MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

Business Case – Immigration National Security Screening (INSS) - Medium Complexity

Project Code/Name:	*3453 –Immigration National Security Screening*		
Project Description: (short)	The Immigration New Zealand (INZ) National Security (INSS) project has the objective that as trusted stewards of the immigration system, we work with our partners to protect New Zealand's National Security. National Security screening will be re-engineered to provide an agile system (i.e. end-to end process) where risks from migrants can be tracked, measured and controlled. s6(a) [redacted]. Deeper assessments of migrants will be conducted on migrants where the threat is greatest. • Staff from INZ and NZSIS will provide specialist threat assessment direction for each of the identified threats as articulated by NZ's National Security intelligence priorities. The management of security risks will be aligned with the INZ risk model. • System enhancements will improve levels of automation and support initiatives digitising processes across INZ. • Learning and development materials and instructions will support the system to ensure it is simple clear and well understood.		
Project Sponsor:	Jacqui Ellis	**Business Owner:**	9 (2) (a) [redacted]
Business Unit:	Insights Data Intelligence	**Project Manager:**	9(2)(a) [redacted]
Complexity	*Medium*	**Delivery Approach**	Staged
Document and Version Submitted	*Medium*	**Date Submitted**	21 May 2020
Capex Investment Bid: (Indicative cost)	*$1.063m*	**Opex Investment Bid:** (Indicative cost)	$45k
Total Capex: (for entire project)	$3.178m	**Total Opex:** (for entire project)	$821k
Capex Requested in this submission:	*$1.063m*	**Opex requested in this submission:**	$34k
Funding Source(s)	INZ Internal Funding	**Cost Centre**	TBC
Treasury Risk Profile Assessment	Medium		

Recommendations:	**Decision**
Approve: Procurement approach for Stage One deliverables **Approve:** Stage One costs for technical deliverables from INZ Internal Funding: • AMS changes integrating with Rules and Portal ($420k) • System environment costs in year one ($93k)	
Approve: ICT and project resource costs for stage one deliverables ($564,740)	
Approve: Expected ongoing Opex for licences supporting technology deliverables: ($194k p.a.) A decision on the cost centre to incur these Opex costs is required **Note:** Ongoing Opex requirements have been reviewed with Finance	
Approve: The project close date of *31/10/2021*	

Released under the Official Information Act 1982

Summary of capital and operational costs including out years							
	Current FY 19/20	FY 20/21	FY 21/22	FY 22/23	FY 23/24	FY 24/25	**Total**
Total project delivery capex expenditure	47,062	2,778,186	353,072	s9(2)(j) [redacted]	[redacted]	[redacted]	[redacted]
Total project delivery opex expenditure	-	10,000	35,000	[redacted]	[redacted]	[redacted]	[redacted]
Estimated on-going business opex (excluding depreciation)	-	-	-	[redacted]	[redacted]	[redacted]	[redacted]
Estimated on-going ICT opex (excluding depreciation)	-	-	193,888	[redacted]	[redacted]	[redacted]	[redacted]
Whole of Life costs (capex + opex + on-going costs)	47,062	2,788,186	581,960	[redacted]	[redacted]	[redacted]	[redacted]
Net cash flow (Benefits less Total Costs)	-47,062	-2,788,186	-581,960	[redacted]	[redacted]	[redacted]	[redacted]

Funding Source	Crown Revenue	Third Party	Capital Injection	N/A
Cost Centre and/or appropriation (Stage 1 only)			1.063m	

Released under the Official Information Act 1982

Endorsed by

The following people have endorsed this document for submission to the Portfolio Board:

Function	Role	Comments; Caveats and Date Caveat to be / or actioned by	Date	Name and Signature
*Project Sponsor (M) **Jacqui Ellis**	Endorse		26/05/20	✉ RE INSS Case 21MA
*Business Owner (M) 9 (2) (a)	Endorse		26/05/20	✉ RE INSS Case 21MA
*MBIE Finance Business Partner (M) s9(2)(a)	Endorse		08/06/20	✉ RE Notes this mornin
Architecture Review Group	Endorse	High Level Design s 6 (a)	16/03/20	
Architecture Review Board	Endorse	High Level Design s 6 (a)	26/03/20	

Reviewed by

The following people have approved this document for submission to the appropriate Portfolio Advisory Committee:

Name	Responsibility	Date	Approval
9(2)(a)	Quality of the document.	09/06/20	
	Quality of the document	09/06/20	

Released under the Official Information Act 1982

Reference Documentation

The following is a list of reference documentation relating to this project:

Document Name & Mako link	Version	Date Endorsed /Approved
Project Brief s 6 (a) [redacted]		
Detailed Business Requirements s 6 (a) [redacted]		
[redacted]		
[redacted]		
Detailed Options Analysis • s 6 (a) [redacted] • s 6 (a) [redacted] • s 6 (a) [redacted] [redacted]		
s 6 (a) [redacted]		
[redacted]		
Background to Issues s 6 (a) [redacted]		
[redacted]		
[redacted]		
High Level Solution Design s 6 (a) [redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
Change Requests to date if any • s 6 (a) [redacted] [redacted]		

