategic and business needs	No	No	Yes	No
Potential for value for money	No	No	Yes	No
Service provider capacity and capability	No	Yes	Yes	Partial
Potential affordability	No	Yes	Yes	Yes
Potential achievability	No	Yes	Yes	No

Testing the sensitivity of the options analysis

Uncertainty in the costs and benefits across all the options is reflected in the use of ranges.

Quantitative Risk Analysis (QRA) has been completed on the costs and benefits to confirm the ranges. See [Sensitivity Analysis](#) for further detail on the QRA.

Multi-criteria analysis was not considered necessary due to the linear progression of the options, from taking no action (Do Nothing) to a more ambitious approach to facial recognition than the current system (Aspirational). This allows a clear decision of which is the best value option to meet the business requirements.

The preferred option

Option 3 was selected as preferred by the stakeholders including the project executive during a meeting on 30 July 2018. The key factors in this decision are summarised below.

1. **Do nothing** – Continue the current system beyond 2021. This would jeopardise the whole passport process, creating a high risk of failure, and was discounted.
2. **Do Minimum, reduce scope** by eliminating the ability to check for a duplicate identity. This would halve the whole of life cost of the facial recognition service, but would create a fraud vulnerability that could harm NZ's passport reputation by creating an avenue for criminals to launder money and sell valid but fraudulent New Zealand passports to terrorists.
3. **Preferred - Replacement** with a similar scope of service using modern software. This option meets the business requirements and fits with Te Ara Manaaki target operating model by creating a common capability. It is the best value for money option that reduces the business risk to acceptable levels. This was the preferred option.
4. **Aspirational option** using artificial intelligence to enhance accuracy and further improve fraud detection. This option was unable to be supplied by the market in the timeframe required.

Option 3 does not exclude upgrading to Option 4 once the technology is established and the value proven, since artificial intelligence capability can be applied across multiple systems.

Commercial Case - Preparing for the Potential Deal

Background

The current facial recognition software was procured as part of the Passport Redevelopment Programme in 2012. The facial recognition system provider was purchased by a larger company (Morpho, now known as Idemia) resulting in DIA's existing facial recognition software product being retired. Development licenses for the product were discontinued in October 2017. The existing facial recognition software is not the latest version and is no longer supported by Idemia. Support has been provided by DXC (previously known as Hewlett Packard Enterprises) on a best efforts basis, but DXC are unable to provide service level warranties since Idemia will not support the product in New Zealand.

As noted in the Strategic Case, DIA's ICT strategy is to take advantage of industry improvements both now and for the future by procuring capabilities 'as a service' (paying through operating expenditure) rather than as a capital investment. The new facial recognition service will include ongoing operational service management, software and infrastructure upgrades over the period of the contract. This will require a combination of a specialist biometric supplier as well as a service provider providing hosting and management services.

A detailed procurement plan for facial recognition services was completed and signed off in April 2017²⁴. A request for proposal (RFP), a testing phase, negotiation phase and a Best and Final Offer (BAFO) stage have now been completed. A summary of the key plan and evaluation elements is provided in the following section.

Market summary

The biometric market

Biometrics²⁵ is the process by which a person's unique physical and other traits are detected and recorded by an electronic device or system as a means of confirming identity. Potential physiological biometric identifiers include, fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Individual or combinations of these measures can be used to support the personal identification and verification.

Of the various biometric technologies available, facial recognition is a mandatory requirement for ICAO E-Passports and as such, has been the preferred biometric identifier for passports in New Zealand since it was introduced. Digital facial images were added into E-passport processing in 2005 and have been used at automated borders since 2007 for facial recognition.

The facial recognition technology market

The market for facial recognition technology is a subset of the wider biometric technology market.

²⁴ [Facial Recognition Project Procurement Plan v8.0](#)

²⁵ <https://www.biometricupdate.com/201601/what-are-biometrics-2>

The facial recognition market has a small number of global suppliers. Since 1994 there has been a period of consolidation through mergers and acquisitions, combining multiple technologies into a single offering, reducing both the number of suppliers and products.

The buyers of facial recognition software are mainly government agencies, commonly for usage for border control and law enforcement, however it is increasingly being used by commercial organisations including banks and retailers. Government buyers have a high influence on the market, depending on the volume in each country. The New Zealand Government is still considered an attractive client to have on a supplier’s portfolio.

Suppliers generally partner with a local service provider in New Zealand who can provide support and infrastructure services.

Competition is primarily based on accuracy of the software along with price. Over time, identification rates are increasing while false match rates decrease. Facial recognition software performance is measured through the National Institute of Standards and Technology (NIST) Face Recognition Software vendor Tests, which have been conducted since 1994. Regular participation and performance in these tests is a key indicator of long term commitment and investment in facial recognition technology.

Table 18 identifies a number of top biometric and potential integration software vendors. See [Appendix J: Supplier overview](#) for further detail on these providers.

Table 18. Facial Recognition technology software vendors and system integration suppliers

Facial Recognition suppliers	System integrators providing data centres and managed services in New Zealand
Gemalto Cogent (formerly known as 3M Cogent and 3M)	Datacom
NEC	DXC (formerly known as Hewlett Packard Enterprise)
Cognitec	IBM
Idemia (formerly known as Safran Identity & Security, Morpho and OT-Morpho)	Fujitsu
Toshiba	Unisys
	Canadian Bank Note Company

The New Zealand Government market for facial recognition technology

A number of government agencies in New Zealand currently use, or intend to use, facial recognition in their identity verification processes²⁶. Of these, DIA has the most experience, along with in-house expertise related to the use of this technology. DIA also actively participates in the Biometric International Standards group (ISO/IEC SC37 – Biometrics) which develops, modifies, reviews and rewrites Biometric standards. This provides DIA with an understanding in the direction and advancements in Facial Recognition Biometric technologies.

²⁶ Includes DIA, NZ Police, Immigration, Customs and the New Zealand Transport Agency (NZTA)

DIA will set the contract as an Open Syndicated Contract. This will create opportunities for other agencies to benefit from reuse of the service and economies of scale, although its use will not be mandatory. Additionally, while DIA will be seen as a relatively small customer for facial recognition as a service, suppliers will see the opportunity for growth across government. DIA will act as the Lead Agency and deal with all aspects of the contract development and management.

Other agencies' involvement in the procurement process

Support for syndication

A workshop with some of the main interested agencies (Police, Immigration, Customs and NZTA) was held in March 2017. See [Appendix K: DIA and Other Agency Use of Facial Recognition Services](#) for further information from each agency on their lessons learnt and how they use facial recognition.

As other agencies requirements were not yet defined, they were not included in the requirements provided to suppliers. However, the contracting arrangements can support new and altered requirements for additional members using the facial recognition service.

Procurement process

The procurement process for the Facial Recognition Service was outlined in the Procurement Plan dated 6 April 2017. This process is in line with good practice and has included MBIE approvals of all key documents including the Procurement Plan. As the responses to the Request for Proposal (RFP) had unaffordable pricing, the process was adjusted, extending the duration for the RFP evaluation, with negotiations being held with all respondents earlier in the process than usual. Proceeding on the original plan was not feasible as DIA would not have had the budget to proceed with the submitted prices.

The approach to the market

The Request for Proposals was issued on 11 April 2017. Suppliers that responded to the RFP are outlined in Table 19.

Table 19. Suppliers that responded to the RFP

Name of supplier	Met procedural requirements	Met mandatory conditions
DXC Technology (partnered with NEC for the Biometric Capability)	Yes	Yes
9(2)(b)(ii)	Yes	Yes

Both suppliers met all of the following pre-conditions before their bids were considered for evaluation:

1. The facial recognition solution must be hosted onshore in New Zealand.
2. The facial recognition service must use NZ based facilities and personnel resources.
NOTE: Technical /level 3 support may be provided from off shore resources, but no remote access is permitted.
3. The service must utilise a commercially available facial recognition engine for which the current or earlier version(s) has undergone NIST testing in FRVT2013 for Class C: Accuracy of algorithms executing one-to-many identification searches to determine either that the person is not enrolled, or to determine the identity of the person, for large population sizes of N=1600K

Evaluation of supplier offers

The RFP was evaluated by a cross-functional team (see Table 20).

Table 20. The cross-functional team responsible for the RFP / BAFO evaluation panel

Role	Membership	Name	Responsibilities
Chair of evaluation panel	Non-voting	Lee Cook	Chair all moderation meetings
Project Manager	Non-voting	Leanne Tomlinson	Capability and Capacity Review
Facial Recognition Expert	Voting	Gerard Harris	Evaluate All Criteria
User group/beneficiary	Voting	Peter Campbell	Evaluate All Criteria
User group/beneficiary	Voting	Esther Williams	Evaluate All Criteria
Product Development	Voting	William Hopgood	Evaluate All Criteria
Project Architect	Voting	Jenny Zhang	Evaluate All Criteria
Commercial Specialist	Voting	Tim Richards	Evaluate Capability & Capacity

The evaluation model used was weighted attribute (weighted score). For the RFP, price was not a weighted criterion. Instead price was taken into account when determining value for money over the whole-of-life of the contract. A two-envelope process was used and respondents pricing was only opened once the non-price scoring was completed.

A number of clarifications sessions were conducted with both respondents, followed by evaluation and moderation sessions with the internal DIA evaluation panel. The initial pricing received was unaffordable, so lengthy negotiations were held with both suppliers to reduce the whole of life costs. The main ways that savings were made during this process were;

- Asking the local integrators to renegotiate their licencing agreement with the software vendors.
- Reducing the service levels (and therefore costs) on the development and testing environments
- Changing the hosting arrangements for the service, and moving it to the IaaS datacentre with Datacom.
- Changes to the Master Syndicated Agreement. The levels of Insurance, liabilities and service level credits were all negotiated to reduce the risk to the local integrator.

Each Respondent was asked to resubmit the RFP response form and highlighting what had changed in their submission based on clarifications and negotiations

The evaluation panel then re-evaluated all the amended sections of the RFP response and a moderation session was held to discuss any change in scores. This was the final stage in the evaluations and therefore the summary scores in the Table 21 are final.

Table 21. Results of the supplier evaluation at the end of the Best and Final Offer (BAFO) stage

		9(2)(b)(ii)	DXC
Non Price Criteria	Criteria Weight	Weighted Score	Weighted Score
Technical Merit		60%	47.03
1 Biometric Capability	24%	18.04	
2 Biometric Accuracy	18%	15.73	
3 Service Architecture and Non Functional Requirements	18%	13.26	
Capability		30%	17.48
Capacity		10%	5.01
Overall Score (out of 100)			69.53
Ranking			1

9(2)(b)(ii)

[Redacted content]

Business requirements

Three services were specified in the business requirements – identification, verification and investigation, with three components within each service (see Table 22).

Table 22. Service Requirements

Service split into three offerings:	Each service (1-3) will be made up of:
<p>1. Identification Service</p> <p>Provides functions to support one-to-many searches using facial characteristics against a biometric enrolment database.</p> <p>For passports, this is a search against the passport population to ensure first time applicants do not hold an existing passport under a different identity.</p>	<ul style="list-style-type: none"> • A Service Category This will consist of a Gold, Silver and Bronze service levels that can be applied and will determine the target availability of the service, the hours of operation, the maximum monthly outage, the recovery time objective and the recovery point objective • Size This will be bands A to F and will determine the enrolled population • Throughput
<p>2. Verification Service</p> <p>Provides functions to enable the performing of one-to-one comparisons searches using facial characteristics.</p> <p>For passports, this is a comparison is performed to</p>	

Service split into three offerings:	Each service (1-3) will be made up of:
verify an applicant is the holder of the previous passport being replaced.	This will be bands A to F and will determine the transaction rate requests per hour
<p>3. Investigation Service</p> <p>Provides functions to enable investigators to investigate identity fraud and perform forensic analysis of facial images.</p> <p>For passports, 9(2)(k) [REDACTED] and passport population are performed outside of passport controlled processing.</p>	

In addition to the service requirements, functional and non-functional system requirements were developed by subject matter experts within DIA and an independent consultant²⁷. Requirements were signed off by the business prior to RFP release. See [Appendix M: Facial Recognition Service Requirements](#).

Assets replaced and acquired

For the preferred option the assets requiring replacement and acquisition are listed in Table 23. All current assets implemented through the last phase of the Passports Redevelopment Programme have been fully depreciated.

The project costs to implement the new facial recognition service, including part of the supplier's costs will be capitalised. The on-going costs will be categorised as operational costs, and include all maintenance and infrastructure costs incurred by the supplier to deliver the service. This includes the provision of a new investigation capability.

Table 23. Assets Acquired and Replaced

Current Asset	Description	Future Action
ABIS (Automated Biometric Identification System)*	Existing Facial Recognition technology used by Identity and Passport Services (IPS). Technology was supplied by Morpho	Replaced with new facial recognition capability provided as a service
FEW (Facial Examiner Workstation)*	Facial Examiner Workstation used by the investigations team on a daily basis to complete work	Replaced with new investigation capability provided as a service
FRAP (Facial Recognition Application Process)*	A batch tool that runs periodically to enrol applicant images submitted via PPTS to ABIS	Retain within changed process

²⁷ [Facial Recognition Service Requirements](#)

New Assets		Future Action
New facial recognition service implemented	The project costs to implement the new facial recognition service, including part of the suppliers costs will be capitalised.	Capitalise

*asset fully depreciated

The preferred supplier

The preferred supplier is DXC Technology, and the evaluation panel recommended that DIA enter into final contract negotiations with them.

The panel decision is based on DXC Technology:

- demonstrating the best solution capability and accuracy
- representing the best value for money for whole of life costs, since it delivers significant accuracy improvements over the other respondent for a similar cost. representing the best organisational capability and capacity overall
- being assessed as the most suitable provider for facial recognition services across NZ Government and would provide a world class solution with extremely high accuracy results.

The DXC proposal includes hosting services from Datacom Cloud Solutions for Government (DCSG). DCSG is one of three New Zealand Government approved Cloud based Infrastructure as a Service providers. DCSG has passed the DIA requirements for cloud solutions, and has the required certifications to host Government Services with up to Restricted Level Data Classifications. DCSG is New Zealand based, meaning New Zealand's privacy legislation applies.

DIA will certify the DXC Service independently before go-live to ensure that it fully complies with the NZISM controls required to achieve certification for a system with Restricted level classification.

Commercial risks

Commercial risks and their approximate allocations are shown in Table 24. The supplier commits to conform to DIA requirements underpinned by specific warranties, service level rebates and liquidated damages for project delay. The supplier's liability for breach of contract is capped in relation to the prices paid in the 15 months preceding the act or omission.

Table 24. Contract risk allocation

Risk Allocation			
Risk Category	DIA	Supplier	Shared
Development and configuration risk		✓	
Transition and implementation risk			✓
Availability and performance risk		✓	
Variability of demand risks			✓
Termination and takeover risks			✓
Technological advancement risks			✓
Financing and residual value risks	✓		
Security risks (IT)			✓

Table 24 shows the risk allocation for various elements of the proposed contract. The categories in bold are the ones identified as the environmental uncertainties with the highest impact and probability.

The complete list of environmental uncertainties and the commercial remedies applied to mitigate them were detailed in the Strategic Case [Table 10. Uncertainty risks with potential impacts on the Facial Recognition Replacement Project.](#)

Management of the risks related to the transition and implementation of the new system will be shared between DIA and the supplier. See the Management Case for further detail on how this will be managed. In the event the supplier fails to meet the final implementation milestones specified in the contract, then damages will be applied.

As the facial recognition capability is provided as a service, the technology advancement risk will be shared. The supplier will be expected to identify if new technology is appropriate and DIA would provide approval of the change (or not). Wider security and privacy risks are covered in detail in the Privacy and Security Impact Assessments. The requirements to protect DIA and its customers were included in the RFP requirements, and were met by all/the selected suppliers.

Pricing and payment mechanisms

Suppliers were requested in the RFP to provide a catalogue of pricing for the three services (Identification, Verification and Investigations) to enable any Government Agency to select the services they required for facial recognition. This was made up of a monthly price for each service in a range of volume and throughput bands, showing any price variations over the contract period of 10

years. In addition suppliers were asked to consider what volume based discounting would be applied within the pricing model.

For the production identification services the preferred supplier (DXC) have agreed a fixed monthly unit cost per enrolment where the per unit cost is scaled based on the accumulative total number of enrolments across all Agencies who have signed up to this agreement. This means the service costs would go down if other Agencies start to use the service.

In the BAFO submission, the preferred supplier requested a fixed implementation fee, and the following approach to the service model charges:

- a. **Production Identification services** are charged
 - a. A fixed monthly unit cost per enrolment where the per unit cost is scaled based on the accumulative total number of enrolments across all agencies,
 - b. A fixed monthly cost band based on the throughput per service instance.
- b. **Production Verification services** are charged a fixed monthly cost band based on the throughput per service instance.
- c. **Investigation services** are charged a fixed monthly cost band charged on a per user basis. Non Production users are the same price.
- d. A separate **non production environment fee** is charged per environment per agency covering all Identification and Verification services at minimal throughputs.

Contractual and other issues

Type of contract

The short-listed supplier will be offered an adjusted Master Syndicated Contract for this service. The following arrangements have been agreed:

- The key performance indicators for measuring the supplier's performance are reflected in the contract
- Specific reporting requirements are reflected in the contract.
- Payment will be based on the supplier's successful completion of milestones as detailed in the contract.
- New intellectual property arising as a result of the contract will be the property of the service provider
- Variations to contract will be in writing and signed by both parties.
- The strategy for exiting the agreement at the end of its term is outlined in the contract.

Contract term

The proposed contract term is ten years. This term was chosen for the following reasons:

- DIA is looking for a long-term relationship with the service provider.
- This will be long enough to allow for algorithm upgrades. Upgrades don't happen very often as it requires long term research and development investment by the supplier.
- A longer term gives time for other agencies across Government to join when they need to.

- Significant initial setup and investment will be needed from the supplier. A 10-year term makes this investment more attractive.
- The market is not anticipated to change significantly enough to repeat this procurement process earlier. This investment from DIA would not be viable during a shorter term.

Key terms of commitment in the contract

Key terms covered in the Master Syndicated Agreement are outline in Table 25.

Table 25. Key terms of the Master Syndicated Agreement

Subject	Description
The Services	Sets out the service catalogue, performance, flexibility, priority, implementation, contracted and future services and resolution of problems. General responsibilities for the provision of facial recognition services, security certification and accreditation and escrow.
Syndication Governance and Terms	Provides clear terms of becoming a Participating Agency and the Lead Agency actions and obligations.
Continuous Improvement	Outlines that the supplier will plan and cater for the continuous improvement of their facial recognition services, and seek to improve its performance under each Participating Agency Agreement, without any additional cost to the relevant Agency.
Liability	Outlines the responsibilities for personnel and subcontractors and indemnification against losses.
Dispute Resolution	Outlines the default, along with the notice and management of disputes for Participating Agencies.
Service Levels	Specifies how performance against Service Levels will be measured and reported; responsibilities in relation to monitoring and remedying Service Level Defaults; and how Service Level Incentive Payments will be calculated and applied.
Liquidated Damages	Sets out that damages that will apply in the event that the final Implementation Milestone is achieved on a date later than the date of the agreed milestone.

Contract management

DIA's long term relationship and contract management of the Facial Recognition Service Agreement will be managed by the Senior Responsible Owner of the Facial Recognition Service. The ICT Procurement Team will provide support in developing the initial contract management plan and a strategic oversight of the contract management and governance moving forward.

Financial Case – Affordability and Funding Requirements

Financial Summary

This project requires a total investment of \$6.500m broken down as follows;

Table 26. Financial summary of the Facial Recognition Replacement

\$'m	FY18/19	FY19/20	All Years
	Forecast	Forecast	Total Budget Required
Opex	0.358	0.142	0.500
Capex	2.147	3.853	6.000
Total	2.505	3.995	6.500

The \$2.147m of Capex for FY18/19 is already included in DIA capital forecasts for FY18/19 and is therefore funded out of the current DIA capital budget. The \$3.853m of additional Capex for FY19/20 is within what was signalled during the initial capital planning round and will be funded out of DIA's capital budget for FY19/20. The Capex forecasts in FY18/19 and FY19/20 include a contingency of \$1.074m.