Released under the Official Information Act 1982

1. Executive Summary

Request for Funding	The INSS project is seeking funding for the first stage of the initiative that will set the foundations of an agile National Security screening system (i.e. end-to end process) that enables the risks to be tracked, measured and controlled effectively. Approval of costs of $1.063m is requested for a first stage. s6(a) [redacted] Processes and systems will be streamlined to improve their agility and adaptability, this supports changes implemented in later stages of the project and then BAU. Improved analytic capability will be introduced to improve the assessment and forecasting of impacts that may result from a change to security threat response.
The problem/ Opportunity	INZ has the statutory requirement that no visa is granted or waiver applied where a person is a likely threat to National Security as defined by NZ's National Security intelligence priorities. There are problems with how this is operationalised. • s6(c), s6(a) [redacted] As trusted stewards of the immigration system, we work with our partners to protect New Zealand's National Security. This initiative seeks to deliver a re-engineered National Security screening system to achieve this.
Affects	**<u>Primary</u>** – directly impacted by the problem: • Border and Visa Operations. • Verification and compliance. • Refugee and Migrant Services. • Intelligence, Data and Insights. **<u>Also impacted</u>** • Operations, Tasking and Improvement • Enablement. • Assurance. **<u>Other parties outside impacted by current issues include:</u>** • NZ Customs – impacted by numbers of arrivals to New Zealand and information available to assess arriving migrants. • NZSIS – impacted by increasing number of visa (and therefore NSC) applicants, information supplied with applications and rework required to deliver good security assessment outcomes.

Released under the Official Information Act 1982

	- Negative impact to desirable migration to New Zealand industry and Public and training institutions. - Reputational impacts on New Zealand and its partnerships.
The impact of which is	- s6(c) [redacted] - Delays to decision making. - Duplication and additional processing work for staff. - Over processing and delays to low risk migrants. - Increased reputational risk to New Zealand and its relationship with partners. - Increased risk of harm to New Zealander and New Zealanders.
Recommended option	Implement changes to address the needs through 4 incremental stages to ensure the final re-engineered security screening process is fit for purpose. Approve stage one to set the foundations of an agile National Security screening system (i.e. end-to end process) that enables the risks to be tracked, measured and controlled effectively. Stage one delivers benefits quickly in itself and supports stages 2 to 4 to reduce risks, improve accuracy of cost forecasts and address key dependencies including vendor and 3rd party arrangements. Other stages are described further in later sections within this document.
A successful stage one solution	An effective solution would: - s6(c) [redacted] - Following appropriate governance approval, allow business users to adjust risk settings in the system, without requiring input from ICT staff. - Provide robust, measurable and adaptable systems and processes and improvements in responsiveness.
Why should we invest now?	INZ should invest now to: - Support strategic initiatives to identify risk early and minimise the number of high-risk migrants entering New Zealand. - Support INZ digitisation initiatives providing enhancements in automation, being delivered through prioritised INZ initiatives like Automated Decision Assistance and Employer Direct Project which are streamlining the process for temporary and work visas. - INZ and government COVID planning for economic recovery and full reopening of the border (in restarting or quota) are underway. This includes assessing the new risk landscape. A responsive, agile system is needed to identify and manage risks and to advise decision makers at all levels. There is an opportunity to work with experts in Border and Visa Operations and risk and verification while they are available before the border reopens fully. - Improve compliance with the requirements in S16 and S4 of the Immigration Act (2009).

Released under the Official Information Act 1982

	• Be ready to support enhancements within NZSIS that can improve support provided to INZ.
Benefits of this Investment in stage one	• Screening coverage and quality can be assessed. (Known level of coverage) • Reduced likelihood of threats from migrants arriving onshore. • System is responsive to changes, able to adapt for most changes within days. (Within 7 days for 90% of changes) • Faster identification of threats, completion of screening assessments. (Responsiveness measured and improved)
Stage One would support:	• A robust approach with clear processes to assess and treat security threats. • Clear guidance to assess on security threats made available to all relevant staff. • Automatic logging of action taken when migrants are assessed against the security threats. • Systematic highlighting of possible threats from migrants using existing threat indicators. • System and process measures and performance indicators to assess screening effectiveness and responsiveness. • Agile and adaptable systems and processes, a change in threat criteria can be completed using business logic not requiring coded change. • s6(c), s6(a) [redacted]

Released under the Official Information Act 1982

2. Document Control

Version history

Date	Version	Author	Description of change
07 November 2019	0.1	s9(2)(a)	Create first draft
09 April 2020	0.2	s9(2)(a)	Revised draft incorporating reset of scope
21 May 2020	0.3	s9(2)(a)	Revised to incorporate feedback from Design Authority. Updated incorrect URL link. Revision/clarification of purpose and problem in description, executive summary. Update to problem statement reflecting border reopening in Sec 3 Strategic Context. Clarification of scope items in Sec 4 Detailed scope and 7 product descriptions. Updates to InRule licencing and platform costs in Financial Summary and Appendix A.

Table of Contents

Released under the Official Information Act 1982

Released under the Official Information Act 1982

Released under the Official Information Act 1982

MINISTRY OF BUSINESS,
INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

IN-CONFIDENCE

Immigration National Security Screening

Business Case
Medium Complexity

New Zealand Government

Released under the Official Information Act 1982

3. Strategic Case (Case for Change)

Strategic Context

INZ has the statutory requirement that no visa is granted or waiver applied where a person is a likely threat to National Security[1].

The Striking the Balance strategy seeks to identify and manage risk early and ensure the immigration system operates seamlessly as an effective regulator. The Immigration New Zealand (INZ) National Security (INSS) project has the joint objective with the NZSIS "that as trusted stewards of the immigration system, we work with our partners to protect New Zealand's National Security".

The Immigration National Security Screening Project (INSS) is re-engineering the end to end National Security screening function for INZ. This re-engineering will support a rapidly adaptable approach to change in the immigration system including initiatives such as the Smart Border.

The INSS project will:

- Re-engineer Immigration National Security Screening to identify risk early and minimise the number of high-risk migrants entering New Zealand.
- Improve the efficiency and effectiveness of threat assessments and treatments supporting more seamless desirable migration.
- Improve compliance with Section 16 and Section 4 of the Immigration Act 2009.

Problem Scope

Immigration National Security screening underpins the statutory requirement that no visa is granted or waiver applied for anyone likely to be a threat around[2]:

- Defence of NZ
- Espionage, sabotage and subversion
- Adverse impact on NZ well-being, reputation, or economic well-being.
- Terrorist acts
- Organised (transnational) crime
- Safety and stability of InterNational Security conventions and arrangements.

s6(c) [redacted] The security priorities of NZs intelligence community has been revised recently. s6(c), s6(a) [redacted]

- [redacted]
- [redacted]
- [redacted]

Inefficiencies in process and systems:

Released under the Official Information Act 1982

[1] S16, Immigration Act 2009

[2] Immigration Act 2009, Sect 4 and 16

- Extend visa processing times.
- Lead to security checks being started on applicants highly likely to be denied quickly for other reasons such as health or financial viability.
- Key information isn't verified early, requiring downstream rework and verification.
- s6(c) [redacted]
- s6(a) [redacted]

Expected Impacts from the border reopening

- INZ and government COVID recovery planning for economic recovery and a full re-opening of the border (in restarting or quota) is underway. This includes assessing the new risk landscape.
- Re-opening will require responsive, agile system to identify and manage risks early and to advise decision makers at all levels.

Strategic Alignment

Strategic Theme	Strategic Response
We minimise the number of high-risk migrants entering New Zealand	All migrants that pose a potential National Security threat are assessed. Only those that present a credible risk to New Zealand are prevented from entering the country.
Identify Risk Early	Security threat and treatment information is directed to the right people at INZ or NZSIS to enable action to be taken at the earliest possible time. The system learns from itself and informs future changes/improvements. Agile systems and processes are continuously refined and consistently improved. The assessment and treatment of National Security threats are reviewed regularly and adapted to the global threat landscape. National Security threats are aligned with INZ risk model
INZ functions as one cohesive team	Shared understanding between agencies and within INZ of security threats and approach to treat them. Roles and responsibilities between agencies and within INZ are clearly defined. Staff operating within the system are adequately trained on roles and responsibilities Operational culture supports staff to make confident decisions and take timely action

Released under the Official Information Act 1982

[redacted]

s 6 (c)

Released under the Official Information Act 1982

Benefit #	Type	Benefit Title	Benefit Description	Baseline	Target
Ben01	Reduced risk	Reduced risk of non-compliance with IA09 s16. No Visa is granted or waiver applied if the person is, or is likely to be a threat to National Security.	s6(a) [redacted].	s6(a) [redacted]	s6(a) [redacted] s6(a) [redacted]
Ben02	Reduced risk	Reduced likelihood of harm from new undetected National Security threats.	Screening coverage adapts quickly to changes in threat levels and new threats.	s6(c) [redacted]	s6(c) [redacted]
Ben03	Reduced risk	Increased number of security threats treated offshore.	s6(a) [redacted]	s6(c) [redacted] There may be other threats that are not detected.	95% reduction in reactive treatment.
Ben04	Improved Responsiveness	Faster identification of threats and completion of screening assessments.	Faster more streamlined National Security screening checks within visa processing.	s6(c) [redacted]	Improvement measured and speed improvement identified via survey. After baseline established objective measures and performance improvement plans are tracked.

Benefit Realisation

Benefit owners have been identified and benefit realisation plans for the benefits above will be drafted after the business case is approved.

Released under the Official Information Act 1982

4. Economic Case

The primary objectives of the INSS project are to effectively manage risk and improve legislative compliance.

The economic case is an assessment on the best value for money to achieve these outcomes.

As part of the development of this business case four areas were focused on for recommendations to be made. The areas are:

- National Security risk model including threat criteria and control framework.
- Improvements to processes, supporting consistency, adaptability and continuous improvement.
- Systems infrastructure and supporting analytical capabilities.
- Training needs and instructions.