The \$0.358m of Opex for FY18/19 and \$0.142m of Opex in FY19/20 will be funded from the Passports Memorandum account. The Opex forecasts in FY18/19 and FY19/20 include a contingency of \$0.068m.

Ongoing costs for the preferred option are an average of \$3.917m per annum post implementation (including Depreciation and Capital Charge of \$0.891m per annum). Offsetting this increase are expected benefits of \$0.094m in FY20/21 and an average of \$0.111m per year thereafter.

As these ongoing costs relate to the provision of the Passports service, they will be funded from the Passports Memorandum Account. Periodic fee reviews are conducted on the memorandum account to ensure that fees charged recover costs over the medium to longer term. The next fee review is due for Cabinet consideration in November 2018.

Whole of Life Costs for the Project are \$24.605m, and therefore outside of the Department's delegated authority to approve. Approval by the Minister is required.

Financial Modelling

The project cost breakdown (both Opex and Capex) is outlined in Table 27.

Table 27. Total project cost breakdown

Total Project Cost Breakdown (\$'000s)	FY18/19	FY19/20	Total
Business Analysis & Project Costs	560	565	1,125
FR Service Design and Implementation	1257	1,115	2,372
Technical Design, Integration and Implementation	657	2,158	2,815
Training and Change Management	31	157	188
Total	2,505	3,995	6,500

Details of the financial model as well as ongoing costs and assumptions are in [Appendix I: Detailed Economic and Financial Data](#).

Sensitivity Analysis

Project cost

The sensitivity analysis on this case has been done through a Quantitative Risk Assessment (QRA) which applies a statistically based framework to key cost components to determine a range of costs within given confidence levels. The independent QRA report has a mean (50% confidence level) of \$6.186m - close to the 'bottom-up' estimate of \$6.430m. The 85% confidence level value is \$6.500m. Therefore, an additional contingency of \$0.070m has been added to the project cost; being the difference between the \$6.430m (project estimate) and \$6.500m (85% confidence level value).

Management Case – Planning for Successful Delivery

Project management planning

Project management arrangements

The project will be managed by an experienced project manager using DIA's project management methodology which is based on the PRINCE2™ methodology.

DIA's Technology Services and Solutions branch will manage the project and have identified the team required to work with the preferred supplier to implement the new service. The project roles and responsibilities section provides more details on the team and structure.

The preferred supplier is DXC Technology (DXC) and their Biometric Capability partner, NEC, who will deliver most of the critical skills to implement the Facial Recognition Service. DXC is DIA's current Passport System Suppliers, so a good working relationship already exists, and they have a clear understanding of the changes needed to integrate the facial recognition service with the Passports System. Existing partners (Datacom and other specialists) will be engaged to implement changes in the network, provide privacy assessments and security assurance activities. Changes to operational processes will be managed by the DIA business specialists as part of the change programme.

DIA will use a collaborative approach to deliver the services and manage risks to ensure successful delivery of the service and integration with the Passports System. This collaborative approach will include:

- establishing an integrated project plan, with roles and responsibilities clearly outlined
- regular project meetings and workshops that includes representation from within DIA (business and technical), DXC, NEC and other suppliers delivering for the project
- governance arrangements that facilitate robust decision-making across this arrangement (see [Proposed governance arrangements](#))
- regular risk management and lessons learned workshops.

Team members will be provided with the objectives for the Facial Recognition Replacement Project to ensure they are working towards shared outcomes.

Scope

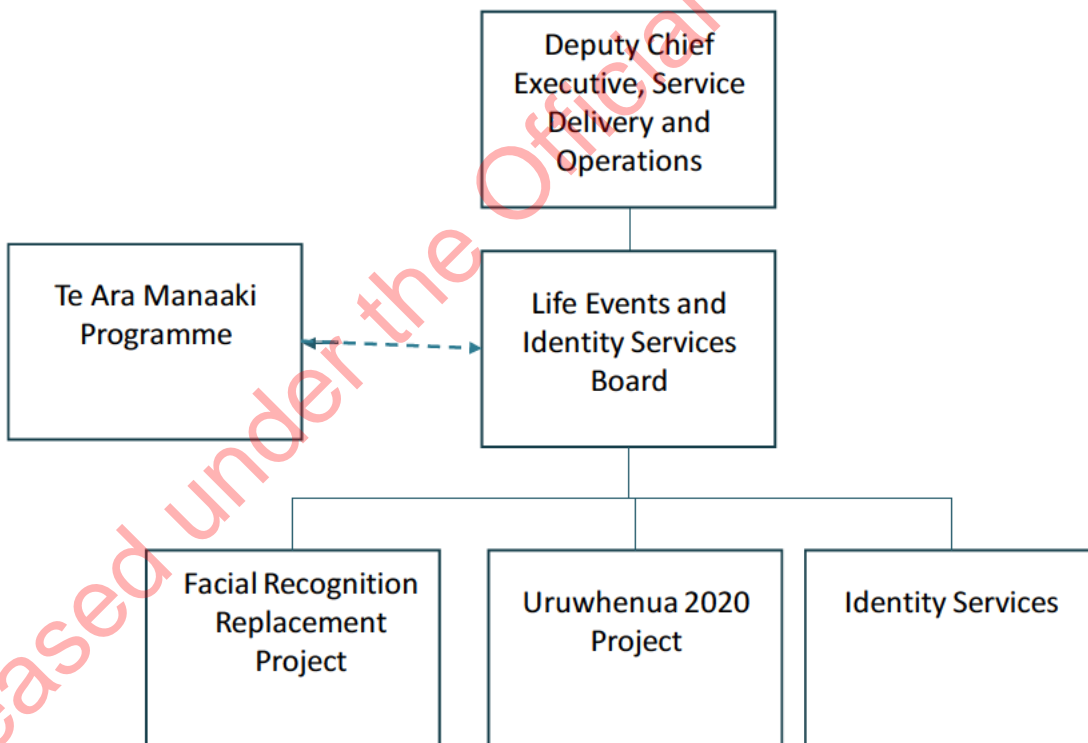
The scope of the Facial Recognition Replacement project is limited to the replacement of the existing facial recognition service and the integrations required with the passport processing system (KIWI). See the Strategic Case [Table 6](#) for a comprehensive summary of the activity and changes that are in and out of scope of the Facial Recognition Replacement Project. The [Magnitude of change](#) section provides an overview of changes as a result of this investment.

Proposed governance arrangements

The project will be governed by the Life Events and Identity Services Board who will:

- provide governance and investment prioritisation across the Service Delivery & Operations Branch's projects approved in the DIA Capital Plan
- provide individual project direction, guidance and support during the project's lifecycle and ensure each project delivers the business case objectives, and the delivered products and services achieve the forecast benefits
- be accountable for ensuring that each project remains on course to deliver the desired outputs to the required quality as defined in the business case
- provide governance across the following three pillars at a consolidated project level:
 - delivery risk and efficiency (forecasted vs actual delivery)
 - optimisation and sound foundation investment including benefits management; and
 - Enterprise risk management eg security, privacy, resilience (disaster recovery and business continuity planning).

Figure 8 shows how the related projects and programmes are governed by the Life Events and Identity Services Board, which has a representative from the transformation programme Te Ara Manaaki. The governance arrangements will ensure there is no overlap in functions and benefits, and

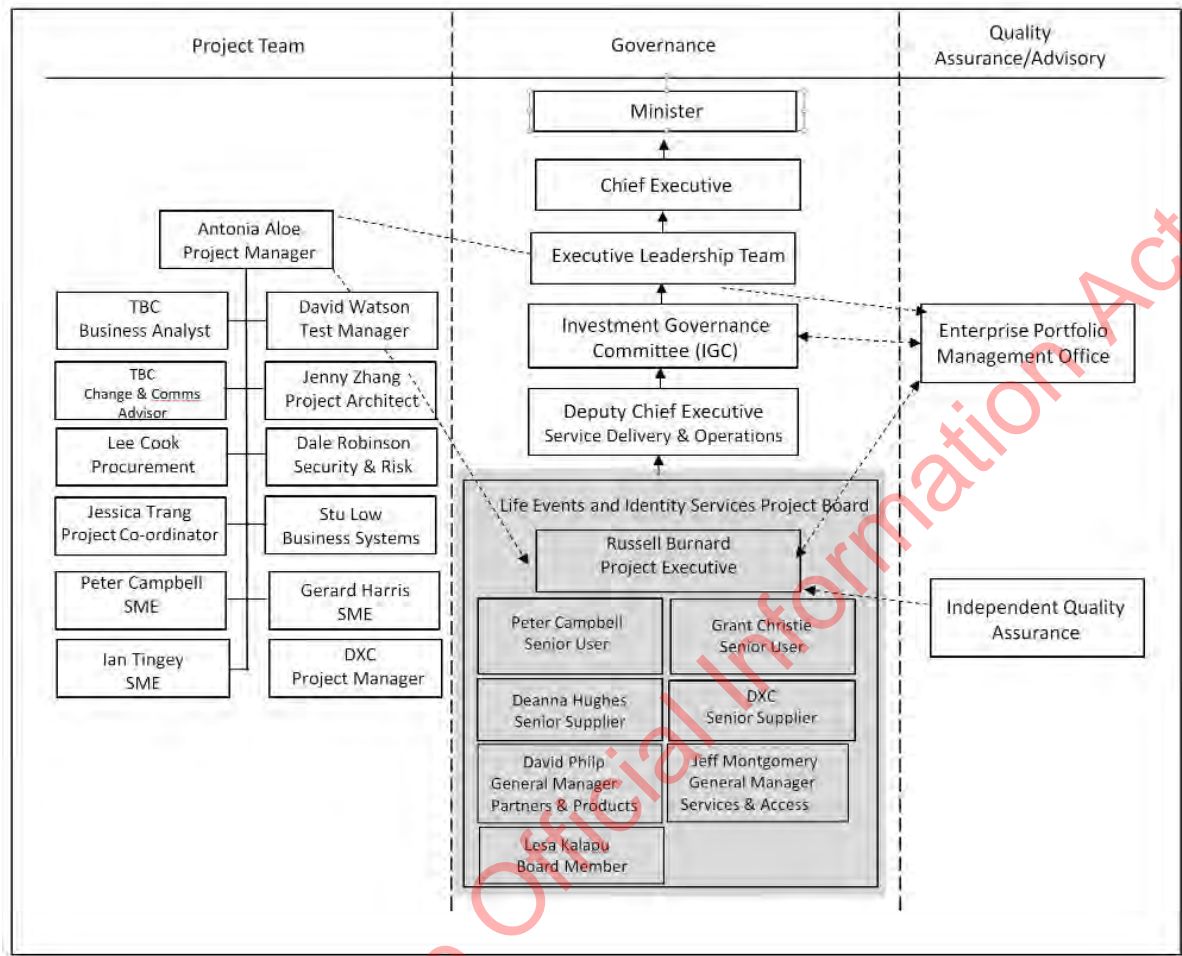


align interdependencies over time.

Figure 8. Life Events and Identity Services Board Scope

Figure 9 shows how the Facial Recognition Project Team and the Life Events and Identity Services Board fits within the broader governance structure of DIA.

Figure 9. Project delivery, governance and quality assurance structure



The Board will include representation from the preferred supplier DXC Technology, and will ensure interdependencies between related projects and programmes are managed, as well as ensuring that risks are managed and benefits are realised. The Board also comprises a range of attendees from across DIA to advise Board members.

The Governance Board members are outlined in Table 28.

Table 28. Life Events and Identity Services Key Board members

Organisation role	Project Role
Key Board Members	
Russell Burnard, Project Executive	Project Executive
Jeff Montgomery, General Manager Services & Access	Business Executive
David Philp, General Manager Services & Access	Business Executive
Peter Campbell, Technical Business Advisor	Senior User
Grant Christie, Manager Service Delivery (Identity & Passport Services)	Senior User
Programme Manager, DXC Technology	Senior Supplier
Deanna Hughes, Delivery Manager SDO	Senior Supplier
Lesa Kalapu, Director Human Resources	Board Member
Attendees	
Antonia Aloe, Project Manager	
Tricia Bond, DXC Project Manager	
Barbara McCallum, Manager Commercial Services	
Ruth Fischer-Smith, Policy Manager	
Sirshen Naik, Finance Business Partner SDO	
John Crawford-Smith, Manager Business Services SDO	
Anna Finlayson, Senior Change Manager, Te Ara Manaaki Programme	
Patrice Price, Senior EPMO Advisor	
John Reynolds, IT Business Partner TSS	
Wayne Gurdler, Service Delivery Manager, TSS	
Secretariat	

The Project Manager will report directly to the Project Executive, Russell Burnard – General Manager Services & Access.

Project roles and responsibilities

All roles and responsibilities required for alignment with the PRINCE2™ / DIA methodology have been assigned, as shown in Table 29. See [Appendix N: Project Team](#) for detail on the core team members' experience and qualifications.

Table 29. Facial Recognition Replacement Project roles and responsibilities

Project role	Name	Key responsibilities
Project Manager	Antonia Aloe	<p>Manage the project on a day-to-day basis.</p> <p>Ensures that the project produces the deliverables to the required standard of quality and within the specified constraints of time and cost, including delivery by DXC and Datacom.</p>
Reporting Project Managers	DXC Project Manager	<p>Manage the implementation of the DXC/ NEC Facial Recognition Service and the DXC KIWI Integration changes.</p> <p>Provide connection between the DXC/NEC and the DIA project teams.</p>
	Datacom Project Manager	<p>Manage the Datacom project team and deliverables including network changes, change and release, Service Support Design package.</p>
Project Architect	Jenny Zhang	<p>DIA Project Solution Architect and Technical Lead.</p> <p>Responsible for technical support, producing and reviewing the architectural design and documentation.</p>
Technical & Business Subject Matter Experts (SMEs)	Peter Campbell Gerard Harris Ian Tingey	<p>Provide SME input and review of project products.</p>
DXC Architect/ Technical Lead	TBC	<p>Facial Recognition as a Service SME.</p> <p>Produces high level design specifications, provide technical support, reviews detailed designs specifications, advises and resolves system architecture and design issues.</p>
Test Manager and Test Analysts	David Watson	<p>Responsible for test governance, producing the test strategy, test plan, managing DIA test activities, defect management process and producing testing handover certificate.</p> <p>Develop test scripts and test execution.</p>
Security and Risk Consultant	Dale Robinson	<p>Provide security and risk advice to the project.</p> <p>Produce business risk assessment, architecture and design review, oversee security testing and review of security test results and certification and accreditation.</p>
Application Support	Stuart Low	<p>Produce technical documentation, prepare for and implement releases, troubleshooting, system testing.</p> <p>Review change management and other technical documentation for deployments.</p> <p>Support testing services.</p>

Project role	Name	Key responsibilities
Business Analyst	TBC	Manages all new requirements and amendments under change control. Liaising with all project team members to provide input and to translate business requirements to support processes, change and technical requirements and activities.
Change & Communications Advisor	Te Ara Manaaki Change Advisor	Produce all change and transition deliverables. Manage all business change and project communications to align approaches and timing with the Te Ara Manaaki Programme and the FR Project.
ICT Procurement Specialist	Lee Cook	Manage procurement process, contract negotiations and contract management plan. Provide procurement advice to the project. Review and updating of existing contracts for services impacted by the implementation of the Facial Recognition Service.
Project Coordinator	Jessica Trang	Provide project support.

Lessons learned from other projects and the preferred suppliers

The project team have drawn on the experience of a number of previous projects in DIA, other NZ agencies, and DXC and NEC's experience delivering Passport related projects and Facial Recognition solutions. See [Appendix O: Best Practices derived from Lessons learned](#) for the best practises to prevent common pitfalls that have been incorporated into the project approach.

Two specific lessons from the previous implementation in 2012 have been addressed in this project. These have both been addressed as Commercial Risks and are mitigated through the contract.

- The earlier implementations of facial recognition services at DIA had issues with the performance experienced by users, and required time to diagnose the source of these issues and resolve them. This specific risk was added to the risk register and will be mitigated by performance testing well before the scheduled "go live" date to ensure any performance issues are addressed before the system goes into production.
- The current software supplier was acquired by a larger competitor and the solution discontinued. To mitigate this risk in future, preference was given during the selection process to larger suppliers, and the contract will specify protection clauses for DIA against software vendor buy out.

Project approach

The project approach has been developed after discussions with the preferred suppliers. Given that the requirements are well known due to previous service experience, a waterfall approach is the preferred methodology. This approach enables complete design and development during one stage, followed by comprehensive testing before transition into production.

In line with the lessons learned from the other projects, the following best practises will be followed during the project:

- The project plan will be updated at each stage with detailed stage plans
- Collaboration between DIA, DXC and NEC, and other delivery resources to develop the plan, ensure there is a shared understanding of the plan, roles and responsibilities and interdependencies.
- Seek out and learn from previous experience – this will include incorporating lessons learned for previous projects that DIA, DXC and NEC have been involved in and running lessons learned workshops throughout the project
- Involve the right people at the right time – this includes business users being engaged throughout the design and development of the solution
- Ensuring end to end performance testing, pilot user testing and user acceptance sign off is completed prior to “go live”.

Project plan and milestones

Figure 10 shows all project stages, with Stage Gate approvals by the Portfolio Board once key milestones are delivered. Detail on the purpose of each stage along with milestones and deliverables are outlined in [Appendix P: Facial Recognition Replacement Project Stages](#).

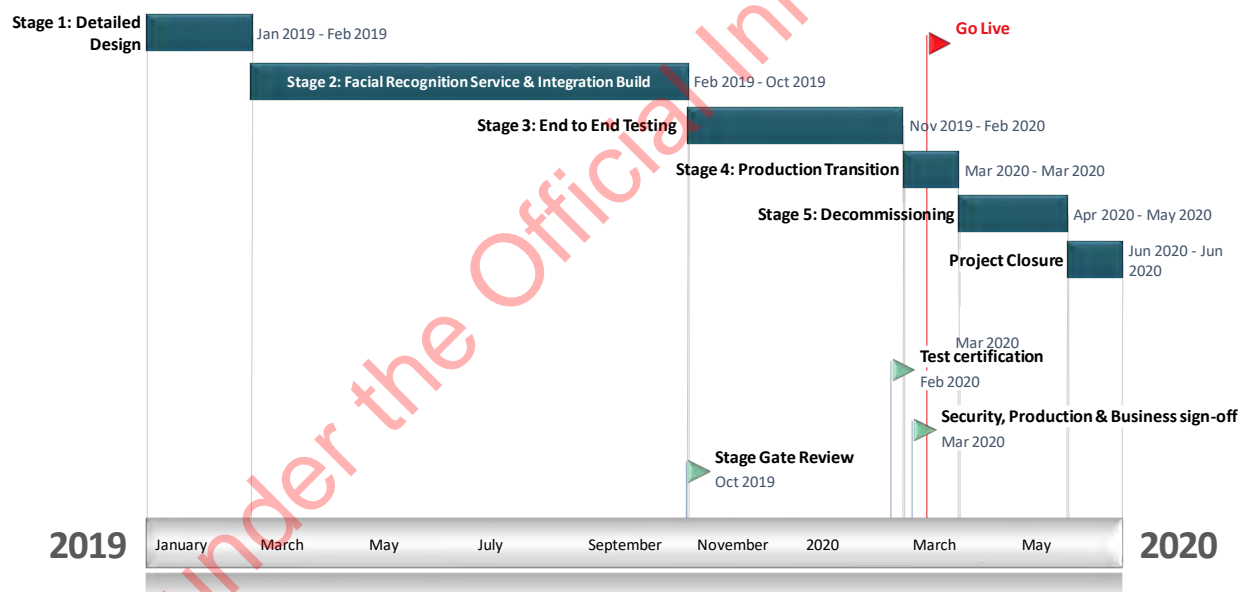


Figure 10. Facial Recognition Replacement Project approach and timeline

Milestones have been designed into the project plan for achievement of significant investment objectives or steps, enabling decision makers to assess at these points whether the project should be stopped, continued, delayed, or accelerated.