Critical Success Factors (CSFs)[3]

Critical Success Factors that describe what the recommended option is to achieve for Immigration NZ are:

#	Description
CSF01	Alignment with Legislation
CSF02	Focused on long term goals working within the capacity of both agencies
CSF03	Maintains public perception within NZ and confidence for partners in NZ
CSF04	Coverage of security threats
CSF05	Feasibility, usability, operability
CSF06	Strategic alignment with objectives of both agencies

Released under the Official Information Act 1982

[3] *CSFs are not necessarily measurable like KPIs or Benefits.*

Summary of Options Analysis

Parameter	Option 1 – do nothing	Option 2 – Single stage with minimum scope	Option 3 – Staged approach focused scope	Option 4 – More ambitious all scope delivered as fast as possible
Summary	No change delivered.	All change delivered in a single drop. Do the minimum change to meet current global threat level?	Change phased in over four stages.	Change phased, but more use of parallel delivery to speed introduction.
Assessment against CSFs	Absent. Unable to address any of the CSFs.	Poor. Meets CSF01 and CS04. Does not deliver CSF02, CSF03, CSF05 or CSF06.	Excellent. Meets all CSFs.	Moderate. Meets CSF01, CSF04, CSF06. May meet CSF03. May not meet CSF02. Does not meet CSF05.
Assessment against benefits	No benefits delivered.	Benefits delivered, Less Ben04 compared to Option 3.	Benefits delivered, with ability to adapt as needed during delivery.	Benefits delivered.
Long run costs	Overall cost high.	Overall cost moderate.	Lowest overall cost.	Highest cost option. May deliver high cost changes with limited additional benefit.
Implementation capacity	NA. No implementation	Lowest capacity for effective implementation as systems, processes, training and people	Moderate. A significant amount of change will be delivered, but it will be staged and manageable.	Moderate. Change would be developed in parallel, which would likely impact adversely on current state activity while increasing risk on future state delivery.
Delivery risk	NA. No implementation.	High. A single drop of all change at once is riskier it is unlikely all changes will be understood upfront.	Low. Least impact on ability to manage migrant risk while building, developing, testing and implementing change. Staged approach allows time and space to test and adjust changes before they are delivered.	Moderate. Parallel delivery requires several changes to be delivered at the same time, increasing risk over the staged approach, while being lower risk than the single stage approach.

Released under the Official Information Act 1982

Parameter	Option 1 – do nothing	Option 2 – Single stage with minimum scope	Option 3 – Staged approach focused scope	Option 4 – More ambitious all scope delivered as fast as possible
Change scale (People, process, tech. policies)	NA. Nothing is delivered.	High. Multiple changes to people, process, technology and policies delivered at the same time.	Moderate. A significant amount of change will be delivered, but it will be staged and manageable.	Moderate to high. Parallel changes will be difficult for teams to absorb effectively.

Recommended Option: Option 3

Option 3 is the preferred option as it delivers the best outcome New Zealand while minimising impact on INZ and partner agencies.

Short-listed options not recommended

Option(s) not selected for recommendation	Reason why not selected for recommendation
Do Nothing	s6(a) [redacted]
Upfront Single refresh	Higher risk option that significantly impacts INZ's people and technology. Requires major changes to be made at one time. Difficult to deliver effective improvement while still assessing and treating migrant threat. Significant learning and development demand on staff.

Details of options explored and excluded in the shortlist considerations are included in Appendix E

Released under the Official Information Act 1982

Summary of the Preferred Option

The preferred solution involves 4 key components these are delivered over 4 stages.

- National Security threats aligned with the INZ risk model supporting:
  - Consistent and well understood threat criteria and control framework.
  - Provide clarity on processes and responsibilities aligned with other immigration functions.
- Structured process improvements to consistently review and adapt threats and controls
- System enhancements and integration supporting a consistent screening process providing tracking and analytic functions ensuring the right information reaches the right place at the right time including the NZSIS.
- Learning and development materials to assist in building and maintaining a connection to the purpose of National Security Screening for all involved staff across INZ.

Risk Model

Some migrants present a threat to the National Security of New Zealand, as outlined in the *Problem Scope* on page 12 (above). The INZ risk model will address these threats through:

- Processes used to assess and treat National Security threats will be improved to be clearer, more consistent and aligned with the INZ risk model.
- The effectiveness of National Security threat assessments and treatments will be measured against key performance indicators. These assessments and treatments will be adapted and utilise intelligence on global threats impacting New Zealand and New Zealanders.
- Processes used to treat National Security threats will be better aligned into other immigration functions.

System enhancements and Integration (Technology)

s6(a), s6(c)

Released under the Official Information Act 1982

Learning and Development

Learning and development materials will assist in building the connection to the purpose of National Security Screening for all staff working with migrant security assessments.

A successful solution should involve delivery of learning materials that are aligned to the risk model. It should build maturity of knowledge and understanding of the end-to-end National Security Screening Process at Immigration New Zealand, including clarity of roles and responsibilities, knowledge on what is required for screening and build skills for specific areas.

Released under the Official Information Act 1982

Staging

	Outcomes and Benefits	Scope Items and Exclusions	Costs and Risks
Stage One	This will set the foundations of a robust, adaptable and consistent National Security screening system (i.e. end-to-end process), that enables the risks to be tracked, measured and controlled effectively: This is expected to capture information from all migrants consistently with minimal disruption while providing analytics to assess the impacts in changing a security threat response. Outcomes in Stage One include: • Clear guidance to assess on security threats made available to all relevant staff. • s6(a) • s6(a) • System and process measures and performance indicators to assess screening effectiveness and responsiveness. • Agile and adaptable systems and processes, a change in threat criteria can be completed using business logic not requiring coded change. • s6(a) Benefits expected include: • Screening coverage and quality can be measured and assessed. • Reduced likelihood of threats arriving onshore. • System is responsive to changes, able to adapt to most changes within days. • Improved responsiveness through clarity, identifying threats early.	Scoped changes for Stage One include: • National Security Learning modules • Online guides, with in context help. • INZ instructions and SOPs reference consistent security instructions and risk indicators. • Processes to assess risks aligned with INZ's risk model • Operationalise National Security requirements currently in legislation • Security threats highlighted systematically based on threat indicators. • Screening action taken logged systematically. • s6(a) • Performance reporting used to assess the effectiveness and responsiveness of screening. Out of scope items for Stage One: • Changes to threat indicators and existing instructions (These will be delivered in stages 2 and 3) • Policy changes (stages 2 and 3). • Automation of data captured from migrants (stage 2). • s6(a) • Changes in responsibilities/risk treatment actions between agencies (stage 3).	Expected cost accuracy for Stage One is good as: • Uses MBIE frameworks for process improvements which were tested during project discovery. • Similar system changes have been made that can be reused. • Vendor estimates have been provided. • No new products are required. Identified risks in Stage One: • COVID-19 coronavirus may impact access to vendors/partners, leadership and project / BAU teams working together. These impacts can be managed by the project team and Steering group...

Released under the Official Information Act 1982

	Outcomes and Benefits	Scope Items and Exclusions	Costs and Risks
Stage Two	Stage 2 will automate more of the process and capture information more information and in digital form. Adjustments to instructions and rules will be made so efficiencies can be achieved using new analytical insights. Outcomes in Stage 2 include: • s6(a) • Security threat information and actions are directed to relevant staff/specialists more quickly using automation. • More in depth and accurate tracking of screening actions supporting assurance and continuous improvement. s6(c) • System usability is improved. • Screening treatments improved using capabilities delivered in stage 1. Benefits expected include: • Responsiveness improvement on Stage 1 through s6(c) and quality of information. • Reduced likelihood of threats onshore than Stage 1 through capturing better quality migrant information. • Improved responsiveness to change over stage 1 through improved reporting and forecasting.	In scope items for Stage Two are: • Digital form with rules for migrant to provide screening information online. • s6(c) digital form for staff to request information relevant to screening needed from migrants applying for Visas offline. • s6(a) . • Screening assessment actions tracked and exceptions highlighted systematically. Specific actions tracked and reported in more depth than Stage 1. • s6(a) • Status updates shared automatically between visa processes completed in parallel with security screening. • Revisions to threat indicators to reduce risk where a reduced overall level of migrants with screening actions Out of scope items for Stage Two are: • Changes to threat indicators and instructions where operational impacts cannot be forecast (stage 3). • Legislation changes. These are not expected to be required. • Changes in responsibilities/risk treatment actions between agencies (stage 3).	Expected cost accuracy for Stage Two is lower than Stage One as: • New products will be delivered, but will use the same approach as other projects including ADA and EAWV. • Cost estimates can be reforecast after ADA has finalised products and partners. • Vendor estimates have been provided. A reduction is as likely as an increase. Identified risks in Stage Two: • Risk level is greater than stage 1 but more time is available to address and reduce risk. • Processes and collection of new information from migrants should be reviewed with steering group, Legal specialists and Op Policy. • More dependency/involvement of the NZSIS to collect and share within their process.
Stage Three	Stage 3 will see adjustments to treatments to meet current security threat levels and better align actions to assess and treat threats between agencies. s6(c) will be included and all threats in the process will be tracked against the established KPIs Outcomes in Stage 3 include: • s6(a) • More effective targeting of threat assessments using analytical capabilities and intelligence delivered in Stages 1 and 2. Benefits expected include: • Screening responsiveness improved over stages 1 and 2 via improved information sharing with NZSIS. • Screening coverage and quality improvements over stages 1 and 2 through a more effective working relationship with NZSIS. • s6(a) • Screening coverage and quality improvements using analytical capabilities and intelligence from stages 1 and 2.	In scope items for Stage Three are: • s6(a) • Revised threat treatments to reduce threat levels within the capacity of both agencies.	Expected cost accuracy for Stage Two is less accurate than Stages 1 and 2 but there is time to adjust and improve: • Estimates are indicative and not supported by a supplier yet. • NZSIS work is assumed out of scope (completed by NZSIS) but interfacing with this is higher risk. • Resourcing impacts in changing threat treatments are difficult to forecast reliably. • Changes made in stages 1 and 2 will improve the accuracy. Identified risks in Stage Three: • Greater than Stages 1 and 2 but more time to reduce them. • Dependency on NZSIS to support changes. • Forecasting time involved on legal agreements, direct access agreements and security arrangements are less reliable to forecast.

Released under the Official Information Act 1982

	Outcomes and Benefits	Scope Items and Exclusions	Costs and Risks
Stage Four	Stage 4 will make minor targeted process improvements and test readiness for the assessments to be operationalised through BAU. The risk process and adjustments can be tested holistically, including the threshold for changes. After this stage change will be ready to be managed through BAU (low enough threshold do not require a new project) Outcomes in Stage 4 include: • s6(c) • s6(c) • Targeted improvements in screening effectiveness and efficiency can be delivered as a business as usual process. • Decommission old NSC systems. Benefits expected include: • s6(c) and quality from earlier stages. • Screening coverage and quality improvements using analytical capabilities and intelligence from stages 1, 2 and 3.	In scope items for Stage Four are: • s6(c) (SC21) • s6(c) • Process handover into BAU is effective. (SC22) • Decommission old NSC systems. (SC22)	Expected cost accuracy for Stage Four is more accurate than stage 3: • Costs of interfaces have been achieved recently with RAP. • s6(c) • The depth of use will be better understood after earlier stages are progressed further. Identified risks in Stage Four: • Less than stages 2 and 3 but require some of the changes delivered through these earlier stages. • Less likely to deliver benefits than changes in other stages.