Table 30. Facial Recognition Replacement Project key milestones

Key Project Milestone	Approximate Date
Business Case Approved	December 2018
Suppliers Contracts Approved	December 2018
Commence Implementation Phase	14 January 2019
Architecture and Detailed Designs complete	26 February 2019
Facial Recognition Service Build, Install and Configuration complete	6 September 2019
Facial Recognition Integration with Passports System Build complete	15 October 2019
DIA QA Environment deployment complete	6 November 2019
DIA Facial Recognition Service & Passport Systems End to End Testing complete	23 January 2020
Facial Recognition Service/Passport Systems Security, Performance, Rehearsal/DR Testing complete	21 February 2020
Production Transition (Go Live)	9 March 2020
Go Live Support & Warranty ends	22 April 2020
Decommissioning activities complete	5 June 2020
Project Closure	30 June 2020

Enabling a smooth transition and off ramps

Ensuring that the facial recognition capability remains available to support passport production is critical. The project will do this by:

- extensive end to end performance testing, user testing and business acceptance sign off prior to production transition
- Conducting a full production data migration in the Facial Recognition Service Production environment during the build, configuration and testing stages to verify data integrity, tuning and optimising of the thresholds and environment and to confirm the assumptions used for benefits realisation prior to production transition.

This approach provides off-ramps (the option for DIA to exit the contract) at the end of testing and at the end of the production data testing run if significant issues that cannot be addressed are identified.

Key constraints and dependencies

Constraints

The main constraint for the project is the availability of business subject matter experts to review project deliverables, participate in user testing and go live support. Multiple projects including Uruwhenua 2020, Identity Services and Te Ara Maanaki are underway and delivering along the same timelines with changes that affect the passport system users, creating potential bottlenecks for change. The project manager will work together with the other major change projects to co-ordinate change and alleviate this constraint. The Life Events and Identity Services Board will determine priorities if clashes arise.

Dependencies and interdependencies

There are currently no hard dependencies that would prevent the implementation of the Facial Recognition Replacement Project and achievement of its benefits.

Te Ara Manaaki is a major transformation programme that will be delivering over a similar timeframe to both the Facial Recognition Replacement Project and the Uruwhenua 2020 Passport Personalisation project and the wider Identity Services Portfolio. The changes to be delivered by the projects will be planned, scheduled and coordinated. The SDO Capital Plan & Te Ara Manaaki Dependency Map will be reviewed and updated regularly through the course of the projects. This will form part of the regular reporting to the Life Events and Identity Services Board.

Change management planning

The strategy, framework and plan for dealing with change management is described below.

Change management approach

The change management approach will be based on PROSCI ADKAR model of change, a recognised best practice change management model. The change will be supported by the project team, a change and communications advisor and a more detailed change management plan that will include Stakeholder Engagement, Communications and Training Plans. These plans will be completed and approved by the Portfolio Board during the detailed design and build stages of the project and updated throughout the project.

The impact of change resulting from implementing the new facial recognition capability is envisaged to be low to medium across people, business process, technology, suppliers and external stakeholders. These change impacts are described in the Magnitude of Change section. Because the changes for staff are minimal, engagement will mainly be through stakeholder communications.

To ensure alignment with others changes in SDO, the project will work closely with the Te Ara Manaaki change management team, the SDO Human Resources Business Partner, the SDO Capability Team and the relevant managers in the Services and Access and Operations Teams.

The project team includes SME's from the SDO Operations Services Team. Power users from these teams and Services and Access will also be nominated and involved in providing input and review of products, training material, business acceptance testing, operational readiness and go live support. This will ensure people and their representatives are informed and involved in project related activities and minimise any impact to delivery of services.

The project will work closely with ICT Procurement, Technology Solutions & Services, SDO System Owner & Commercial Portfolio Manager, the preferred supplier and Service Desk to ensure that the new service is set up for success.

Stakeholder Engagement & Communications

A Stakeholder Engagement and Communications Plan has been developed to coordinate and align engagement and communications activities in support of the implementation of the new facial recognition service with other key programmes of change such as Te Ara Manaaki and Uruwhenua.

The project's internal stakeholders include all people potentially impacted by the implementation of the new Facial Recognition Service. Priorities include governance groups, senior leaders and managers from the Services and Access, Operations and Products and Partnerships Groups within the Service Delivery and Operations Branch, managers across Shared Services Branch and subject matter experts.

The project's external stakeholders include other government agencies with an interest in adopting the shared facial recognition service contract that DIA will set up, the Corporate Centre, Government Ministers and suppliers.

Training

It is anticipated that there will be minimal training required for Passport System users. Engagement with system users will primarily be through communications.

Training will be provided by the supplier for the Investigations Team and DIA's TSS branch Application Support team who provide second level support for the Passports System and the new Facial Recognition Service. SDO branch's Capability Team will work together with the Investigations SME, using training collateral from the supplier, to help develop the training material for the new functionality to be used by the Investigations Team.

Magnitude of change

The following table summarises change across key areas.

Table 31. Facial Recognition Replacement Project change impacts

Area	Known Impacts
Process	<p>The passport issuance process is expected to remain unchanged.</p> <p>However, it is anticipated that the accuracy of the facial recognition algorithm will result in processing efficiencies for Identity & Passport Officers as fewer false matches will be presented to an Officer for a manual decision.</p> <p>The project will align its change approach around staff behavioural shifts with the work planned by Te Ara Manaaki.</p> <p>The project will work together with Operations to update the relevant processes, policies and procedures to reflect the new facial recognition service. However, any updates are envisaged to be minor as there will be no re-engineering of processes.</p>
Standards / policies / legislation	<p>No change to legislation is required, as the new system will operate within existing legislation.</p> <p>No anticipated impact on security, privacy and risk from the implementation of the changes across SDO or the Department. This will be confirmed through the project delivery.</p>

Area	Known Impacts
User interfaces	<p>The Passport System's user interface is not expected to change for the up to 250 Identity & Passport Officers and Customer Services Officers.</p> <p>The Investigations solution will change and training will be provided for the seven members of the Investigations Team.</p> <p>Four members of the Data & Technical Capabilities Team will also require training on the new Facial Recognition Service.</p>
Organisational and Staff	<p>No impact on the Department's structure.</p> <p>There is a productivity benefit that will be realised by reducing the number of hours spent on the facial recognition process for a passport application. In 2020, the latest forecast demand will be assessed to determine how these benefits will be reflected in staffing numbers – either through avoidance of staff increases or staff reductions. The impact on staff would be minimal.</p>
External Stakeholders	<p>Other agencies such as MBIE, Customs, Police, will have the opportunity to join the Open Syndicated Agreement.</p>

Systems and Technology Changes

Some of the key changes for the system and technology area include;

- Shift from an on-premise solution to a capability provided as a managed service
- Replacement of the Investigation Team's Facial Examiner Workstation with the Investigations interface provided as part of the Facial Recognition Service.
- The DIA Applications Support Team, who provide second level support will require training on a new system.
- Replacement of integrations between the Passport system and the Facial Recognition system.
- The preferred supplier for the Facial Recognition Service is also the supplier for the Passports System, KIWI, so a good working relationship already exists. The two diagrams below outline the architectural scope of Systems and Technology change for the Facial Recognition Replacement Project. Figure 11 shows the current facial recognition components and Figure 12 the proposed future state architecture.

9(2)(k)



Figure 11. Current facial recognition components

9(2)(k)



Figure 12. Proposed future state architecture for facial recognition in passports

Engaging users / the business

The project will engage users by:

- including two Business subject matter experts from the SDO Operations Group (Technical SME and Investigations SME) on the core project team. Other SMEs will be approached as required to provide specific input e.g. into thresholds, business assurance and risk advice.
- including representatives from Services and Access Delivery Teams, Operations Business Services Team (Technical and Investigations team) in business acceptance testing, developing training material, and being power users for their teams following Go Live.
- working closely with the Investigations SME and Application Support project resource to ensure they are provided adequate training prior to Go Live.
- stakeholder engagement and communications will be delivered to users and the business throughout the project. Specific communications will be delivered to users in Services and Access, Operations and Application Support who will be directly impacted by the new Facial Recognition Service.

Benefits management planning

The summarised Benefit Management Plan is shown in [Appendix F: ILM and Benefit Management Plan](#). Individual Benefit Profiles (IBPs) will be developed as part of the project Benefit Realisation Plan (BRP). These will include:

- The Benefit Owner – the person accountable for the realisation of the benefit
- The Measure Owner(s) – the person(s) responsible for the monitoring and tracking of the measures
- Key performance Indicators and Measures
- Baseline values
- Target values
- Realisation dates

The Benefit Realisation Plan will continue to be updated during the testing phases to ensure alignment of expected benefits with the actual results from the new system. Any variation to expected results that require changes to the benefit management plan targets will be referred to the board for decision.

After the system is in production the Project Executive will report on realised benefits to the Investment Governance Committee every six months, with full benefit realisation expected one year after the system is in production.

Risk management planning

The project's risk register lists the current rating, status and treatment for all identified risks. The risk register will be continuously updated and reviewed throughout the project, in line with DIA EPMO delivery control standards. The major environmental uncertainties have been reviewed in the Strategic Case, and the major Commercial Risks have been reviewed in the Commercial Case. Table

32 shows the higher probability and impact project management risks that remain. Both the first and third risks are to do with the amount of change that the Service Delivery Organisation of DIA is undergoing. Over the next two years, Te Ara Manaaki, Identity Services, and Uruwhenua 2020 will be introducing changes to SDO systems, at the same time as the Facial Recognition replacement project is delivering.

To manage this risk, the changes to be delivered by the four projects will be planned, scheduled and coordinated, in consultation with SDO senior users, testing, change and release, and business change management. The SDO Capital Plan & Te Ara Manaaki Dependency Map will be reviewed and updated regularly through the course of the projects. Detailed design activities will occur in the same quarter and lead by the SDO Projects Architect (who is architect for the Uruwhenua 2020, Facial Recognition Projects and Identity Products projects) and involve the Te Ara Manaaki Project Architects. This activity will identify any overlaps, confirm delivery scope, system, process and people change impacts that need to be assessed, planned and managed. Change management will be planned and co-ordinated together with the Te Ara Manaaki change and communications activities. The Change Advisor will be resourced from the Te Ara Manaaki change management team. Decisions around contention resolution and prioritisation will be made by the SDO senior management team.

Table 32. Key risks to delivery for the Facial Recognition Replacement Project

Risk Description	Estimated Impact	Consequence Minimal → Severe	Likelihood Almost never → Almost certain	Treatment
<p>If there is too much change introduced or implemented simultaneously into the DIA (business and technical) environment, then managers and staff may not be focused on the implementation and business preparation activities for the new Facial Recognition Service capability.</p> <p>SD01200_R_11</p>	1-2 months delay	Moderate	Possible	Co-ordinate and manage dependencies, business change and system releases across the SDO portfolio, Te Ara Manaaki Uruwhenua and BAU changes.

Risk Description	Estimated Impact	Consequence	Likelihood	Treatment
<p>If the new system does not perform as expected, then additional time and budget may be required to resolve the issues.</p> <p>Potential drivers of the non-performance include issues around Integration of the Facial Recognition Service and wider Passports System, as well as the new service itself</p> <p>SDO1200_R_18</p>	<p>Estimated additional cost of \$265k per month for FR Service and integration and up to 8 weeks to resolve.</p> <p>Actual costs will depend on severity of issue.</p>	Moderate	Possible	<p>Performance Test plan agreed with supplier and DIA Test team.</p> <p>Strong service level agreements agreed with the supplier, including penalties for non-delivery.</p> <p>One Prime Contract ensure responsibilities are clear and supplier can be held accountable.</p>
<p>If there is contention with other projects (TAM, Identity Services and Uruwhenua) and BAU changes for the pre-production QA environment, then this may delay QA deployments and testing of the Facial Recognition Service and Integrations, and incur supplier and resource costs where these resources cannot be reallocated</p> <p>SDO1200_R_16</p>	<p>1-2 months delay, up to \$365k per month increase on budget</p>	Moderate	Possible	<p>Plan and agree environment and release schedules and required resources with managers, and monitor and manage any slippages across all release candidates.</p>

Issues identified

The table below shows the issue identified for the project and how this will be resolved.

Table 33. Facial Recognition Replacement Project issues

Issue Description	Estimated Impact	Impact rating (consequence) Minimal → Severe	Resolution activity
There is only one pre-production (QA) environment for the Passports System that is shared for all relevant changes. The prioritisation of this change will be contending with other projects and BAU changes for the pre-production QA environment. This may delay QA deployments and testing of the Facial Recognition Service and Integrations, and incur supplier and resource costs where these resources cannot be reallocated	1-2 months delay, up to \$365k/ month increase on budget	Moderate	Plan and agree environment and release schedules and required resources with managers, and monitor and manage any slippages across all release candidates.

Project and business assurance arrangements

The project will adopt an integrated assurance approach during project planning and throughout the life of the project as follows:

- Day to day project management processes and controls based on the Department's Prince2 based project management methodology and DIA financial management practices being consistently applied
- Internal governance and oversight of the project, including signed terms of reference for all governance bodies.
- Business and system security risk assessments, privacy risk assessments, independent quality assurance reviews and assurance deliverables being reviewed and approved at key milestone and stage gates determined within the project.

The approach will provide the Project Executive with assurance at key decision points, such as prior to go-live requests and deliver stage gates. This approach will give the Department assurance that the project is on track to deliver, and will give early indications if there are emerging issues and provide advice on managing and resolving them.

The key assurance activities that will be performed for the project are summarised in Table 34. A complete list of all assurance activities are listed in [Appendix Q: List of Assurance Activities](#).

Table 34. Key Assurance Activities

Assurance Activity	Purpose	Audience	Assurance Provider	Frequency date scheduled
--------------------	---------	----------	--------------------	--------------------------

Assurance Activity	Purpose	Audience	Assurance Provider	Frequency date scheduled
Life Events & Identity Services Board Meetings	Review project status, provide direction and respond to escalated issues and risks	SRO / DCE	Project Executive	Monthly
Quantitative Risk Assessment (QRA)	Provide review of the project's financial model, and provide information on the appropriate setting of the contingency, and budget tolerance.	Investment Governance Committee, Project Executive, Treasury	Ascent Business Consulting Ltd	August 2018 – to be included in Financial Case/ SSBC
Independent Quality Assurance (IQA)	Provide independent assurance that the Project is being managed in accordance with good practice.	Project Executive, Project Board, EPMO, Investment Governance Committee, Corporate Centre	EPMO	Prior to Implementation Business Case submission (November/December 2018)
Stage Gate Reviews	To review performance of stage, and provide approval to proceed based on project deliverables being completed to the appropriate quality standard.	Project Executive, Portfolio Board, EPMO	Manager Project Delivery SDO	At the end of each project stage (as specified in the PID)
Security risk assessment and Certification & Accreditation	To assess the design, implementation and controls for the Facial Recognition Service against DIA security polices and standards and NZISM.	Project Executive and Senior Users Chief Security & Risk Officer	Security & Risk	Pre-requisite for production transition
Production Transition Acceptance	To provide assurance that all the technical and stakeholder pre-requisites for production transition have been approved, and the operational teams that will receive and use the capabilities are ready to receive the change.	Project Executive, Project Board, TSS Management,	Technical Approval Board Change Approval Board	Prior to Production Release

Post-project evaluation planning

A post project review is planned for 6 months post-Go Live. This review will focus on the implementation of the project with the objective of assessing the success of the project, the tracking of benefits and to evaluate benefits realisation realised at the time of the review.

Next Steps

This business case seeks formal approval to:

- **Approve** investment of one off capital of up to \$2.15 million in 2018/19 and up to \$3.85 million in 2019/20;
- **Approve** investment of one off operating expenditure of \$0.36m for 2018/19 and \$0.14m in 2019/20 to replace the current facial recognition software which is no longer supported;
- **Approve** investment of ongoing operating expenditure of \$3.92m (including Depreciation and Capital Charge of \$0.89m) per annum to ensure DIA can continue reliable and secure production of passports;
- **Endorse** the project finalising the contract for the syndicated procurement of Facial Recognition Services in line with the costs approved above;
- **Note** that in the event the scope or cost of the final contract changes materially, the project team will present the new contract and memo to the Investment Governance Committee for endorsement prior to being tabled with the Minister of Internal Affairs for approval; and
- **Note** that operating expenditure for this investment will be funded from the Passports Memorandum Account; and
- **Note** whole of life cost for the project is \$24.60m.

On approval of the business case, our next steps are:

- finalise contract negotiations
- commence project implementation (subject to approvals).

Appendix A: Chief Executive's Letter

September 2018

To whom it may concern

Facial Recognition Replacement Business Case

This Business Case is a significant deliverable of a strategic project by the Department Of Internal Affairs to investigate value for money options to meet its future operational requirements.

I confirm that:

- I have been actively involved in the development of the attached investment proposal through its various stages
- I accept the strategic aims and investment objectives of the investment proposal, its functional content, size and services
- the indicative cost and benefit estimates of the proposal are sound and based on best available information
- the financial costs of the proposal can be contained within the agreed and available budget
- the organisation has the ability to pay for the services at the specified price level, and
- suitable contingency arrangements are in place to address any current or unforeseen affordability pressures.

This letter fulfils the requirements of the current Better Business Cases guidance. Should either these requirements or the key assumptions on which this case is based change significantly, revalidation of this letter of support should be sought.

Yours sincerely

Peter Murray



Acting Chief Executive

28.9.2018

Department of Internal Affairs

Released under the Official Information Act 1982

Appendix B: Glossary of Terms and Abbreviations

Term	Description
ABIS	Automated Biometric Identification System. Existing Facial Recognition technology used by IPS. Technology is supplied by Idemia
DIA	Department of Internal Affairs
FEW	Facial Examiner Workstation used by the investigations team on a daily basis to complete work
FR	Facial Recognition
FRAP	Facial Recognition Application Process, a batch tool that runs periodically to enrol applicant images submitted via PPTS to ABIS.
FTE	Full Time Equivalent. Measurement of full time staff
Gallery	A collection of enrolled images, typically in a database, upon which a search request is performed.
ICAO	International Civil Aviation Organisation. The organisation responsible for Passport standards.
Identification Rate	The proportion of genuine identification attempts for which the correct enrolment is returned in the candidate list for an identification search.
Identification Search (1: many)	Comparison of one image against all images in a gallery to determine if there is a matching image in the gallery.
IPS	Identity and Passport Services business unit.
IPLS	Image Processing Lookup System, DIA legacy watch list system by Face4Systems
KIWI	Keeper of identity with Integrity. DIA's current travel document application processing system
Many: Many	Comparison of all images with all images held in the gallery
Match	When the biometric system determines that two or more biometric samples are from the same source at a predefined threshold.
PCC	Photo Capture Client for KIWI
PIC	Photo Image Capture, a component of the legacy Personalisation System used to capture the book images for printing on the travel document ^{9(2)(k)} [REDACTED] [REDACTED] PIC is used to support PPTS.
PIMS	Personalisation Interface Management System for passports. This is the interface between PPTS and passport personalisation system.
PPTS	Passport Processing Transformation Systems, legacy Passports application processing legacy system. Some of the travel document applications types can only be processed in PPTS. PPTS is the old source of truth for passports applications, persons registry and travel document lifecycles. It also supports travel document stock management.

Term	Description
Threshold	Value selected as the operating point of the system. The decision point which determines the trade-off between the FMR and FNMR metrics.
Verification (1:1)	Comparison of one image with another image to determine if they are the same identity.
Verification Rate	The proportion of genuine verification attempts for which the sample is correctly matched to image of the user.
Failure to enrol (FTE)	If the failure occurs during enrolment, it is known as a failure to enrol. The proportion of enrolment transactions that fail is known as the failure to enrol rate (FTE).
Failure to acquire	If an error occurs while acquiring the biometric sample during a verification or identification; it is known as a failure to acquire. The proportion of verification or identification attempts that fail for this reason is the failure to acquire rate (FTA).
False non-match	A genuine match that is declared to be a non-match. This is due to the match receiving a score below the match threshold.
False match	An impostor match that is declared to be a match. This is due to the match receiving a match score above the match threshold.
False non-match rate (FNMR)	The probability that a sample will be falsely declared not to match a template from the same user. A false non-match is sometimes called a "false negative"
False match rate (FMR)	The probability that a sample will be falsely declared to match a single randomly-selected "non-self" template. A false match is sometimes called a "false-positive".
9(2)(k)	9(2)(k)

Appendix C: High-level principles and requirements for the facial recognition service

The principles below have been taken from the *Guiding Principles for the Use of Biometric Technologies for Government Agencies* (2009).