Released under the Official Information Act 1982

High Level Requirements

High level requirement (Table is a summary of the requirements shown in Appendix F)
s6(a) . Staff from INZ and NZSIS will provide specialist threat assessment direction for each of the identified threats, with the lead specialists at: • s6(a) This collaborative approach will support consistency of threat assessment and treatment. After deeper assessments have been conducted, unclassified plain language advice will be provided back to Immigration Officers to support good decision making.
Migrants will able to apply for visas and NZeTAs online. They may also be asked to provide focussed supplemental information at or after time of initial application. This will support earlier and more comprehensive security reviews. s6(c), s6(a)
Traceability of INSS systems and processes to the Immigration Act 2009 will be maintained. The traceability hierarchy is: • Legislation and regulations (primarily IA09 and IAS17, plus other Acts as appropriate) • MBIE / INZ operating policies • MBIE / INZ Standard operating procedures (SOPs) and Risk Indicator Guides (RIGs) Traceability will be formally reviewed periodically (initial proposed setting is annually) to ensure compliance with this requirement is maintained. s6(a)
[redacted]
Staff will be provided with training at on boarding and receive ongoing learning and development opportunities appropriate to their needs, to build knowledge and ensure National Security screening objectives can be effectively met.
To support INSS effectiveness, agreed KPIs will be introduced to measure threat assessment and treatment outcomes and the impact of any change on screening treatments.
Enhancements to existing assurance tools to ensure migrant assessments are consistently applied across the immigration system.
A systematic approach to support the introduction of new assessment and treatment capability allowing prompt response to new threats or changes in threat levels.

Released under the Official Information Act 1982

Detailed Scope

The scope of the work required falls into four areas: People and Training; Process; Technology, Agreements/collaboration arrangements.

People and Training		
#	In Scope	Out of scope
SC1	Develop learning modules providing an overview and introduction to National Security screening at INZ, and made available for ongoing refresher training.	
SC2	Amend Visa SOPs to consistently reference National Security screening instructions.	Changes to legislation or policy Note: Legislation and instructions are broad so don't require legislation or ministerial approval to enact process change
SC3	Consolidate NSC Instructions and SOPS to a single set of SOPS linked to codified Risk Indicator Guides	Changes to legislation or policy Note: Legislation and instructions are broad so don't require legislation or ministerial approval to enact process change
SC4	Make online guides providing in context information available to staff involved in screening migrants.	
SC5	Operationalise National Security requirements currently in legislation	
Process		
SC6	Implement framework to quantify, evaluate and prioritise the treatment of security threats aligned with the INZ Risk framework.	Prioritisation of National Security threats (these are set by DPMC)
SC7	Make templated responses available to staff to notify migrants of screening decisions and their rights when refused a visa or entry into NZ.	
SC8	Implement changes to adapt National Security assessments and treatments to changes in threat levels/new threats.	
SC9	Clarify how exceptions and escalations are made for staff treating migrants that are a potential threat to National Security.	
SC10	Design and implement approach to audit, track and review performance indicators used to assess the effectiveness of National Security threat screening.	
Technology		

Released under the Official Information Act 1982

SC11	Implement system rules to detect threat indicators in migrant Visa applications and identify required screening actions for staff to complete.	
SC12	Track updates to the screening and Visa application status and automate the communication of changes.	
SC13	Measure and report the performance of screening steps and volumes of migrants processed with potential threat indicators to inform future improvements, forecast impacts of change.	
SC14	s6(a), s6(c) [redacted]	s6(c), s6(a) [redacted]
SC15	s6(c) [redacted] the capture of additional data from migrants where there are gaps in information provided in migrant applications.	
SC16	Make digital forms available for INZ staff to submit and capture additional information from migrants where there are gaps in information provided in physical applications.	
SC17	AMS changes to prevent Visas being issued when screening is in progress.	
SC18	s6(a), s6(c) [redacted]	
SC19	s6(a) [redacted]	s6(a) [redacted] .
SC20	s6(a), s6(c) [redacted]	
SC21	s6(a), s6(c) [redacted]	
SC22	Decommission old NSC systems.	
Collaboration arrangements		
SC23	Revisions to INZ/NZSIS direct access agreements to include new systems and information sources.	

Released under the Official Information Act 1982

5. Procurement / Commercial Performance

Following consultation with ICT Commercial it has been determined that a Procurement Plan is required for this project.

The selection of the technology solution followed MBIE's formal architectural options analysis process. The recommendations were considered and approved by the MBIE Architectural Review Board (ARB). The commercial case thus covers the selection of a suitable supplier who is capable of licensing the appropriate technology and providing any/all professional services required for the solution implementation and support.

Products and/or Services required to deliver the recommended option

- **Technology & Licensing** – this will include the identification, procurement, and contractual licensing of a suitable technology/product to deliver the core capabilities.
- **Integration and Implementation Services** – this will include the specialist skills required to complete the detailed design through to implementation of the solution (including the configuration, integration, testing, and implementation of the technology to support prioritised business processes)
- **Hosting and deployment services** - Hosting and deployment services used to store data used and deploy changes to the environments.
- **Ongoing Support** – this will include a support contract to ensure access to suitable resources for the maintenance of the technology and our context-specific integration and configurations.