Guiding Principles Described

GP1. There is a justified use of biometric technologies for identity-related processes.

Agencies must critically evaluate the need to use biometric technologies for identity-related processes to ensure that it is the most appropriate and cost effective solution and there is no suitable equivalent alternative that meets the business needs. An agency must justify its decision to use biometric technologies.

GP2. The use of biometric technologies for identity-related processes must be lawful and appropriately authorised.

Biometric technologies deployed must be:

- consistent with specific enabling legislation or appropriately authorised by the relevant persons when used specifically within an agency
- fully compliant with the relevant New Zealand laws, particularly with regard to the Privacy Act 1993, the New Zealand Bill of Rights Act 1990 and the relevant international laws.

GP3. Consideration should be given to identify opportunities to collaborate with other agencies and stakeholders.

Opportunities for inter-agency or stakeholder collaboration should be considered as early as possible in the process. Examples of collaboration include:

- sharing infrastructure
- common design between systems
- interoperability
- joint business case/budget bid
- joint procurement
- implementing pilot programmes.

GP4. Consideration must be given to the end users²⁸ of any business processes that will include biometric technologies.

Appropriate consultation must be undertaken with the end users of any business process that will include biometric technologies. The extent of consultation is likely to vary according to the different circumstances in which the biometric technologies are proposed to be used (eg law enforcement, opt-in or mandatory).

²⁸ “End User – the individual who will interact with the system to enrol, to verify or to identify.” Source: Biometrics Glossary, National Science and Technology Council (NSTC), 14 September 2006.

Information gathered from consultation, such as social and cultural considerations, accessibility issues or constraints, should inform the type of biometric to be selected.

This information should also inform the development of requirements for the biometric technologies and implementation details. Examples of implementation details include different operational procedures, which may need to be developed when taking into consideration different cultural sensitivities, accessibility issues or other specific needs identified by different groups in the community.

GP5. The biometric technology used must be appropriate and meet the purposes for which it is designed.

Thorough research must be undertaken to identify the range of biometric technologies that can appropriately meet the business requirements. The effectiveness and weaknesses of these alternatives must be understood, as well as the expected benefits and costs. This will ensure that the biometric technologies that will be used are appropriate and proportional to business requirements.

Note: It may be desirable to use proven or tested technology to ensure future proofing.

GP6. Relevant domestic and international obligations must be met.

Agencies must have regard to, and demonstrate compliance with, domestic and international obligations. These obligations could include treaties and international agreements, United Nations conventions and those from relevant organisations such as the International Air Travel Association (IATA).

GP7. Stewardship of biometric information must be robust with supporting systems and processes established and maintained.

The stewardship and integrity of the biometric information that is collected, stored or used by agencies must be robust. Biometric information must be secure and only used by agencies as authorised by the end users of the biometric technology or as permitted by law.

End users and agencies could be provided with information about this where appropriate.

Ongoing governance of data, systems and processes is required.

Implementation Principles Described

IP1. Appropriate information should be provided to end users and appropriate consultation shall be undertaken with end users and stakeholders.

End users should be provided with information about biometric technologies, their purpose, their expected benefits, the issues with biometrics, management of their information once collected and stored and their rights over this (including their rights under the Privacy Act 1993).

End users should be consulted, if appropriate, as early as possible to gain their views on implementation issues including usability, cultural considerations, and privacy. As implementation issues are not limited to end users, other relevant stakeholders, such as system implementers, designers, technicians and system operators should also be consulted as they can also provide valuable input.

IP2. Core processes and procedures associated with the use of the biometric system by a user²⁹ and end user must be established.

Processes and procedures must be established to manage all aspects associated with the use of the biometric system. These would cover, but are not limited to, the following:

- how to collect, convert, store, compare, make decisions about biometric matches or dispose of biometric information
- data access security levels
- the circumstances relating to the disclosure of biometric information, noting that the information collected must be used only for the purposes for which it was gathered or as permitted by law
- exception handling for false positives, false negatives, problems with biometrics provided such as end users unable to use the biometric technologies, or damaged storage devices
- resolving problems with the biometric system
- resolving issues/complaints raised by end users
- system failure
- security
- regular auditing of the biometric system and processes
- staff training.

Processes and procedures must be established to ensure compliance by users and end users and to ensure that the usage of biometrics does not expand beyond that authorised, ie safeguard against scope creep.

IP3. The life cycle of biometric information must be managed and secure.

Agencies must apply the relevant legislation and standards for the management of the biometric information collected. All appropriate steps must be taken to ensure biometric information collected, stored and used is appropriately protected by reasonable security safeguards against risks, such as loss or unauthorised access, destruction, modification or disclosure.

Independent audits and reviews are recommended to ensure the information collected, stored and used is consistent with the purposes for which it was collected. Privacy impact assessments must be completed at the outset of the project and periodically reassessed and updated to take account of changes, for example, legislation, policies, business requirements or other agreements. Refer to www.privacy.org.nz

IP4. Best practice procurement processes should be applied.

In keeping with existing government procurement policies and guidelines, agencies procuring biometric technologies/systems should:

²⁹ User – A person, such as an administrator, who interacts with or controls end users' interactions with a biometric system. Source: Biometrics Glossary, National Science and Technology Council (NSTC), 14 September 2006.

- undertake detailed scoping and definition of requirements in consultation with relevant agencies and stakeholders (where relevant)
- investigate opportunities for collaborative procurement, eg joint procurement
- investigate the option of utilising existing contracts negotiated by other agencies.

These steps aim to achieve best value for agencies and government as a whole and will assist to inform procurement decisions.

IP5. Standards for interoperability should be followed where appropriate.

The relevant domestic or international standards (both technical and operational) should be followed by agencies to enable national and international interoperability between systems and like/similar jurisdictions, where appropriate, eg ISO/IEC 19785 Common Biometric Exchange Formats Framework.

IP6. Information matching and sharing must be legal.

Prior to any information matching or sharing occurring between any agencies, each agency must ensure the legislative authority and the necessary agreements are in place and the persons affected have been appropriately informed – refer to Privacy Act 1993, Schedule 4 – Information Matching Rule 1.

Appendix D: Privacy Assessment

Privacy risk assessment

Some types of initiatives are more likely to create privacy risks. If the initiative involves one or more of these risk areas, it's likely that a Privacy Impact Assessment will be valuable.

Use the following checklist to identify and record whether your proposal raises certain privacy risks. Delete any that do not apply.

Does the initiative involve any of the following?		Yes (tick)	No (tick)	If yes, explain your response
Information management generally				
A substantial change to an existing policy, process or system that involves personal information		<input checked="" type="checkbox"/>	<input type="checkbox"/>	This is an entirely new system (even though it is performing the same functions as a previous system).
Any practice or activity that is listed on a risk register kept by your organisation		<input checked="" type="checkbox"/>	<input type="checkbox"/>	The FRS is part of the Passports System. As part of the FRS Certification and Accreditation process risks are identified and controls applied. Any Residual Risks are included in the certificate for acceptance by the Business Owner and DCE. An initial Risk Assessment has been performed for FRS, this will be updated once a Service Provider has been selected and the system design is known.
Collection				
A new collection of personal information		<input type="checkbox"/>	<input checked="" type="checkbox"/>	
A new way of collecting personal information		<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Storage, security and retention				

Does the initiative involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
A change in the way personal information is stored or secured	✓		In ABIS the biometric template is stored with a small amount of biographic information for 'binning' purposes (filtering). This is limited to Gender, Date of Birth, Place of Birth and Country of Birth. This will NOT be stored in the new FRS system. In the new system both images and biometric templates will be stored together to improve functionality and operational efficiency. In the current system (ABIS) there are no stored images.
A change to how sensitive information is managed		✓	
Transferring personal information offshore; using a third-party contractor or Cloud storage	✓		Data will not be transferred offshore. At this stage in the RFP process there is the potential to use third party contractors and cloud storage. This will be risk assessed during the RFP evaluation.
A decision to keep personal information for longer than you have previously		✓	
Use or disclosure			
A new use or disclosure of personal information that is already held		✓	
Sharing or matching personal information held by different organisations or currently held in different datasets		✓	
Individuals' access to their information			
A change in policy that results in people having less access to information that you hold about them		✓	
Identifying individuals			
Establishing a new way of identifying individuals		✓	
New intrusions on individuals' property, person or activities			

Released under the Official Information Act 1982

Released under the Official Information Act 1982

Does the initiative involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
Introducing a new system for searching individuals' property, persons or premises		✓	
Surveillance, tracking or monitoring of movements, behaviour or communications		✓	
Changes to your premises that will involve private spaces where clients or customers may disclose their personal information		✓	
New regulatory requirements that could lead to compliance action against individuals on the basis of information about them		✓	
List anything else that may impact on privacy, such as bodily searches, or intrusions into physical space		✓	

Released under the Official Information Act 1982

Initial risk assessment

If you answered "Yes" to any of the questions above, use the table below to give a rating: **Low (L)**, **Medium (M)**, or **High (H)** – for each of the aspects of the project set out in the first column. For risks that you've identified as Medium or High, indicate (in the right-hand column) how the project plans to lessen the risk (if this is known).

If you answered "No" to all the questions in the privacy risk assessment above, move on to the Summary section below.

Privacy Principle affected	Rating (Low, Medium, High)	Describe any medium and high risks and how they will be mitigated
Level of information handling L – Minimal personal information will be handled M – A moderate amount of personal information (or information that could become personal information) will be handled H – A significant amount of personal information (or information that could become personal information) will be handled	High	This system will hold biometric data and images for approximately 4.5 million individuals. A risk assessment has been carried out and appropriate controls will be implemented, e.g. separation of biometric and biographic data, assurance testing of the system, strict controls on physical and logical access. This will be documented and recorded in a FRS Service Security Certificate.
Sensitivity of the information (eg health, financial, race) L – The information will not be sensitive M – The information may be considered to be sensitive H – The information will be highly sensitive	Low	
Significance of the changes L – Only minor change to existing functions/activities M – Substantial change to existing functions/activities; or a new initiative H – Major overhaul of existing functions/activities; or a new initiative that's significantly different	Low	

<p>Interaction with others L – No interaction with other agencies M – Interaction with one or two other agencies H – Extensive cross-agency (that is, government) interaction or cross-sectional (non-government and government) interaction</p>	<p>Low</p>	
<p>Public impact L – Minimal impact on the organisation and clients M – Some impact on clients is likely due to changes to the handling of personal information; or the changes may raise public concern H – High impact on clients and the wider public, and concerns over aspects of project; or negative media is likely</p>	<p>Low</p>	

Released Under the Official Information Act 1982

Summary of privacy impact

Complete the table below based on the assessment outcome so far.

The privacy impact for this initiative has been assessed as:	Tick
Low – There is little or no personal information involved; or the use of personal information is uncontroversial; or the risk of harm eventuating is negligible; or the change is minor and something that the individuals concerned would expect; or risks are fully mitigated	
Medium – Some personal information is involved, but any risks can be mitigated satisfactorily	✓
High – Sensitive personal information is involved, and several medium to high risks have been identified	
Reduced risk – The project will lessen existing privacy risks	

Recommendation

A full privacy impact assessment is not required for FRS, providing no significant risks are identified during the completion of security and cloud risk assessments for the system.

Should the selected provider not be able to answer or address risks arising from the security and cloud risk assessments, a targeted PIA may be required.

Authorisation

The Business Owner is ultimately responsible for ensuring that the Privacy Impact Assessment has the appropriate scope, and that the recommendations are actioned. The Principal Advisor Privacy should be consulted before the document is finalised to ensure that the Threshold Check addresses the necessary privacy considerations.

Authorised by	Signature	Date
Business Owner(s) David Philp General Manager Identity and Passport Services		21/3/17

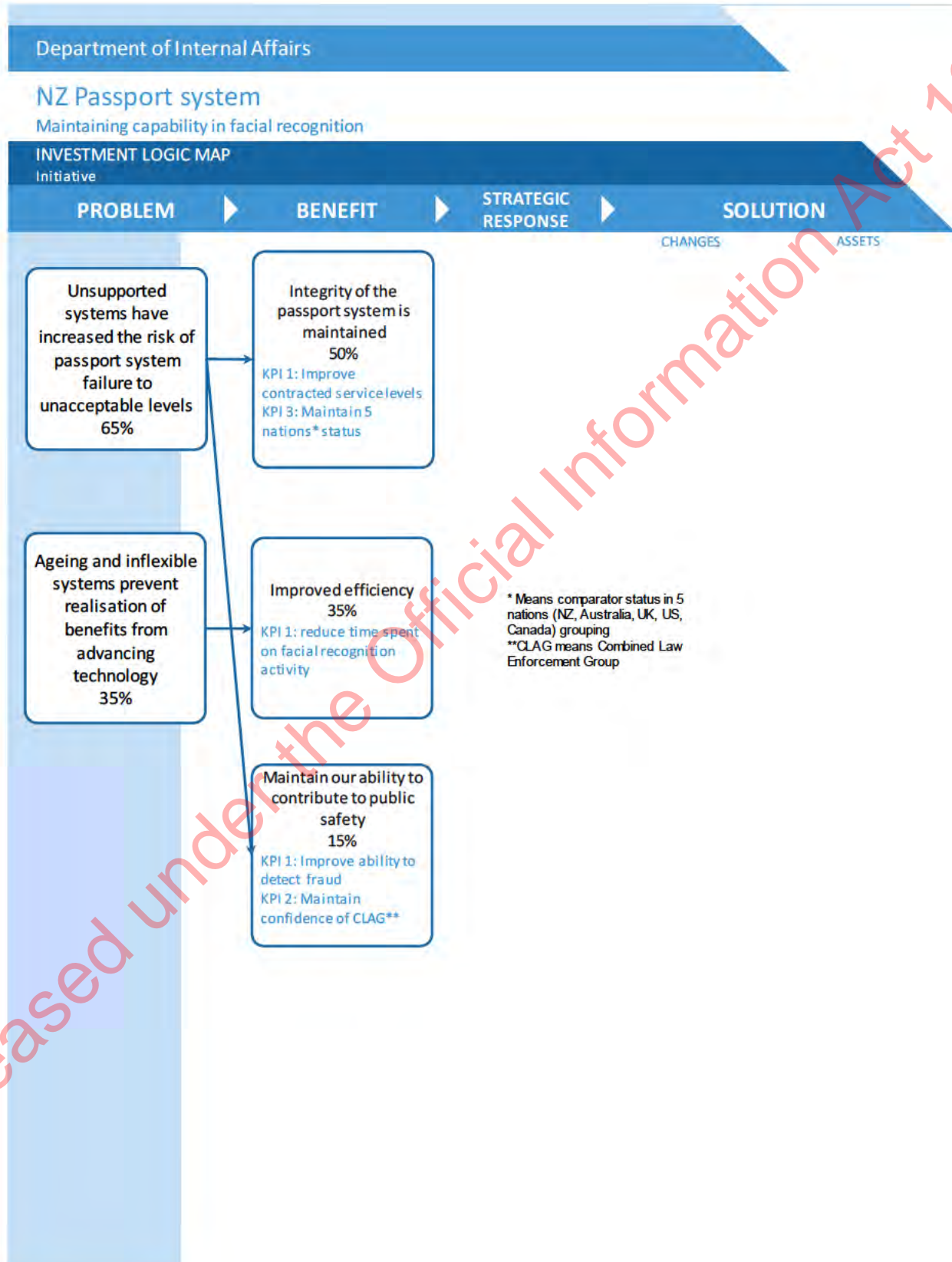
Forward a copy of the final signed document to privacy@dla.govt.nz.

Appendix E: DIA outcomes framework

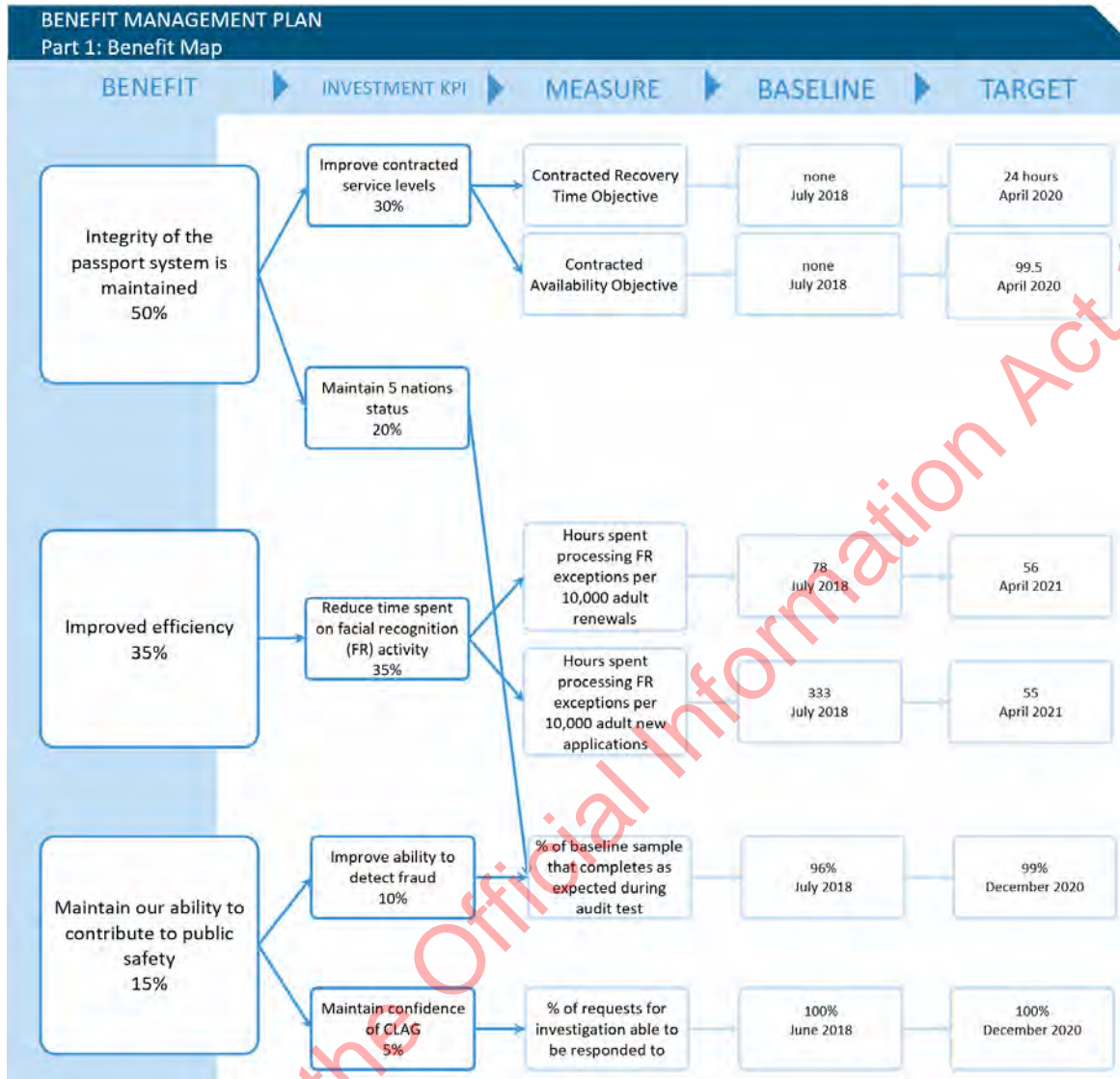
Aspects:	Departmental outcome framework:									
Vision	Connected citizens, communities and government									
Focus Areas: the difference we make	Transforming service delivery Measure areas: Public sector cost and Online service use			Strong resilient communities Measure area: Sense of community belonging			Trusted information Measure area: Number of data sets Trust and confidence			
Supporting outcomes	Contributing to people having access to public services, which are designed around them, when they need them	Contributing to the creation of new social, economic and cultural value from New Zealand's information and knowledge	Connected, informed and resourced communities	Reducing community harm	Strong and transparent community governance and institutions	NZers access and use digital information for a range of purposes	NZers experience better services and have a hand in shaping them	NZers have increased trust and confidence in the public service	Data and information is used effectively to inform policy and design services	
Outputs	<ul style="list-style-type: none"> providing one access point for customer interaction with government transforming delivery of public services, including RealMe leading government direction for investment in ICT, data, and information (including data.govt) providing assurance and support to all-of-government on ICT and privacy 			<ul style="list-style-type: none"> translation and language services supporting community projects; and guidance for funding schemes financial assistance to low income earners connecting ethnically diverse people and providing advisory and information services regulatory services and regulation of charities administering racing safety development fund and legislation, statutory and other bodies, local government legislation; and processes for grants funding support for Ministerial and Executive services purchasing and maintenance of Crown assets 			<ul style="list-style-type: none"> online authentication publishing civic information maintaining the Charities Register Alexander Turnbull Library donations administering Public Records Act managing and administering identity information preserving films collecting, preserving, and maintaining NZ heritage ensuring access to NZ authored books in NZ libraries; managing and administering information 			
Focus Area: how we deliver	A fit-for-purpose Department Te Aka Taiwhenua, Te Ara Vaka Measure areas: Staff engagement and Fiscal sustainability									
Resources applied	Financial Statements					Service Performance				

Appendix F: ILM and Benefit Management Plan

Facial Recognition Investment Logic Map (ILM) v0.7



Facial Recognition Benefit Management Plan (BMP) v0.6



Released under the Official Information Act 1982

Appendix G: Facial Recognition Risks and Uncertainties

Risk Description	Estimated Impact	Consequence Minimal → Severe	Likelihood Almost never → Almost certain	Treatment
<p>If there is too much change introduced or implemented simultaneously into the DIA (business and technical) environment then managers and staff may not be focused on the implementation and business preparation activities for the new Facial Recognition Service capability.</p> <p>SD01200_R_11</p>	1-2 months delay	Moderate	Possible	Co-ordinate and manage dependencies, business change and system releases across the SDO portfolio, Te Ara Manaaki and BAU changes.
<p>If the new system does not perform as expected, then additional time and budget may be required to resolve the issues.</p> <p>Potential drivers of the non-performance include issues around Integration of the Facial Recognition Service and wider Passports System, as well as the new service itself</p> <p>SD01200_R_18</p>	<p>\$265k a month increase on budget and up to 8 weeks to resolve.</p> <p>Actual costs will depend on severity of issue.</p>	Moderate	Possible	<p>Performance Test plan agreed with supplier and DIA Test team.</p> <p>Strong service level agreements agreed with the supplier, including penalties for non-delivery.</p> <p>One Prime Contract ensure responsibilities are clear and supplier can be held accountable.</p>

Risk Description	Estimated Impact	Consequence Minimal → Severe	Likelihood Almost never → Almost certain	Treatment
<p>If there is contention with other projects and BAU changes for the pre-production QA environment, then this may delay QA deployments and testing of the Facial Recognition Service and Integrations, and incur supplier and resource costs where these resources cannot be reallocated</p> <p>SDO1200_R_16</p>	<p>1-2 months delay, up to \$365k increase on budget and up to 8 weeks to resolve</p>	<p>Moderate</p>	<p>Possible</p>	<p>Plan and agree environment and release schedules and required resources with managers, and monitor and manage any slippages across all release candidates.</p>
<p>If additional business requirements unfold during the detailed design stage as more is understood about the FR Service and any consequential changes to the Passport System and other integrating components, then the costs could be higher than estimated and there may be additional time required to accommodate these changes.</p> <p>SDO1200_R_17</p>	<p>\$528k increase on budget and up to 4 weeks delay</p>	<p>Moderate</p>	<p>Possible</p>	<p>Accelerate business requirements development and impact assessments from suppliers and updated resource estimates during the design stage.</p>
<p>If the full migration of enrolments from the old to new environment and deduplication of potential duplicates results in a series of determinations, analysis and assessment of findings, fine tuning and testing, that require more time or expertise than has been allowed for in the schedule and budget</p> <p>SDO1200_R_19</p>	<p>\$309k increase on budget and delay of 1-2 months.</p>	<p>Moderate</p>	<p>Possible</p>	<p>Comprehensive migration and deduplication plan in place, work closely with supplier and business SMEs to plan to mitigate any arising issues.</p>

Risk Description	Estimated Impact	Consequence Minimal → Severe	Likelihood Almost never → Almost certain	Treatment
<p>If the thresholds need to be changed during post go live support then changes will need to be reconfigured, tested and released.</p> <p>SDO1200_R_23</p>	<p>\$100k increase on budget.</p>	<p>Possible</p>	<p>Moderate</p>	<p>Allow sufficient time for configuration, testing and tuning of thresholds.</p> <p>Comprehensive testing to determine thresholds prior to production.</p> <p>Acceptance criteria to be established for thresholds and signed off prior to exiting testing.</p>
<p>If there is an issue or disruption during the production transition that may require significant fixes and retesting then this may delay the implementation up to 1-2 months depending on the severity, and resolve any contention with release windows across DIA.</p> <p>SDO1200_R_22</p>	<p>1-2 months delay. Up to \$309k increase on project budget depending on severity of changes required and testing and redeployment effort.</p>	<p>Possible</p>	<p>Moderate</p>	<p>Comprehensive test plan including rehearsals and sign off prior to Production Transition.</p> <p>Comprehensive production transition plan and risk management plan.</p> <p>All suppliers and DIA to work closely to plan and implement the changes.</p>
<p>Contracts are not yet agreed with the preferred supplier. Further clarifications or requirements that arise during contract negotiations may increase the price of the Facial Recognition Service Offering</p> <p>SDO1200_R_24</p>	<p>Allow up to 5% increase on the implementation fee</p>	<p>Possible</p>	<p>Moderate</p>	<p>Finalise contract in parallel to business case development.</p>

Appendix H: Presentation of the Long-list Options Assessment

Options Analysis for Facial Recognition Business Case

9 Aug 18

	Scope (What)					Services & Solutions (How)								Service Delivery (Who)					
	S0	S1	S2	S3	S4	H1	H2	H3	H4	H5	H6	H7	H8	W1	W2	W3	W4	W5	W6
	S0: No Change - retain existing 1:1 and 9(2)(k) 1: many matches on DIA Passport images	S1: current - replace like for like 1:1 and 9(2)(k) 1: many matches on DIA Passport images	S2: Only verification 9(2)(k) 1:1 and 9(2)(k) 1: many matches on DIA Passport images	S3: Do without FR No FR checking	S4: multi agency access and information 1:1 Lmany Police NZTA Immigration Teacher Ed Council	H1: Do nothing - continue with current provider and set up	H2: A modern FR service	H3: Public social APIs eg Google	H4: Use existing gov agencies service / set up for FR (MBIE Police)	H5: Crowd sourcing adjudication	H6: Artificial Intelligence built into the FR system	H7: Live capture	H8: Multiple algorithms / systems	W1: In house	W2: NZ hosted and managed Service for DIA	W3: Cloud software as a service	W4: open syndicated locally hosted and managed service (open to ADG)	W5: Outsource FR and Photo QA	W6: Outsource advanced image checking
Investment Objectives (Benefits and SMART)																			
Maintain availability passport SLA	Partial	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Maintain integrity (eg visa waiver maintained)	Partial	Yes	No	No	No	No	Yes	No	Yes	Partial	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Partial	Partial
Improve efficiency	No	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Maintain public safety (eg fraud detection)	Partial	Yes	No	No	Partial	No	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Critical Success Factors																			
Strategic fit (with gov and DIA) priorities and business need	No	Yes	No	No	Yes	No	Yes	No	Yes	No	No	No	No	No	Partial	Partial	Yes	Yes	Yes
Value for Money	Yes	Yes	Partial	No	No	No	Yes	No	No	No				Yes	Yes	Yes	Yes	Partial	Partial
Acceptable level of risk	No	Yes	Partial	No	No	No	Yes	No	No	No				Yes	Yes	Yes	Yes	Partial	Partial
Capability and capacity to deliver	No	Yes	Yes	Yes	Yes	No	Yes	No	No	Yes	Partial	Partial	Partial	Yes	Yes	No	Yes	Yes	Yes
Affordable	Yes	Yes	Yes	No	Partial	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Partial	Partial
Achievable	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	No				Yes	Yes	Yes	Yes	Yes	Yes
Shortlist option: Do nothing	★					★								★					
Shortlist option: Do minimum			★				★										★		
Shortlist option: Preferred option		★					★										★		
Shortlist option: Aspirational		★					★				★						★		
Notes	Existing system has no software or hardware support and licensing restrictions make hardware changes high risk. Licensing volumes will be exceeded in a couple of years requiring a system change to provide capacity.	As technology has moved on since the current system was procured replacing 'like for like' with the new Facial Recognition system will give more accurate results compared to the current technology (S0).	This scope option reduces current capability. It removes identification services with one-to-many matches. This also removes the ability to conduct full deduplication searches (many-to-many matches). It would result in increased risk of fraud requiring other actions or mitigations to be taken. Responsibility and effort for identification (validating new identities) would require another form of test if the one-to-many test is not available.	Would need increase staff to maintain passport production SLAs (complete facial recognition manually). Likely to result in longer turnaround times Increased risk of fraud and more effort for the customer if other verification methods were used	Although other agencies (Police NZTA Immigration Council and others) are interested in using facial recognition they either do not have a clear set of requirements or are currently tied into existing contracts so a combined contract was not possible however the commercial contract was designed as a syndicated contract allowing future entry to the service.	Existing high risk option due to the lack of contracted support and inability to make changes as the components around the solution change.	A modern facial recognition service will provide full delivery of the investment objectives since modern systems are more accurate. Value for money assumed as the tender process and intensive negotiations have been completed and good value options short listed. A roadmap of how new technology and changes can be provided to ensure the solution is as future proof as possible.	This approach would not align with DIAs privacy requirements and risk strategy 9(2)(k) However Incumbent challenges include likely issues with integration complexity with intermediaries and restrictive licensing contracts. No other system was designed for the load required for passport processing.	Using or linking into another agencies facial recognition service is attractive as it would support the investment objectives and align with government priorities for shared services. However Incumbent challenges include likely issues with integration complexity with intermediaries and restrictive licensing contracts. No other system was designed for the load required for passport processing.	This approach has been implemented by DIA for some services such as photo categorisation of library archives. This option was eliminated due to misalignment with automation priorities and privacy concerns.	Rather than discrete algorithms from the supplier an AI solution will learn and improve over time including preventing fraud and adjusting to new security threats. This option was taken forward for further investigation.	Live Capture integrates the photo process in real time with a customer application to prevent fraud and improve image quality. This would require coordination across the wider passports system (including with Te Ara Manaaki) and is already part of the Real/ve Now App.	Rather than depending on one suppliers' algorithms alone this could bring together several to provide a more robust system. This option was not taken forward because it would increase the cost of the service without a clear value proposition.	This option does not align with DIA priorities as it would require bringing in significant capability including the purchase of the facial recognition software (and a maintenance contract).	This option does not fully support the AOG Shared Services Strategy as it would be for DIA alone.	This option was available for suppliers to propose through the RFP process with no relevant submissions. Concerns around data sovereignty and integrity limit the options for cloud software as a service.	This approach creates the opportunity for other agencies to benefit from the agreement (supporting the AOG Shared Services Strategy). If other agencies take up the service there is the potential for reduced cost to government overall.	Until the software capability is available to automate this process outsourcing the work would increase DIA's risk since the supplier would hire a similar skill set but would have less experience at managing that skillset.	Advancements in image QA to provide reliable face image detection and QA analysis of facial features and image manipulations would allow full automation of the process removing reliance on DIA staff for checks. However this option was not offered by the market.

Options identification

A. Scope

The longlist of scope options was developed around combinations of facial recognition capabilities, since there were few other scope elements that could be modified. These are:

- **Identification Service:** Provides functions to support one-to-many searches using facial characteristics against a biometric enrolment database.
- **Verification Service:** Provides functions to enable the performing of one-to-one comparisons searches using facial characteristics.
- **Investigation Service:** Provides functions to enable investigators to investigate identity fraud and perform forensic analysis of facial images.

In addition to the three capabilities, consideration of other government agencies was an extension of scope.

Table 35 shows the components in each long-list option, with the assessment of all the scope options summarised in Table 36.

Table 35. Facial recognition services included in scope long list options

Components / services	Identification service	Verification service	Investigation service	Multi-agency comparisons*
S0: No change -retain existing	✓	✓	✓	-
S1: Current – replace with modern solution	✓	✓	✓	-
S2: Smaller scope (only verification ⁹⁽²⁾ (k)	-	✓	✓	-
S3: Do without Facial Recognition	-	-	-	-
S4: Multi-agency service	✓	✓	✓	✓

*ie 1 to many comparisons with other agencies databases

Table 36. Summary of scope options

Option	Pros and Cons	
S0: No change - retain existing solution <i>Carried through to short-list as baseline</i>	Pros	
	Cons	Existing system has no software or hardware support and licensing restrictions make hardware changes high risk. Licensing volumes will be exceeded by mid-2020, requiring a system change to provide capacity.
S1: Current – replace with modern solution <i>Carried through to short-list</i>	Pros	As technology has moved on since the current system was procured, replacing the current system with a modern Facial Recognition system will give more accurate results compared to the current technology (S0).
	Cons	
S2: Reduce scope (only verification 9(2)(k)) <i>Carried through to short-list</i>	Pros	
	Cons	This scope option reduces current capability. It removes identification services with one-to-many matches. This also removes the ability to conduct full deduplication searches (many-to-many matches). It would result in increased risk of fraud requiring other actions or mitigations to be taken. Responsibility and effort for identification (validating new identities) would require another form of test if the one-to-many test is not available.
S3: Do without Facial Recognition	Pros	
	Cons	Would need increase staff to maintain passport production SLAs (complete facial recognition manually). Likely to result in longer turnaround times, increased risk of fraud and more effort for the customer if other verification methods were used
S4: Multi agency service	Pros	
	Cons	Although other agencies (Police, NZTA, Immigration, Teacher Education Council and others) are interested in using facial recognition, they either do not have a clear set of requirements, or are currently tied into existing contracts, so negotiation of a combined contract was not possible, however the commercial contract was designed as a syndicated contract allowing future

Option	Pros and Cons
	entry to the service.

B. Solution (How the Service is Delivered)

The solution long list options describe how the facial recognition capability could be delivered for DIA. Table 37 summarises the assessment of all the solution options that were considered.

Table 37. Summary of Solution Options

Option	Pros and Cons
H1: Current - Continue with current provider and set up <i>Carried through to short-list as baseline</i>	Pros
	Cons Very high risk option due to the lack of contracted support, and inability to make changes as the components around the solution change. Would also exceed the number of photos allowed in the database under the current license by 2020
H2: A modern facial recognition service <i>Carried through to short-list</i>	Pros A modern facial recognition service will provide full delivery of the investment objectives since modern systems are more accurate. Value for money assumed as the tender process and intensive negotiations have been completed and good value options short listed. A roadmap of how new technology and changes can be provided to ensure the solution is as future proof as possible.
	Cons
H3: Public social APIs (eg Google)	Pros This approach would not align with DIA’s privacy requirements and risk strategy, 9(2)(k)
	Cons

Option	Pros and Cons	
H4: Use existing govt agencies service (MBIE, Police)	Pros	Using or linking into another agencies facial recognition service is attractive as it would support the investment objectives and align with government priorities for shared services.
	Cons	However, insurmountable challenges include likely issues with integration, complexity with intermediaries and restrictive licensing contracts that prevent DIA using the service.
H5: Crowd sourcing adjudication	Pros	This approach has been implemented by DIA for some services, such as photo categorisation of library archives.
	Cons	This option was eliminated due to misalignment with automation priorities and privacy concerns.
H6: Artificial Intelligence (AI) built into the facial recognition system <i>Carried through to short-list for further investigation</i>	Pros	Rather than discrete algorithms from the supplier, an AI solution will learn and improve over time including adjusting to new security threats. This option was taken forward for further investigation.
	Cons	
H7: Live Capture	Pros	Live Capture integrates the photo process in real time with a customer application to prevent fraud and improve image quality. This would require coordination across the wider passports system (including with Te Ara Manaaki), and is already part of the RealMe Now App. This option was outside the scope of the Facial Recognition project, and should be part of Te Ara Manaaki, since it involves the user interface.
	Cons	

Option	Pros and Cons	
H8: Multiple algorithms / systems	Pros	Rather than depending on one suppliers' algorithms alone, this could bring together several to provide a more robust system. This option was not taken forward because it would increase the cost of the service without a clear value proposition.
	Cons	

C. Delivery Options

Table 38 shows the assessment of all the delivery options that were considered.

Table 38. Summary of Delivery Options

Option	Pros and Cons	
W1: Inhouse <i>Carried through to short-list as baseline</i>	Pros	
	Cons	This option does not align with DIA priorities as it would require bringing in significant capability, including the purchase of facial recognition software (and a maintenance contract).
W2: NZ hosted and managed Service for DIA	Pros	
	Cons	This option does not fully support the AOG Shared Services Strategy as it would be for DIA alone.
W3: Cloud software as a service	Pros	
	Cons	This option was available for suppliers to propose through the RFP process, with no relevant submissions. Concerns around data sovereignty and integrity limit the options for cloud software as a service. DIA has made a decision that no passport data will be hosted overseas. Options for delivery have also been reinvestigated.

Option	Pros and Cons	
W4: Open syndicated locally hosted and managed service (open to AOG) <i>Carried through to short-list</i>	Pros	This approach creates the opportunity for other agencies to benefit from the agreement (supporting the AOG Shared Services Strategy). If other agencies take up the service, there is the potential for reduced cost to government overall. This option supports continuous improvement as technology improves over the life of the project
	Cons	
W5: Business Process Outsource facial recognition and photo quality assurance	Pros	
	Cons	Until the software capability is available to automate this process, outsourcing the work would increase DIA's risk since the supplier would hire a similar skill set, but would have less experience at managing that skillset.
W6: Outsource advanced image checking	Pros	Advancements in Image QA to provide reliable face image detection and QA analysis of facial features and image manipulations would allow full automation of the process, removing reliance on DIA staff for checks.
	Cons	However this option was not offered by the market.

D. and E. Implementation timing and Funding options

There was only one feasible option for both the implementation timing and funding sources.

- **Implementation: Go Live within one year** – a supplier will not be able to deliver any faster, and any later will increase risks of failure across the passports system.
- **Funding: Memorandum Account** – this is the current approach in which passport fees cover the cost of providing the passport service, and will be continued.