Approach

The project has complied with the MBIE Sourcing and Contract Policy,

s 6 (a) [redacted]

Negotiated Deal

No products or services have been agreed at this time as funding has not been secured.

Recommended Supplier(s)

Contracts will be established with suppliers for the following services in Stage 1.

- s9(2)(j) [redacted]

Released under the Official Information Act 1982

- s9(2)(j) [redacted]

Stage 2 Changes

Joint ADA and EAWVP teams have identified multiple viable products and associated supplier partners in the market with sufficient maturity to deliver the kind of capabilities required for INSS.

- The implementation of the project scope will require the procurement of a technology (product) and specialist professional services to support the installation, integration/configuration, and ongoing support of that technology.
- ADA and EAWV are expected to negotiate master services agreements with a chosen vendor.
- There is efficiency and synergy gained working with other projects who are introducing the same technologies.
- A SOW for INSS specific changes will be linked to the master services agreements once these are selected.

MBIE Sourcing

ICT will be engaged to provide hosting and deployment services through existing MBIE ICT processes.

Architecture, Security Architecture, Technical Business Analysts, Data specialists, Testing Specialists will also be requested from MBIE ICT.

Vendor Management

Formal arrangements will be in place to successfully manage the contract once commercials are complete. An MBIE contract manager will manage the relationship with the recommended supplier(s) over the term of the contract.

A nominated delivery lead for each vendor delivering a service the relationship with the project team will be managed by the INSS Project manager.

Next Steps

s9(2)(j) [redacted]

A further update to the commercial activity for stage 2 products will be provided after ADA and EAW have selected vendors.

Released under the Official Information Act 1982

6. Financial Summary

Summary of capital and operational costs including out years							
	Current FY 19/20	FY 20/21	FY 21/22	FY 22/23	FY 23/24	FY 24/25	**Total**
Total project delivery capex expenditure	47,062	2,778,186	353,072	9(2)(j) [redacted]	[redacted]	[redacted]	[redacted]
Total project delivery opex expenditure	-	10,000	35,000	[redacted]	[redacted]	[redacted]	[redacted]
Estimated on-going business opex (excluding depreciation)	-	-	-	[redacted]	[redacted]	[redacted]	[redacted]
Estimated on-going ICT opex (excluding depreciation)	-	-	193,888	[redacted]	[redacted]	[redacted]	[redacted]
Whole of Life costs (capex + opex + on-going costs[4])	47,062	2,788,186	581,960	[redacted]	[redacted]	[redacted]	[redacted]
Net cash flow (Benefits less Total Costs)	-47,062	-2,788,186	-581,960	[redacted]	[redacted]	[redacted]	[redacted]
Depreciation			403,607	[redacted]	[redacted]	[redacted]	[redacted]

Tolerance

The following tolerance levels have been agreed by the Project Sponsor:

Time	3 weeks	21 days
Cost	5%	$150,000

Released under the Official Information Act 1982

Contingency

The following Contingency has been agreed for this project:

Contingency has been set by MBIE Finance in a memo dated 27 October 2016. The memo set out that:

- A standard approach to contingency be applied across MBIE projects where contingency will not be approved as part of upfront funding as the portfolio boards need to focus on mitigating risks during the life of the project.
- Portfolio Boards will assess the level of contingency to ensure they are appropriate for the scale, complexity and uncertainty related to the project based on the Risk Adjustment Cost (RAC).

A Change Request will be raised to the appropriate governance board to draw down on the contingency if required.

Cost assumptions and constraints

The following are the cost assumptions for this Project:

Cost Assumption(s)	Comments
Ongoing costs ICT	Supplier provided licencing and hosting costs assume test and simulation environments. Shared products and ongoing licencing costs with ADA on workflow, rules and forms.
Ongoing costs Business	No additional resources have been costed and it is assumed that screening changes can be achieved using existing capacity.
Other cost related notes	No provision has been made for: • Technology support costs these will involve shared technologies and suppliers of workflow, rules and forms engines.
Depreciation and Capital Charge	Depreciation of Assets are based on 7 year useful lifecycle

Released under the Official Information Act 1982

7. Delivery Approach

This project will follow the Immigration NZ Project Governance Framework.

A link to the framework is below:

s 6 (a) [redacted]

Decisions outside of tolerance will be made by the Business Reference Group and Business Change Board.

ICT governance processes will be followed for any technology deliverables.

This describes how the recommended option will be successfully delivered. This section outlines the detailed plan/work breakdown structure, the schedule/timeline, dependencies, resources, risks, assumptions, constraints, and the change management approach for the manage and close stages of the project.

Delivery Approach

Due to a lack of consistent review of the end-to-end Security Screening process, significant change and uncertainty exists. The INS project will deliver change through a staged approach, making incremental change over 4 stages to ensure the final re-engineered process is fit for purpose.

The first stage is expected to capture information, s6(a) [redacted] Processes and systems will be streamlined to improve their agility and adaptability, this supports changes implemented in later stages of the project and then BAU. Improved Analytic capability will be introduced to improve the assessment and forecasting of impacts that may result from a change to security threat response.