Appendix I: Detailed Economic and Financial Data

Forecast Passport Demand

Identification - New Applications											
Forecasts New Issues financial years		20/21	21/22	22/23	23/24	24/25	25/26	26/27	27/28	28/29	29/30
Children (0-10)		82,321	85,540	89,083	92,243	95,147	97,758	99,657	100,954	102,131	102,789
Youth (11-12)		4,907	5,002	5,056	5,031	4,967	4,864	4,959	5,023	5,082	5,114
Youth (13-15)		6,853	6,993	7,076	7,049	6,966	6,830	6,962	7,053	7,135	7,181
Adults		69,659	74,492	79,642	85,017	90,476	96,114	101,765	106,228	110,509	114,585
Totals		163,739	172,027	180,857	189,339	197,556	205,566	213,343	219,258	224,857	229,669

Verification - Renewals											
Forecasts Replacement Issues financial years		20/21	21/22	22/23	23/24	24/25	25/26	26/27	27/28	28/29	29/30
Children (0-10)		51,134	54,117	56,429	58,913	61,539	64,283	66,368	68,645	70,760	72,738
Youth (11-12)		17,084	18,550	19,510	20,263	20,884	21,440	22,135	22,895	23,600	24,260
Youth (13-15)		25,406	27,590	29,019	30,140	31,065	31,892	32,926	34,056	35,106	36,087
Adults		292,546	138,551	87,540	66,006	80,896	380,271	559,517	619,369	658,994	643,624
Totals		386,169	238,808	192,497	175,322	194,384	497,886	680,946	744,964	788,461	776,707

Total Project and Ongoing Costs for Preferred Option														
	2016/2017	2017/2018	2018/2019	2019/2020	2020/2021	2021/2022	2022/2023	2023/2024	2024/2025	2025/2026	2026/2027	2027/2028	2028/2029	Total
\$000	<u>Sunk Costs</u>		<u>Year 0</u>											
Capital expenditure														
DIA project cost	-	-	425.5	1,170.3	-	-	-	-	-	-	-	-	-	1,595.7
External vendor costs	-	-	1,721.2	2,683.1	-	-	-	-	-	-	-	-	-	4,404.3
Purchase of tangible assets	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Software	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Others	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	-	-	2,146.7	3,853.4	-	-	-	-	-	-	-	-	-	6,000.0
Operating expenditure														
Project operating expenditure														
Personnel	229.8	80.8	199.5	81.7	-	-	-	-	-	-	-	-	-	591.8
Software maintenance	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Hardware maintenance	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Others	84.2	126.6	158.3	60.5	-	-	-	-	-	-	-	-	-	429.6
Total project operating expenditure	314.0	207.4	357.8	142.2	-	-	-	-	-	-	-	-	-	1,021.4
On-going operating expenditure														
Other operating expenditures	-	-	-	756.6	3,026.6	3,026.6	3,026.6	3,026.6	3,026.6	3,026.6	3,026.6	3,026.6	1,513.3	26,482.6
Depreciation & amortisation	-	-	-	171.4	685.7	685.7	685.7	685.7	685.7	685.7	685.7	685.7	342.9	6,000.0
Capital charge	-	-	128.8	349.7	308.6	267.4	226.3	185.1	144.0	102.9	61.7	20.6	-	1,795.1
Total on-going operating expenditure	-	-	128.8	1,277.8	4,020.9	3,979.7	3,938.6	3,897.4	3,856.3	3,815.2	3,774.0	3,732.9	1,856.2	34,277.7
Total expenditure	314.0	207.4	2,633.3	5,273.3	4,020.9	3,979.7	3,938.6	3,897.4	3,856.3	3,815.2	3,774.0	3,732.9	1,856.2	41,299.2
WOLC Before Discounting	-	-	2,504.5	4,752.2	3,026.6	3,026.6	3,026.6	3,026.6	3,026.6	3,026.6	3,026.6	3,026.6	1,513.3	32,982.6
Discounted WOLC			2,504.5	4,441.3	2,643.5	2,470.6	2,309.0	2,157.9	2,016.7	1,884.8	1,761.5	1,646.3	769.3	24,605.4
Cash Benefits Before Discounting	-	-	-	-	93.6	88.4	88.4	88.4	104.0	130.0	145.6	161.2	83.2	982.7
Discounted NPV	-	-	2,504.5	4,441.3	2,561.8	2,398.4	2,241.5	2,094.9	1,947.4	1,803.9	1,676.8	1,558.6	727.0	23,956.1
Capital funding required	-	-	2,146.7	3,853.4	-	-	-	-	-	-	-	-	-	6,000.0
Operating funding required	-	-	486.6	1,420.0	4,020.9	3,979.7	3,938.6	3,897.4	3,856.3	3,815.2	3,774.0	3,732.9	1,856.2	34,777.7
Realisable cash benefits	-	-	-	-	93.6	88.4	88.4	88.4	104.0	130.0	145.6	161.2	83.2	982.7

Key assumptions used in the financial model include:

1. Sunk costs are excluded from the Whole of Life calculation (2016/17 and 2017/18 opex costs)
2. Discount rate of 7% - Year 0 is the first year of investment in 2018/19, Year 10 is 8 years post implementation 2028/29
3. Asset life of 8.75 years post implementation, in line with the proposed Facial Recognition as a service contract period
4. Ongoing pricing is based on the passports volume forecast between 2016/17 and 2025/26

5. All assets to be decommissioned have been fully depreciated and will not require any impairment charge
6. Capital charge at 6% and 21% contingency built into once off project expenditure for 2018/19 and 2019/20

Released under the Official Information Act 1982

Appendix J: Supplier overview

Sample of top biometric software vendors

Gemalto Cogent (formerly known as 3M Cogent and 3M)

As a world leader, Gemalto Cogent provides first class Automated Biometric Identification Systems, identity management solutions, and biometric access control products to governments, law enforcement agencies, and commercial customers worldwide. Establishing a reputation for successful deployment of cost-effective finger, face, and iris biometric systems, Gemalto Cogent products allow for real-time identification of individuals in a wide variety of applications, including: voting, asylum seekers, citizen benefits, identity credentialing, driver licenses, law enforcement, criminal investigations, border security, and others.

NEC

Since the 1970's, NEC has invested significant resources in the research and development of its biometric identification technologies, and its consistently achieved world-leading result in independent, third-party testing. Our solutions for fingerprint identification and facial recognition ensure that agencies can accurately and swiftly identify people in the field, within an organization or at the border.

Leveraging its leading multi-biometric recognition solutions, NEC offers system integration services to deliver reliable identity verification solutions.

Today, with more than 700 deployments in over 70 countries, NEC continues to be the leading provider and one of the largest market share holders of Multi-Modal Biometrics Identification System worldwide.

Cognitec

Cognitec Systems was founded in 2002 by a team of experts who recognized the growing need for software and hardware solutions in the field of biometrics. Our founders have been working on algorithms for the FaceVACS face recognition technology since 1995. Starting in 1996, government and industry customers have relied on the FaceVACS technology for a wide range of applications.

The development of products and the growth of our company build on the extensive knowledge of our scientists and software engineers and their continuing dedication to deliver the best performance available on the market. We also offer consulting services and excellent technical support.

Cognitec currently employs nearly 60 staff members. Our headquarters are located in Dresden, Germany with sales and support offices in the United States and Australia.

FRVT 2013: Test results on the performance of automated age estimation algorithms confirmed Cognitec Systems' leading position in the face recognition market. The test compared nine algorithms submitted by six participants, five companies and one university, and applied them to seven million images. Results show that Cognitec's algorithm performs with the highest accuracy for all age groups. Most notably, the algorithm shows superior performance "in the youth and senior age groups, leading the next most accurate algorithm in 5-year accuracy by 30% and 16%, respectively," according to the report.

Idemia (formerly known as Safran Identity & Security, Morpho and OT-Morpho)

Idemia is a global leader in multi-biometric solutions for security and identity applications. Backed by more than 40 years of experience in biometrics, Idemia secures and simplifies everyday lives, through a wide range of fingerprint, iris and face recognition technologies.

Its solutions meet a wide range of security needs for people, companies and governments worldwide, including identity management, personal rights for residents and travellers, physical access to airports or other high-value sites, and logical access, either online or via secure terminals.

Toshiba

Face recognition technology is finding increasingly wide use, in areas including target detection by surveillance cameras in public spaces; personal identification at airports and financial institutions; and for marketing by demographic data (age, gender, etc.).

Toshiba's long-term commitment to face recognition technology—over 20 years now—has allowed the company to develop fast, highly accurate algorithms, whose performance has been independently confirmed in third-party testing.

System integrators providing data centres and managed services

Datacom

Datacom are an approved AoG ITSM and IaaS Service Provider and are the incumbent ITSM Service provider to DIA.

They are the system integrator for the MBIE Immigration Biometric implementation.

DXC (formerly known as Hewlett Packard Enterprise)

DXC sublease Datacom facilities in an approved AoG data centre and are the incumbent Passport System Integrator. They have an existing partnership with Idemia via the acquisition of L1 Identity Systems. They provide ITSM services to a number of Government Agencies.

HPE selected L1 after a Biometric evaluation between L1 and Cognitec in 2009.

IBM

IBM are an approved AoG data centre for IaaS, although they do not currently supply DIA they have ongoing partnerships with Biometric vendors with solutions in other jurisdictions.

Fujitsu

Fujitsu are an approved AoG ITSM Service provider, although they do not currently supply DIA they have ongoing partnerships with Biometric vendors with solutions in other jurisdictions.

Unisys

Unisys is an ITSM Service and Data centre provider. Although they have no current relationships with DIA they have ongoing partnerships with Biometric vendors with solutions in other jurisdictions and are the System Integrator for NZTA Driver Licences in NZ

Canadian Bank Note Company

Provide existing “Pay per Book” personalisation service to DIA and therefore may be a provider that Biometric Vendors may choose to partner with.

Released under the Official Information Act 1982

Appendix K: DIA and Other Agency Use of Facial Recognition Services

DIA Potential Uses for the Facial Recognition Service

DIA – citizenship

Facial recognition services could be incorporated into the processes around Citizenship. Te Ara Manaaki has two high level use cases for FR and Citizenship.

One scenario is that Citizenship would integrate with NZ Immigration to obtain applicants immigration movement plus photos. The system then runs a verification check to verify the citizenship image with the image from immigration to ensure they match. In this use case, Te Ara Manaaki's architect has been advised that they will need to subscribe to a separate facial recognition verification service with DXC and applicable SLAs.

Te Ara Manaaki's second use case is Citizenship by descent where a facial recognition check is run against the parents. They might require a check against the passports gallery. This will have an impact on passports facial recognition volume, performance and pricing. Te Ara Manaaki's architect has been advised that they develop their own interface instead of using the KIWI biometric service. Te Ara Manaaki will need to keep the facial recognition project informed once they clearly identify their requirements.

DIA – Identity Services

The Identity services roadmap for DIA could incorporate Facial Recognition as a component of the mobile application. The same board governs both Identity Services and the Facial Recognition project, which will maximise opportunities for maximising the investment made in Facial Recognition.

How Other Agencies Use Facial Recognition

Detailed below is the information collected from each Agency that attended the Cross-Agency Workshop.

Ministry of Business Innovation & Employment

MBIE use facial recognition for:

- Identification (1: many) searches for visa applications
- Investigation services similar to DIA (adhoc searches)
- They do not do verification matches (1:1)

The MBIE Immigration NZ (INZ) processing system (IDme) provides an integrated Identity storage and matching solution which integrates Facial Recognition for identification (1: many) as well as Fingerprint matching with a person biographical data (name, date of birth etc).

A custom developed Adjudication process is used for the manual resolution of biographic and Face match exceptions where the system cannot automatically determine an Identity.

INZ have worked with Australia's Department of Border Protection around the ongoing training of these face specialists and continue to work with DIBP, DIA, Police and Customs around a common set of standards for facial resolution as well as common levels of adjudication competence with a view to senior practitioners being formally recognised as experts through levels of qualification.

Since INZ only recently implemented the new facial recognition solution, they are not in a position to consider the shared service until their contract review period in 7 years.

New Zealand Transport Agency

NZTA do not currently use facial recognition but new legislation is currently before government to increase the automation and online processing of Driver licences. This can only be implemented by using facial recognition. NZTA is therefore interested in DIAs market approach for facial recognition. Therefore they confirm the following:

- NZTA needs facial recognition capability for future application
- Will be looking at requirements and implementation within the next 1-2 years
- NZTA are looking to leverage other Government data sources to assist in online processing such as the passport photo, or Immigration photos to verify (1:1) an identity for a new driver licences application.
- NZTA therefore have a need to share facial recognition capability of other agencies and are not constrained by any existing facial recognition supplier contract.
- When NZTA arrives at a point of understanding their full requirements for facial recognition, NZTA will be able to determine how to leverage the other agency data and whether this can leverage the DIA's shared service, or if an alternative solution is required.

Customs

Broadly speaking the high-level service capabilities described should be in line with any Customs future usage.

Customs have an existing contract with Morpho (the supplier of the eGates into which their current facial recognition capability is integrated) through until 30 June 2018, but this is likely to be renewed through until the end of the useful life of the gates (so through until 2020 or 2021, which is about the earliest that Customs expect they would look at replacing the existing gates with something else).

Police

Police use both finger print and facial recognition technology. Their finger print technology was upgraded in 2016.

Police would give consideration to the outcomes of the DIA led procurement however participation would be dependent on the successful supplier being able to meet police requirements in respect of the five standards.

Appendix L: Commercial Case details

The evaluation model used was weighted attribute (weighted score). For the RFP, price was not a weighted criterion. Instead price was taken into account when determining value for money over the whole-of-life of the contract. A two-envelope process was used and respondents pricing was only opened once the non-price scoring was completed.

A number of clarifications sessions were conducted with both respondents, followed by evaluation and moderation sessions with the internal DIA evaluation panel.

The BAFO stage was a way of bringing the negotiations to an end and the Respondents submitting their final offer. Each Respondent was asked to resubmit the RFP response form and highlighting what had changed in their submission based on clarifications and negotiations.

The evaluation panel then re-evaluated all the amended sections of the RFP response and a moderation session was held to discuss any change in scores. This was the final stage in the evaluations and therefore the summary scores in the Table 21 are final.

Criterion	Weighting
Technical Merit (Fit for Purpose)	60%
The degree to which the service meets or exceeds the requirements. The overall quality of the services being offered and the level of risk that may be involved if adopting the service. This section is broken down into the following sub criteria:	
Biometric Capability and Functional Requirements	24%
Biometric Accuracy	18%
Service Architecture and Non-Functional Requirements	18%
Capability	20%
The degree to which the respondent has the capability to deliver the services including: <ul style="list-style-type: none"> • Methodology and approach to implementation and risk mitigation. • Organisational and personnel track record in successfully delivering similar solutions for Government Departments. • Suitability of reference sites of previous deployments. • Experience of working together with any proposed third parties including references. • Evidence of your capability in relation to other deployments including services provided for: <ul style="list-style-type: none"> ○ Implementation ○ Training ○ Professional Service Support ○ On-going support and updates ○ Membership of professional body/association and relevant certification/accreditation or similar 	
Capacity	20%
The degree to which the respondent has the capacity to successfully deliver the services in the required time frames including: <ul style="list-style-type: none"> • Availability of suitably skilled resources to confirm requirements, design/build, test and deliver the service 	

in 2018 and ongoing management and support of the service.

- Approach for managing and ensuring the availability of appropriate resources, the required knowledge to complete the work, and ensuring the successful delivery of the services including contingency requirements.

Total weightings	100%
-------------------------	-------------

Completed procurement milestones

The completed milestones for the procurement process are outlined in below. The negotiations with all respondents (two pairs of two suppliers) were closed off through a Best and Final Offer (BAFO) stage.

Step	Date Completed	Attendees
Request for Proposals (RFP)		
RFP Released	11 th April 2017	
RFP Responses Received	17 th May 2017	
RFP Moderation 1	12 th /13 th June 2017	DIA
RFP Value for Money Discussions	16 th June 2017	DIA
Respondents Clarification Sessions	23 rd June 2017	DIA/Respondents
Respondents Clarifications Received	30 th June 2017	
Review of Clarifications and Revised Pricing	7 th July 2017	DIA
Facial Recognition Solution Testing	10 th to 28 th July 2017	DIA/Respondents
RFP Pricing Negotiations 1	31 st July 2017	DIA/Respondents
RFP Moderation 2 and Value for Money Discussions 2	7 th August 2017	DIA
RFP Pricing Negotiations 2	8 th /9 th August 2017	DIA/Respondents
Contract & Pricing Negotiations 1	22 nd August 2017	DIA/Respondents
Contract & Pricing Negotiations 2	8 th September 2017	DIA/Respondents
RFP Moderation 3	15 th September 2017	DIA
Best and Final Offer (BAFO)		
BAFO Document Released	5 th October 2017	
Respondents Implementation Planning Session	24 th /25 th October 2017	DIA/Respondents
BAFO Responses Received	1 st November 2017	
BAFO Evaluation Moderation	3 rd /13 th /14 th November 2017	DIA
Respondents BAFO Pricing Clarifications Sessions	21 st November 2017	DIA/Respondents

A summary of the full procurement process has been described and approved through the Facial Recognition Solution Evaluation Panel Recommendation (also known as the Final Recommendation Report)³⁰.

Agreed service levels

The supplier will be responsible for the development and configuration of the facial recognition system to meet the specifications outlined in the contract. The supplier will also be responsible for meeting availability and performance service levels as detailed in the table below. For the shared service, new Agencies will be able to select the appropriate category for production and non-production environments as required. Where a service level is not met, penalties will be calculated as per the calculation specified in the contract.

Service Category	Target Availability	Hours of Operation	Time to Restore	Monthly Outage	RTO	RPO
Gold	99.5%	24 * 7	2 hours	216 minutes	24 hours	15 mins
Silver	95.0%	24 * 7	8 hours	1.5 days	5 days	24 hours
Bronze	90.0%	24 * 7	24 hours	3 days	5 days	24 hours

³⁰ [FR Evaluation Panel Recommendation](#)

Appendix M: Facial Recognition Service Requirements

Functional Service Requirements

Value	Description
Mandatory	<ul style="list-style-type: none"> The product must meet this requirement. This is business critical functionality and products that do not meet this requirement will be significantly impacted.
Desirable	<ul style="list-style-type: none"> The product should meet this requirement. Not essential but the business might be impeded without it. Alternative or work around solutions may be considered.
Optional	<ul style="list-style-type: none"> 'Nice to have'. The product could meet this requirement provided the time and cost involved are not prohibitive. Alternative workarounds are available.

Enrolment

This section presents the requirements for enrolment within facial recognition Service.

Ref	Requirement Description	Priority
3.1.1	The facial recognition Service must provide a system interface to enable automated enrolment to be performed	Mandatory
3.1.2	The facial recognition Service must provide a user interface to enable manual enrolment to be performed by an authorised user.	Mandatory
3.1.3	The facial recognition Service must be able to enrol facial images which conform to the ICAO Specification for facial images.	Mandatory
3.1.4	The facial recognition Service must be able to perform quality checks of images during enrolment to ensure they meet the required standard for an ICAO facial image.	Mandatory
3.1.5	The facial recognition Service must enrol facial images which have been accepted by DIA as being suitable facial image for passport processing. (note: Business operational practices sometimes require the enrolment of a facial image which does not conform to the ICAO quality standard for a facial image)	Mandatory
3.1.6	The facial recognition Service must perform quality checks of images during enrolment to ensure they meet the required quality standard for a facial image accepted by DIA as a suitable facial image for passport processing.	Mandatory
3.1.7	The facial recognition Service must report an error and not enrol an image which does not meet the required quality standard	Mandatory

Ref	Requirement Description	Priority
3.1.8	The facial recognition Service threshold settings which control the quality check of an image must be configurable by an authorised user.	Mandatory
3.1.9	The facial recognition Service must automatically determine the eye coordinates of a facial image during enrolment when eye co-ordinates are not provided with enrolment data.	Mandatory
3.1.10	The facial recognition Service must use the eye coordinates provided when eye coordinates are provided with the enrolment data, instead of automatically determining the eye coordinates.	Mandatory
3.1.11	The facial recognition Service must enable an image to be enrolled into a specific gallery.	Mandatory
3.1.12	The facial recognition Service must initially provide separate galleries containing: <ul style="list-style-type: none"> • Passport identities • 9(2)(k) 	Mandatory
3.1.13	The facial recognition Service must be extendable to enable additional galleries to be added in the future.	Mandatory
3.1.14	The facial recognition Service threshold settings, which control the quality check of an image, must be configurable to different values for enrolling images into different galleries. 9(2)(k)	Mandatory
3.1.15	The facial recognition Service must be able to be configured to enable the storage of subset of related biographical data during enrolment of a facial image, to support performing Identification Searches on subsets of enrolled images within a gallery	Mandatory
3.1.16	The facial recognition Service must enable a unique identifier, provided externally, to be included with the enrolment data that uniquely identifies the person's image.	Mandatory
3.1.17	The facial recognition Service must enable a unique transaction identifier to be included with an enrolment that uniquely identifies the specific transaction.	Mandatory
3.1.18	The facial recognition Service must store the quality check results for all enrolments in a manner such that the results are available for operational analysis.	Mandatory
3.1.19	The stored results shall include the unique transaction identifier to enable correlation of results to passport processing activities.	Desirable
3.1.20	An audit record must be stored within the system for all attempts to enrol and include at a minimum: <ul style="list-style-type: none"> • The unique transaction identifier • The unique image identifier • The gallery being enrolled in • The measured quality score • The outcome (success/failure) of the enrolment attempt 	Mandatory

Ref	Requirement Description	Priority
	<ul style="list-style-type: none"> The reason for failure, when an image fails to enrol. The authenticated account identifier which initiated the request <p>The authenticated account identifier must be in a readable format that can identify the end user or automated system process submitting the request.</p>	
3.1.21	The facial recognition Service must be capable of storing the enrolled facial image within the facial recognition Service in a manner such that it is available for viewing when reviewing match results.	Mandatory
3.1.22	The facial recognition Service shall be capable of determining if facial images are to be stored within the facial recognition Service based on a configuration setting for each gallery.	Desirable
3.1.23	The configuration setting controlling the storing (or not) of a facial image should be modifiable by an authorised administrator.	Desirable
3.1.24	The facial recognition Service will enable the bulk enrolment of images. Bulk enrolment of images must be consistent with all other requirements for enrolment of facial images.	Mandatory
3.1.25	Where multiple images are enrolled for a single person in a gallery, the facial recognition Service will enable the enrolment of images to be performed in a manner that enables them to be used together to improve the matching performance of identification and verification matches over a single image being enrolled in the gallery.	Desirable
3.1.26	<p>The facial recognition Service will provide a report of enrolment failures for a requested period (date range) providing a breakdown of the quality scores and reasons images fail to enrol.</p> <p>This report must be suitable for use by the business in consultation with the facial recognition Service Provider to adjust quality check settings to meet business objectives.</p>	Mandatory

Verification

This section presents the requirements for verification comparisons (1:1) within the facial recognition Service.

Ref	Requirement Description	Priority
3.2.1	The facial recognition Service must provide a system interface to enable automated verification comparisons to be performed	Mandatory
3.2.2	The facial recognition Service must provide a user interface to enable manual verification comparisons to be performed by an authorised user.	Mandatory
3.2.3	The facial recognition Service must be able to perform verification between 2 images when a probe image and the reference image are provided on the request.	Mandatory

Ref	Requirement Description	Priority
3.2.4	The facial recognition Service must be able to perform verification between 2 images when the unique image identifier of the probe image and reference image is provided on the request and both images have been enrolled in the gallery.	Mandatory
3.2.5	The facial recognition Service must be able to perform a verification between 2 images in a gallery when the probe image and the unique image identifier of the reference image is provided on the request, and the reference image has been enrolled in the gallery.	Mandatory
3.2.6	The facial recognition Service must return a comparison score representing the likelihood of a correct match between the probe image and the reference image.	Mandatory
3.2.7	The comparison score returned for individual image similarity to the probe must be deterministic in that the same comparison score must be returned for the same probe and reference image pair on each execution.	Mandatory
3.2.8	The facial recognition Service Provider must determine the appropriate operating thresholds for verification for each application risk profile in consultation with DIA.	Mandatory
3.2.9	The facial recognition Service Provider must implement an on-going process to ensure the facial recognition Verification Service is operating at the agreed operating point. The process must ensure the integrity and privacy of data is maintained including ensuring the process cannot be used for phishing of individuals.	Mandatory
3.2.10	When an image is provided on a verification request, and the eye coordinates are included with the image on the request, the facial recognition Service must utilise the provided eye coordinates when generating a template from the image(s) in the request	Mandatory
3.2.11	Where multiple reference images are available for a single identity the Verification should be capable of utilising the available images to improve the likelihood of a correct match over the use of a single reference image.	Desirable
3.2.12	The facial recognition Service must enable a unique transaction identifier to be included with a verification request that uniquely identifies the specific transaction.	Mandatory
3.2.13	The facial recognition Service must store all results for all verification requests in a manner such that the results are available for operational analysis.	Mandatory
3.2.14	The stored results should include the unique transaction identifier to enable correlation of results to passport processing activities.	Desirable
3.2.15	An audit record must be stored within the system for all attempts to perform a verification and will include at a minimum: <ul style="list-style-type: none"> • The unique transaction identifier • The unique image identifier(s) provide on the request • The gallery the comparison is performed against • The comparison score • The outcome (success/failure) of the verification attempt • The reason for failure, when verification fails to be completed. 	Mandatory

Ref	Requirement Description	Priority
	<ul style="list-style-type: none"> The authenticated account identifier which initiated the request <p>The authenticated account identifier must be in a readable format that can identify the end user or automated system process submitting the request.</p>	
3.2.16	<p>The facial recognition Service will provide a mechanism to extract verification comparison scores including transaction and image identifiers, for a requested period (date range).</p> <p>This extract must be suitable for use by the business in consultation with the facial recognition Service Provider to adjust thresholds to meet business objectives.</p>	Mandatory

Identification

This section presents the requirements for Identification Searches (1: Many) within the facial recognition Service.

Ref	Requirement Description	Priority
3.3.1	The facial recognition Service must provide a system interface to enable automated identification searches to be performed	Mandatory
3.3.2	The facial recognition Service must provide a user interface to enable manual identification searches to be performed by an authorised user.	Mandatory
3.3.3	The facial recognition Service must be able to perform an identification search using a probe image provided on the request against a gallery of enrolled images.	Mandatory
3.3.4	The facial recognition Service must enable the gallery used for a search to be specified as part of the request.	Mandatory
3.3.5	The facial recognition Service must return a ranked list of comparison scores and unique image identifiers for all images in the gallery that are deemed to be a match to the probe image.	Mandatory
3.3.6	The comparison score returned for individual image similarity to the probe must be deterministic in that the same comparison score must be returned for the same probe image/reference image pair on each search execution, despite any change in the total enrolled images.	Mandatory
3.3.7	The facial recognition Service must enable the requestor to choose if the stored facial image is included in the result list for each result	Mandatory
3.3.8	The facial recognition Service should include a reference (url) in the result list which will enable the facial image to be retrieve at a later date when the result is being viewed by an operator.	Desirable
3.3.9	The facial recognition Service must enable the list of results returned to be restricted based on a pre-configured maximum number of results.	Mandatory
3.3.10	The facial recognition Service should enable the list of results returned to be restricted based on a pre-configured score threshold.	Desirable

Ref	Requirement Description	Priority
3.3.11	The facial recognition Service must enable the pre-configured maximum number of results to be overridden, when a maximum number of results is included in the request.	Mandatory
3.3.12	The facial recognition Service should enable the pre-configured score threshold to be overridden, when a score threshold is included in the request	Desirable
3.3.13	When the eye coordinates for the probe image are included in the request, the facial recognition Service will utilise the provided eye coordinates when generating a template from the probe image to perform the search.	Mandatory
3.3.14	Where different algorithms parameters or configurations are available to tune a search to control speed, accuracy or to reflect image quality or other conditions, these must be preconfigured for normal use to control the operating point of the identification searches.	Mandatory
3.3.15	The facial recognition Service will support identification searches against the full enrolled population.	Mandatory
3.3.16	The facial recognition Service Provider must determine the appropriate configuration settings to set the agreed operating point for identification searches in consultation with DIA.	Mandatory
3.3.17	The facial recognition Service Provider must determine the appropriate score thresholds for identification searches for each application risk profile in consultation with DIA, based on the configured operating point.	Mandatory
3.3.18	The facial recognition Service Provider must implement an on-going process to ensure the facial recognition Identification Service is operating at the agreed operating point for each gallery. The process must ensure the integrity and privacy of data is maintained including ensuring the process cannot be used for phishing of individuals.	Mandatory
3.3.19	Where multiple images are available for a single identity the identification search should be capable of utilising the available images to improve the likelihood of a correct match over the use of a single reference image.	Desirable
3.3.1	The facial recognition Service must enable a unique transaction identifier to be included with an identification request that uniquely identifies the specific transaction.	Mandatory
3.3.20	The facial recognition Service must include a unique transaction identifier with the identification results which can be used to correlate the results to passport processing activities.	Mandatory
3.3.21	The facial recognition Service must store all results for all identification searches in a manner such that the results are available for operational analysis.	Mandatory
3.3.22	The stored results should include the unique transaction identifier to enable correlation of results to passport processing activities.	Desirable
3.3.23	The Watch list gallery must be capable of supporting 5000 entries.	Mandatory

Ref	Requirement Description	Priority
3.3.24	<p>An audit record must be stored within the system for all attempts to perform an identification search and will include at a minimum:</p> <ul style="list-style-type: none"> • The unique transaction identifier • The unique image identifier(s) provide on the request • The gallery the search is performed against • The comparisons scores for the candidate list(s) • The outcome (success/failure) of the identification attempt • The reason for failure, when identification fails to be completed. • The authenticated account identifier which initiated the request <p>The authenticated account identifier must be in a readable format that can identify the end user or automated system process submitting the request.</p>	Mandatory
3.3.25	<p>The facial recognition Service will provide a mechanism to extract Identification comparison scores including transaction and image identifiers, for a requested period (date range).</p> <p>This extract must be suitable for use by the business in consultation with the facial recognition Service Provider to adjust thresholds to meet business objectives.</p>	Mandatory

Withdrawal

This section presents the requirements for the withdrawal (removal) of enrolments within facial recognition Service.

Ref	Requirement Description	Priority
3.4.1	The facial recognition Service must provide a system interface to enable automated withdrawals to be performed	Mandatory
3.4.2	The facial recognition Service must provide a user interface to enable manual withdrawals to be performed by an authorised user.	Mandatory
3.4.3	The facial recognition Service must be able to withdraw an enrolled facial image and all associated data.	Mandatory
3.4.4	The facial recognition Service must enable an enrolled facial image to be withdrawn from a specific gallery.	Mandatory
3.4.5	The facial recognition Service must withdraw the enrolled facial image for the unique image identifier provided on the request.	Mandatory
3.4.6	The facial recognition Service must enable a unique transaction identifier to be included with the withdrawal that uniquely identifies the specific transaction.	Mandatory
3.4.7	<p>An audit record must be stored within the system for all attempts to withdraw an enrolled facial image will include at a minimum:</p> <ul style="list-style-type: none"> • The unique transaction identifier • The unique image identifier • The Gallery being withdrawn from 	Mandatory

	<ul style="list-style-type: none"> • The outcome (success/failure) of the attempt to withdraw • The reason for failure, when an image fails to withdraw. • The authenticated account identifier which initiated the request <p>The authenticated account identifier must be in a readable format that can identify the end user or automated system process submitting the request.</p>	
3.4.8	The facial recognition Service must retain all existing audit records related to the enrolled facial image being withdrawn.	Mandatory
3.4.9	The facial recognition Service will enable the bulk withdrawal of enrolled images. Bulk withdrawal of enrolled images must be consistent with all other requirements for withdrawal of enrolled images.	Mandatory
3.4.10	The facial recognition Service will provide a report of withdrawn enrolments for a requested period (date range).	Mandatory

Investigations

This section presents the requirements for providing Investigations the capability to perform ad-hoc biometric forensic investigations with facial images using the facial recognition Service outside of the control of the passport processing system.

Ref	Requirement Description	Priority
3.5.1	<p>The facial recognition Service must provide a user interface for an authorised investigator to perform:</p> <ul style="list-style-type: none"> • Identification Searches • Verification • Manual Facial Image comparisons 	Mandatory
3.5.2	An investigator must be able to upload 1 or more facial images which can be submitted as the probe image for an Identification search.	Mandatory
3.5.3	An investigator must be able to select the gallery the Identification search must be performed against.	Mandatory
3.5.4	An investigator must only be able to select a gallery they are authorised to search.	Mandatory
3.5.5	Where different algorithms parameters or configurations are available to tune a search to control speed, accuracy image quality or other conditions these should be able to be modified, or pre- configured alternative configurations selected, to be used for 1 or more searches	Mandatory
3.5.6	Where a configuration change is used by an investigator for searching it will have no impact on the normal configuration used for system-controlled searches.	Mandatory
3.5.7	On performing a search, a ranked list of results based on comparison scores will be presented to the investigator including the unique image identifier, comparison score and facial image.	Mandatory

Ref	Requirement Description	Priority
3.5.8	The search results should optionally include any other information provided during enrolment.	Desirable
3.5.9	The investigator must be able to perform a verification comparison between 2 images uploaded by the investigator.	Mandatory
3.5.10	Images uploaded by an investigator should be able to be stored within a secure workspace restricted to only the investigator, for later reuse until manually deleted by the investigator.	Desirable
3.5.11	The result of the verification comparison must be displayed to the investigator.	Mandatory
3.5.12	The investigator must be able to select an individual result from identification searches or verification and perform a detailed manual image comparison between the matched image and the probe image.	Mandatory
3.5.13	While comparing images, the investigator must be able to perform manipulation on either image and/or overlay parts of images on each other.	Mandatory

De duplication Searches

This section presents the requirements for performing many to many searches of the full passport (or other galleries) to assist DIA in identifying duplicates identities resulting from processing errors or fraudulent applications.

Ref	Requirement Description	Priority
3.6.1	The facial recognition Service must provide sufficient processing resources to enable a deduplication search to be completed without impacting normal operational performance of the facial recognition Service.	Mandatory
3.6.2	A facial recognition Service provider must perform a deduplication search when required: To establish or re-establish base operating metrics following a change in algorithm. When a change in passport processing requires a large bulk enrolment for images where identification searches have not been previously performed.	Mandatory
3.6.3	Prior to performing a full deduplication search on a new algorithm, the facial recognition Service Provider must perform an initial evaluation on a subset of representative data using a selection of configurations to determine the preferred configuration for the new algorithm which is the optimum configuration for DIA.	Mandatory
3.6.4	When performing a deduplication search, the data included in results must be kept to a minimum to protect individual's privacy, as such only the unique image identifier and match scores should be recorded in results.	Mandatory
3.6.5	On completion of a deduplication search, only match results which exceed a threshold(s) will be extracted and provided to DIA for further analysis.	Mandatory

Ref	Requirement Description	Priority
3.6.6	The threshold must be agreed in consultation with DIA.	Mandatory
3.6.7	On completion of a deduplication search an evaluation report must be provided to DIA detailing the biometric performance and the changes/improvements from the previous version. The report must include the recommended score thresholds for identification searches for each application risk profile, based on the new configuration operating point.	Mandatory
3.6.8	The new thresholds must be agreed in consultation with DIA	Mandatory

Released under the Official Information Act 1982

Non-Functional Service Requirements

The following table presents the general service requirements the successful Facial Recognition solution will need to meet. The general service requirements have been prioritised using the following criteria:

Value	Description
Mandatory	<ul style="list-style-type: none"> The product must meet this requirement. This is business critical functionality and products that do not meet this requirement will be significantly impacted.
Desirable	<ul style="list-style-type: none"> The product should meet this requirement. Not essential but the business might be impeded without it. Alternative or work around solutions may be considered.
Optional	<ul style="list-style-type: none"> 'Nice to have'. The product could meet this requirement provided the time and cost involved are not prohibitive. Alternative workarounds are available.

Availability and Recoverability

Ref	Requirement Description	Priority
4.1.1	<p>The Service must be designed to provide services at different levels of availability. At least 3 Service Categories shall be provided to allow differing levels of availability at different price points for the same size service to meet production and non-production usage.</p> <p>Where a Service Category is defined by the following:</p> <ul style="list-style-type: none"> Target Availability Operational Hours MTRR Recovery Time Objective (RTO) Recovery Point Objective (RPO) <p>(Target Availability excludes approved Planned Outages.)</p>	Mandatory
4.1.2	<p>The Production Service Category must provide an Availability of the least 99.9% excluding planned outages.</p> <p>Availability will be reported on monthly as defined by the service contract.</p> <ul style="list-style-type: none"> Target Availability = 99.9% Operational Hours = 24 *7 MTRR = 30 minutes RTO = 24 hours RPO = 15 minutes 	Mandatory
4.1.3	Production planned outages must be limited to a maximum of 1 outage per month	Mandatory

Ref	Requirement Description	Priority
	for a maximum of 2 hours.	
4.1.4	Services must be designed and deployed with a level of separation that ensures there is no resource contention between services. Each service must meet the defined service levels regardless of other service loads.	Mandatory
4.1.5	In the situation where a major event causes an outage, the product must support the DIA's Recover Time Objective (RTO) of 24 hours (the maximum amount of time permitted to recover the system following a major incident).	Mandatory
4.1.6	In the situation where a major event causes an outage the product must support the DIA's Recovery Point Objective (RPO) of 15 minutes. (the maximum amount of data that may be lost when the service is restored following a major incident)	Mandatory
4.1.7	The Service Provider must provide DR capability that must: Be a full equivalent of the Production environment meeting all the Functional and Non-Functional requirements when in use. Meet the specified RTO and RPO. Be geographically separated from production environment. Ensure that use of other environments (e.g. Performance testing in QA) have no impact on the DR environment.	Mandatory

Performance and Scalability

Ref	Requirement Description	Priority
4.2.1	The service provider shall ensure that for all user-initiated requests: <ul style="list-style-type: none"> 85% must return a successful result to the user within 2 seconds. 99% must return a successful result to the user within 4 seconds. NOTE: Where a response time has been stated for a specific transaction, this will override the timings stated in this requirement.	Mandatory
4.2.2	The service provider shall ensure that for all system requests response times are in line with industry best practice for the planned usage. NOTE: A contractual response time will be agreed in consultation with the preferred supplier, which meets the required throughput and minimises operator delays when executing tests.	Mandatory
4.2.3	The service provider must measure and record all transaction response times. Transaction performance shall be reported on monthly and provided to DIA.	Mandatory
4.2.4	Transaction response times for the service are as experience by the client calling the service. Any network latency between the Service Provider data centre and the agency servers must be allowed for in service design to meet the response times.	Mandatory
4.2.5	The facial recognition Service provider must support a throughput that will enable a passport processing volume averaging 600 Applications per hour, consisting of a	Mandatory

Ref	Requirement Description	Priority
	<p>work load distribution of:</p> <ul style="list-style-type: none"> • 80% Renewal Applicants requiring <ul style="list-style-type: none"> ○ one enrolment, one 1:1 and two 1:9(2)(k) ○ two 1:9(2)(k) • 20% First Time Applicants requiring <ul style="list-style-type: none"> ○ one enrolment, one 1: many and two 1:9(2)(k) ○ two 1:9(2)(k) <p>Note: Processing of an Application may require tests to be executed multiple times which vary depending on the Application Type and Channel.</p>	
4.2.6	The facial recognition services must be able to scale to process increases in processing volumes	Mandatory
4.2.7	The facial recognition services must be able to scale to process increases in population sizes.	Mandatory

Support and Maintenance

Ref	Requirement Description	Priority
4.3.1	The solution must have the ability to handle both recoverable and unrecoverable errors to maintain data atomicity, consistency, isolation and durability. It must capture date, time, user, correlation ID, error code and descriptions in the service response and log files for problem diagnosis purpose.	Mandatory
4.3.2	24 x 7 x 365 monitoring, alerting and proactive response to incidents and threats.	Mandatory
4.3.3	The Service Provider must comply with DIA's incident management processes.	Mandatory
4.3.4	The Service Provider must be able to send system alerts/events to DIA on request.	Mandatory
4.3.5	The Service Provider must comply with DIA's change management processes.	Mandatory
4.3.6	The Service Provider must provide ongoing management of the service and all related components required for the delivery of the services.	Mandatory
4.3.7	The Service Provider must provide ongoing hardware and software upgrades over the contract period.	Mandatory

Security

Ref	Requirement Description	Priority
4.4.1	The Service Provider must ensure that the service is designed, built and operated in such a manner to support DIA compliance with the Protective Security Requirements (PSR) https://www.protectivesecurity.govt.nz/ and New Zealand Information Security Manual (NZISM) http://www.gcsb.govt.nz/publications/the-nz-information-security-manual/ . Compliance must be maintained with	Mandatory

Ref	Requirement Description	Priority
	subsequent updates.	
4.4.2	The Service provider must create and operate an Information Security Management System that is compliant with ISO/IEC 27000 Series and subsequent updates. http://www.iso27001security.com/html/27001.html	Mandatory
4.4.3	The Service Provider must ensure that the service is compliant with the baseline control set in the NZISM for protectively marked information at 'RESTRICTED'.	Mandatory
4.4.4	The Service Provider must apply an appropriate level of encryption, compliant with NZISM, to both data at rest and data in transit. All data in transit between security zones MUST be encrypted. All data in transit within a security zone SHOULD be encrypted.	Mandatory
4.4.5	All access to the solution must be authenticated and authorised using an appropriate means as detailed in NZISM.	Mandatory
4.4.6	User authorisation must be granular to enable access to individual gallery to be authorised	Mandatory
4.4.7	All infrastructure used to deliver the service must be secured using industry best practice including configuration, hardening, regular patching and maintenance.	Mandatory
4.4.8	There must be strict segregation of DIA data from data belonging to all other clients of the Service Provider. The segregation must be assured to a level appropriate to the service model agreed with DIA.	Mandatory
4.4.9	Security must be integrated with the appropriate information monitoring and management services.	Mandatory
4.4.10	Provide an independent security assurance program on at least an annual basis. Comply with ISAE3402.	Mandatory
4.4.11	The hosting data centre, infrastructure and operational service MUST have DIA Security Certification and Accreditation. This must be achieved before go live.	Mandatory
4.4.13	The Service Provider must protect the integrity of audit records by ensuring they are protected from tampering and from unauthorised access or modification	Mandatory
4.4.12	The facial recognition Service will provide a report of service audit events for a requested period (date range).	Mandatory
4.4.13	The Service provider must have the capability to capture and provide DIA the historic data required for audits and after the event reviews including but not limited to email, web and network activities of staff for up to 18 months. This information must be provided on request.	Mandatory

Standards

Ref	Requirement Description	Priority
4.5.1	The Service Provider must comply with the Privacy Act and subsequent updates. http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html	Mandatory
4.5.2	The Service Provider must comply with the legislative requirements to maintain public records. The Service Provider must ensure the integrity of stored data. Retention of data must not prevent archiving. http://www.legislation.govt.nz/act/public/2005/0040/latest/DLM345529.html	Mandatory
4.5.3	The solution shall expose services via an industry standard interface (eg REST, SOAP). This will increase the interoperability of the existing DIA systems and the service	Desirable
4.5.4	Web based user Interfaces solution shall conform to NZ Government Web Usability and Accessibility Standards, except where specific exemptions have been granted from the appropriate DIA governing body. https://webtoolkit.govt.nz/standards/web-usability-standard-1-2/ https://webtoolkit.govt.nz/standards/web-accessibility-standard-1-0/	Desirable
4.5.5	The solution must be able to process images conforming to ICAO Doc 9303 (2015) Part 9: Deployment of Biometric Identification and Electronic Storage of Data in eMRTDs	Mandatory
4.5.6	The solution must be able to process images conforming to the ISO/IEC 19794:2005 Information technology — Biometric data interchange formats — Part 5: Face image data	Mandatory

General

Ref	Requirement Description	Priority
4.6.1	The Service Provider must provide services to support the following environments: <ul style="list-style-type: none"> • Production • Quality Assurance • Disaster Recovery • Test • Development 	Mandatory
4.6.2	The Service Provider shall enable additional instances to be configured for the following environments to support parallel development of DIA systems: <ul style="list-style-type: none"> • Quality Assurance • Test • Development 	Desirable
4.6.3	Current as-built documentation must be maintained for all services provided, and updated within one month of any change	Mandatory

Appendix N: Project Team Bios

9(2)(a)

[Redacted]

9(2)(a)

[Redacted]

9(2)(a)

[Redacted]

9(2)(a)

[Redacted]

9(2)(a) [Redacted]

9(2)(a) [Redacted]

[Redacted]

Released under the Official Information Act 1982

Appendix O: Best Practices derived from Lessons learned

Key findings from the lessons learned review process with DXC Technology, NEC and the DIA project team are summarised below. These lessons have been incorporated into the project approach including for change management.

- Have a clear governance structure, decision making and escalation path and a Communications Plan that includes these aspects of the project.
- Ensure Service Delivery & Operations Management is kept well informed of proposed changes and issues to enable them to make sound decisions and to not negatively impact operations.
- Ensure the roles, responsibilities and organisational boundaries and interfaces between DIA project team and all suppliers involved in the implementation are clear
- Ensure the project team includes expertise required to deliver the project.
- Bring the project delivery team together at the start of the project to discuss and agree the integrated plan, interdependencies, responsible resources and project management and governance structure.
- Engage project team, staff and suppliers so that everyone has shared expectations and will work together to anticipate issues that could occur and risks.
- Confirm and review dependencies during the planning stage and throughout the project lifecycle.
- Ensure team members have visibility of risks and issues and are not afraid to raise concerns immediately, otherwise delays may occur.
- Use a risk assessment approach to diagnose potential problems and apply mitigations early where possible
- Strong scope management, requirements and traceability matrix management.
- Manage resourcing across Business as Usual and Project allocations more effectively and realistically.
- Hold regular and effective team meetings and where practical co-locate teams.
- Good preparation planning for all stages.
- Allow enough time for document clarification process and reviews and that the documents are understood by relevant teams.
- DIA project resources, SMEs and supplier teams to work collaboratively on deliverables and activities to share knowledge and to mitigate any gaps or disconnections and to learn from others experience.
- Involve the Capability and Training team and Business representatives early on in the design process to build engagement and open discussion around what was needed versus what was possible
- Involve business PIV/ SMEs early in the project in user acceptance testing and deployment planning to enable business planning.

- If time and cost considerations allow, the correct number of environments should be available. Where this is not possible, rigorous environment and release planning needs to be agreed by the business owners and their priorities.

Released under the Official Information Act 1982

Appendix P: Facial Recognition Replacement Project Stages

The following sections outline further detail on the stages including overall project milestones (Table 30).

About the stages

Stage 1: Detailed design

Stage 1 is intended to develop and complete the architecture document for the Facial Recognition Service and Passport Systems Integration, and the design documents for the Facial Recognition service and functionality. During this stage the project team will begin to build their understanding of the new capability, to inform the planning and delivery of their key activities and deliverables.

Stage 2: Facial Recognition Service & Integration Build

This stage consists of the build, installation, configuration and testing that the supplier will undertake of the new Facial Recognition capability and its integration with the Passports System prior to handover to DIA for deployment into its Quality Assurance (QA) environment for end to end testing.

This stage involves:

1. Facial Recognition Service Build activities:
 - a. Commissioning Facial Recognition Service platforms to two datacentres
 - b. Commission Facial Recognition software environments
 - c. FR Software installation and configuration including thresholds
 - d. Transition of the supplier's Facial Recognition Service development and test environments
 - e. Supplier's acceptance testing
 - f. Transition of the Facial Recognition Service QA environment including enrolment of images.
 - g. Transition of the Facial Recognition Service Production environment including a full production data migration conducted as a rehearsal to inform production transition, verify data integrity, tuning and optimising the environment.
 - h. Supplier Facial Recognition Service system integration testing.
 - i. Performance testing and failover testing in the Facial Recognition Service Production environment.
2. Passport System, KIWI, integration and enhancement build activities
 - a. Detailed design and build activities for the Facial Recognition integration and enhancements
 - b. System integration testing
 - c. Release package handover to DIA

In parallel to the technology activities, the following activities will be undertaken:

- a. data migration approach planning
- b. security certification and accreditation

- c. change management and business engagement planning, training and business acceptance test planning
- d. updating policies and procedures
- e. developing support model for ongoing operations and support
- f. planning decommissioning activities

Stage 3: DIA Testing

Once the QA environment deployments are completed by DIA's Application Support team, DIA will carry out user acceptance testing and business acceptance testing.

This testing stage also includes penetration testing, performance testing and disaster recovery/rehearsal scenario planning and testing.

Training material will have been developed and the business acceptance testers trained prior to their business acceptance testing.

During this phase, communications for stakeholders and those users impacted by the new Facial Recognition service and Passport system enhancements will be developed and updated ready for production transition.

Stage 4: Production Transition

This stage will involve confirming that all production transition, operational readiness, support arrangements and governance sign off pre-requisites are completed and approved prior to Production Transition.

Planning and confirming of the production transition plan, risk management plan and resource plan for the transition and post go live support will occur during this stage.

This phase includes the production transition and post go live support (technical and business operations support) by the supplier, project team and Passport system power users.

Project deliverables

Project management documents

- Project Initiation Document
- Integrated Project Plan
- Benefits Management Plan
- Assurance Plan
- Project Board meeting papers
- Open Syndicated Agreement for Facial Recognition Services
- Third party supplier statements of work
- Amend/ revocation of existing supplier contracts/ licences for decommissioned assets
- Adaptive - Project budget and forecasts
- Psoda (PMIS) – decisions, risks, issues, project controls
- Project status reports
- Change requests

Architecture & Design documents

- Architecture document
- FR Service Design Specification
- Biometric Design Specification
- FR Integration High Level and Detailed Design specifications
- Network design
- Release Package
- Software Source
- Data migration approach document
- Decommissioning plan

Requirements, Processes, Polices

- FR Service Requirements
- FR Integration requirements
- Processes, policies and procedures

Business Change Management

- Change Management Plan
- Stakeholder Management Plan
- Communications Plan
- Training Plan
- Training material for Business Acceptance Testers
- Training material for Investigations and Application Support Teams
- Effectiveness for Maori

Privacy & Security

- Privacy Impact Assessment: Threshold
- Business security risk assessment
- Security Certification and Accreditation
- Penetration testing report

Test Governance

- FR Service Test Strategy
- SIT Test Cases
- FR Service Performance test cases
- FR Service technical failover test plan
- FR Service test results
- UAT Test Strategy Plan
- UAT Test cases and scripts
- UAT test results
- Rehearsal/ DR Scenarios
- Performance test scenarios and plan
- DIA Test Exit report

Support model

- Service Support Design Package
- Service Desk Standard Operating Procedures & Knowledge Articles
- Tuwhiria updates of applicable policies and procedures

Production Transition

- Production transition plan
- Production transition risk management plan
- Operations Guide
- Technical Advisory Board & Change Authority Board change orders
- Operational Readiness checklist
- Governance GO/NO GO Decision Approval Memo
- Post Implementation Verification Test scripts
- Post Implementation Verification Test sign off

Closure

- Lessons Learned
- Post Implementation Review report
- Financial report
- End Project Report

Appendix Q: List of Assurance Activities

Assurance Activity	Purpose	Audience	Assurance Provider	Frequency date scheduled
Project Status Reports	Provides stakeholders with a view of project status, highlights and exceptions	Life Events & Identity Services Portfolio Board, Project Exec, EPMO, Senior Supplier	Project Manager	Monthly
Project Financial Budget and Forecast Updates	Ensure project budget and contingency are validated. Ensure project spend remains within approved budget. Ensure project spend is accurate against forecast estimates. Highlight variance risks and opportunities	Life Events & Identity Services Portfolio Board, Project Exec, EPMO	Project Manager and Senior Management Accountant	Monthly
Life Events & Identity Portfolio Board Meetings	Review project status, provide direction and respond to escalated issues and risks	SRO/DCE	Project Executive	Monthly
Project RAID (Risks, Assumptions, Issues, and Dependencies) reviews	Review the treatment and active management of risks, identify, analyse and record new risks. Agree on risks that require escalation or closure.	Portfolio Board, EPMO	Project Manager	Fortnightly
Business Case reviews	Assurance that the options analysis and financial model are robust and that it can be delivered.	Joint Ministers, Cabinet, IMAP, CE, ELT, OLT, IGC, DCE SDO, Project Executive	Project team, EPMO, DIA SME	Business case review, prior to submitting for approval
Quantitative Risk Assessment (QRA)	Provide review of the project's financial model, and provide information on the appropriate setting of the contingency, and budget tolerance.	Investment Governance Committee, Treasury	Ascent Business Consulting Ltd	August 2018 – to be included in Financial Case/ Business Case
Benefits and Value Management	Oversight of benefits realisation	Project Executive, Investment	Manager, Analytics & Reporting	Every six months once system is in production

Assurance Activity	Purpose	Audience	Assurance Provider	Frequency date scheduled
Reviews		Governance Committee		
Project Initiation Document review	Assurance that all aspects of the project scope, delivery plan, budget, resource plan, management and controls are in place so that the project can deliver successfully including the supplier and other third-party resources.	Project Executive	Project Manager, Project Team, EPMO, Manager Project Delivery SDO	Prior to Implementation Stage Gate approval
SDLC and Project Management Tailoring Checkpoints	Agree the artefacts that the project is required to completed based on risk and complexity.	Project Executive	EPMO, TSS Assessment Group	Stage gates
Deliverable / artefact quality assurance	Confirm that each document output is fit for purpose and meets the standards relevant to that document	Consumers of information in documents	Peer review Management review and approval	Scheduled as part of the document creation and update cycle
Internal delivery monitoring	Assurance of delivery supplier status reports, project meetings, weekly schedule updates and other engagements e.g. 1-1 meetings.	Project Executive, Portfolio Board	Project Manager	Daily, ongoing
Stage Gate Reviews	To review performance of stage, and provide approval to proceed based on project deliverables being completed to the appropriate quality standard.	Project Executive, Portfolio Board, EPMO	Manager Project Delivery SDO	At the end of each project stage (as specified in the PID)
Sourcing & Procurement Governance	Ensures that procurement process follows due process, is in accordance with the government rules of sourcing and that probity is observed.	MBIE – Government Procurement Project Executive	Manager, ICT Procurement Probity Audit	As per project schedule
Strategic Solution Approach & Architecture Document	Assurance that all solution architecture documents are traceable to ISSP Themes, EAF, reference architectures, SSAs, privacy and security	Portfolio Board	Design Authority & Digital Business Governance	Prior to Implementation Business Case approval and Detailed Design

Assurance Activity	Purpose	Audience	Assurance Provider	Frequency date scheduled
	requirements, technical design principles and standards, and project benefits		Board (DBGB)	stage
Privacy Impact Assessment	Privacy impacts of proposed designs are understood and appropriately managed	DIA Privacy Advisors Project Executive Senior Users	Business Analyst Third Party Provider	Privacy Threshold Assessment was approved by the Privacy Team To be updated if any further changes arise
Security risk assessment and Certification & Accreditation	To identify and assess the design, implementation and effectiveness of controls for the FR Service against the agency's risk profile and appetite, design specifications, agencies security polices and standards and NZISM.	Project Executive and Senior Users Chief Security & Risk Officer	Security & Risk	As per project schedule and pre-requisite for production transition
Test Certification	Provides assurance that deliverables are fit for purpose, do not contain high severity defects are the solution can be deployed to production	Project Executive, Portfolio Board	Testing Services	End of Feb 2020 Pre-requisite for production transition
Operational Readiness Review	Assurance that a new or changed solution, system, or service is ready to go live into the production environment, that operational teams have received and accepted everything they need to deliver and support the service to the agreed quality levels, that operational/delivered risks are confirmed & understood.	Project Executive, Senior Users, Te Ara Manaaki Change Director	Project Manager/ Change Advisor	On a release basis
Production Transition Acceptance	To provide assurance that all the technical and stakeholder pre-requisites for production transition have been approved, that the production transition and support arrangements have been planned and are in place for	Project Executive, Project Board, TSS Management	Technical Approval Board Change Approval Board	Prior to Production Release

Assurance Activity	Purpose	Audience	Assurance Provider	Frequency date scheduled
	production transition, and the operational teams that will receive and use the capabilities are ready to receive the change.			
IGC Capital Plan Reporting	Review Capital Plan, project status and respond to escalated issues and risks.	Investment Governance Committee	Finance, EPMO	Quarterly
Quarterly ELT Project Status Reports	Review project status (based on project quality data and including benefits management) and provide direction.	CE/ ELT	Finance, EPMO, Strategy & Governance	Quarterly
DIA EPMO meetings	Ensures compliance with DIA methods, standards and good practice.	Project Executive	Project Manager, Senior EPMO Advisor	Monthly
Project Governance Review	Assess whether Programme Governance is still fit for purpose.	ELT	SRO	Yearly
Independent Quality Assurance (IQA)	Provide independent assurance that the Project is being managed in accordance with good practice. Provides Project Sponsor with confidence that the expected business outcomes and benefits will be realised. At the discretion of the Chief Portfolio Manager and the Project Sponsor, an IQA may be undertaken by an external third party.	Project Executive, Portfolio Board, EPMO, Investment Governance Committee, Corporate Centre	EPMO	Prior to Implementation Business Case submission for Joint Ministers' approval (November/December 2018)
End project review	Assurance that lessons learned are identified with the Project team and incorporated into project management practices.	Project Executive, Portfolio Board	Project team, Manager Project Delivery SDO, EPMO	Project Closure

Addendum 1: Responses to State Services Commission feedback

Responses to questions from State Services Commission received after Life Events & Identity Services Board approval, which could not be incorporated into the approved business case.

1. *Can you quantify (or at least approximate/proxy) the value of the NZ passport 5 nations status and visa waiver in other countries which arises as a result of using FR? i.e. the benefit to customers? If so, can/should this be included as a "dis-benefit" under option 1? Should the preferred option also include quantification of "customer benefits"? At the moment the business case is primarily oriented around cost and benefit to DIA.*
 - A. The value of NZ visa waiver status has not been calculated as an economic benefit. The cost of the economic analysis to answer this question was considered too high, considering that Option 1 was eliminated as not meeting strategic/business needs. Option 2 did consider customer impact, because if DIA were to choose to return to the old way of validating passport applications photos with a witness signature, then customer dis-benefit would be high, however, this was not considered to be the only choice available, with other identity verification measures now becoming available, so this dis-benefit could not be reliably used to discount Option 2. In the end, option 2 was discounted as not meeting strategic or business objectives.
2. *Does/should option 1 include the cost of additional staff to complete manual checking to "compensate" for discontinued use of FR, as well as adjusted service levels etc? (I couldn't tell if this is what is included in the \$1m whole of life costs?). Was an option considered that would involve for example, doubling the number of processing staff while halving service levels (e.g. 20 days rather than 10 days to receive a passport).*
 - A. Option 1 was to continue using an unsupported facial recognition system. The option to return to manual passport application processing was scope option 3 (S3) of the long list, and it was discounted for multiple reasons, including not matching strategic Te Ara Manaaki 'straight-through processing' objectives, the inability of humans to do 1 to many fraud detection, and the desire of customers to have the option to pay for rapid passport application turnaround times.

As a public service system we need to know whether we can realistically move to one or fewer FR systems, rather than 4-6 different systems across different agencies – particularly for agencies working at the border. My questions are:

3. *Did the existing providers to INZ, Police, and Customs respond to the RFP? If so, what ruled them out? (Esp INZ who have recently implemented a new solution).*
 - A. INZ (MBIE), NZTA, Police and Customs were involved in discussions prior to the market engagement, to evaluate the possibility of sharing their solutions. Unfortunately none of the existing solutions had been designed as open, syndicated services, and were not able to be shared /used by DIA.
4. *How realistic is the proposition that other agencies may join a syndicated contract in the future? Is it possible to know this if their requirements are not yet "known"?*
 - A. DIA has, despite additional cost and effort, followed the government ICT strategy and ensured that the new service can be shared. There are examples of government agencies using shared services once they become available (ECM as a service being one). NZTA, who

does not yet have a facial recognition solution, is likely to be the earliest external agency adopter of the shared service, since they do not have to wait for existing contracts to expire. Their business case for the use of a facial recognition service has not yet been approved, so it was not possible for them to make a commitment. Their expected usage (explained in Appendix K) would allow them to use the 1:1 module in a similar way to the method DIA uses for passport renewals.

5. *What would be the consequences if this business case/investment was delayed until the NZTA requirements were understood, and potentially included to deliver one solution for both?*
 - A. We don't need to delay for NZTA to come on board. The syndicated agreement already contains benefits to the NZ government for adoption of the service by more agencies, since this was part of the lengthy negotiations. There is significant risk to DIA of delay, since the current solution is unsupported and cannot be upgraded to match infrastructure operating system updates.

6. *Did DIA consider an independent member on the governance as a further assurance measure? What about including a senior manager from one of the other future users, eg NZTA, as a first step to building system capability/interoperability?*
 - A. The shared service has been architecturally designed to be "called" by an application through a set of open standards (see page 54). This enables it to be used by other applications within DIA or by other agencies, without future design changes. There is a stakeholder engagement plan which includes keeping members of the NZ government Cross Government Biometrics Group up to date with progress of the project and availability of the shared service. This is likely to be the preferred method for these agencies to be kept updated.

7. *As I understand it, the passports system is fully cost-recoverable. How will this investment affect future fees/revenue? I compare for example, the LINZ ASATs business case which is prepared on the basis that it is a repayable capital injection, and the fee review is a critical dependency of the programme to realise its benefits. This appears to be a significant gap in the business case?*
 - A. As Facial Recognition relates to the provision of the Passports service, it will be funded from the Passports Memorandum Account. Periodic fee reviews are conducted on the memorandum account to ensure that fees charged recover costs over the medium to longer term. The next fee review is due for Cabinet consideration in November 2018, and includes the project and ongoing cost impacts of the Facial Recognition project. Reference to this has been made in the financial case and executive summary of the business case.