Stage 2 will automate more of the process and capture information more information and in digital form. Adjustments to instructions and rules will be made so efficiencies can be achieved using new analytical insights.

Stage 3 will see adjustments to treatments to meet current security threat levels and better align actions to assess and treat threats between agencies. Further enhancements in automation will be included and all threats in the process will be tracked against the established KPIs.

Stage 4 will make minor targeted process improvements and test readiness for the assessments to be operationalised through BAU. The risk process and adjustments can be tested holistically, including the threshold for changes. After this stage change will be ready to be managed through BAU (low enough threshold do not require a new project).

Product Descriptions (Deliverables)

Further feedback is needed from NZSIS on sequencing and impacts in their environment this is not expected to impact stage 1.

Title	Description of Scope Item / Major Deliverable	Date to be delivered by
SC1	Develop learning modules providing an overview and introduction to National Security screening at INZ, and made available for ongoing refresher training.	30 November 2020
SC2	Amend Visa SOPs to consistently reference National Security screening instructions.	30 November 2020

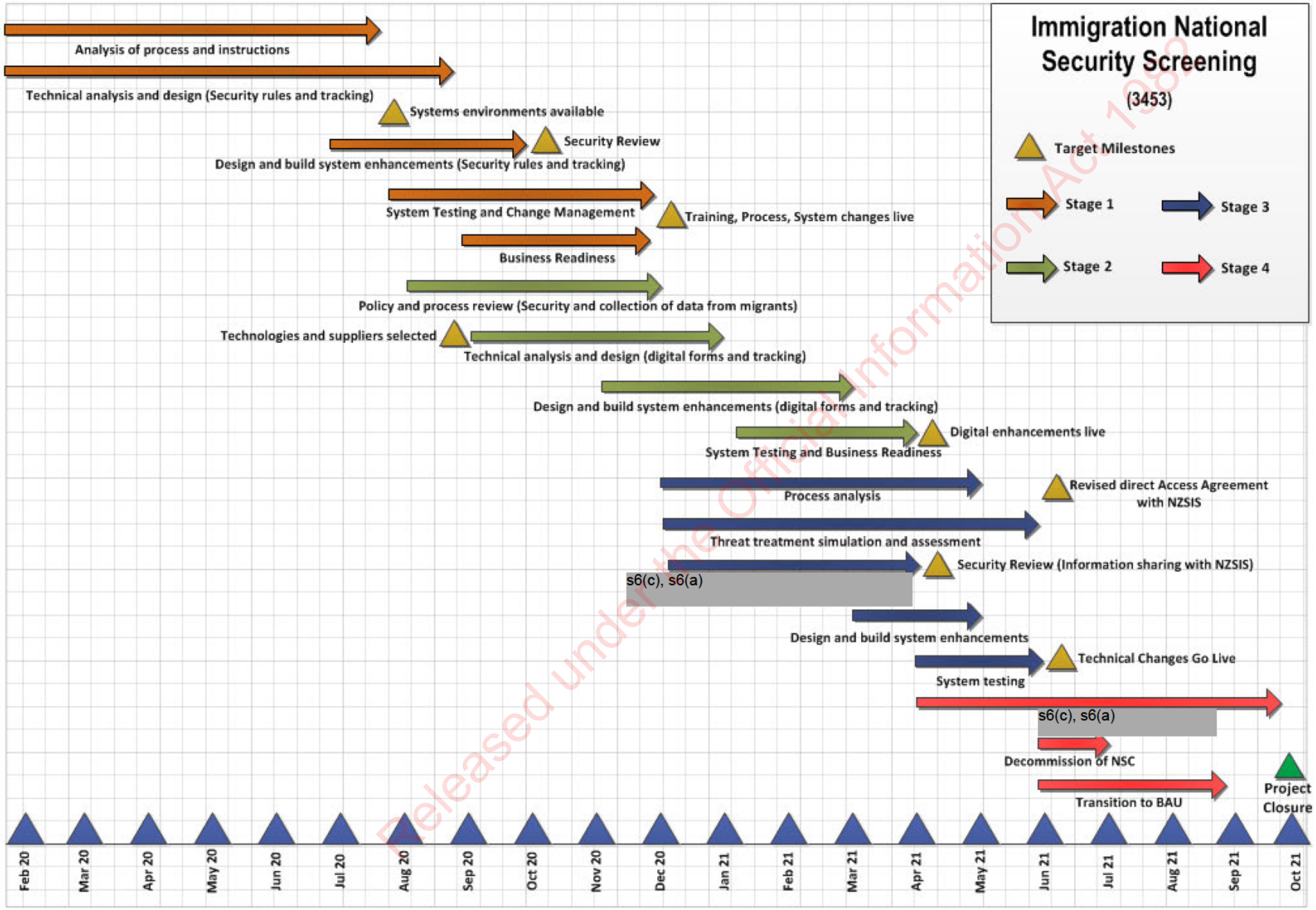
Released under the Official Information Act 1982

Title	Description of Scope Item / Major Deliverable	Date to be delivered by
SC3	Consolidate NSC Instructions and SOPS to a single set of SOPS linked to codified risk indicators.	30 Nov 2020
SC4	Make online guides providing in context information available to staff involved in screening migrants.	30 Nov 2020
SC5	Operationalise National Security requirements currently in legislation.	30 Nov 2020
SC6	Implement framework to quantify, evaluate and prioritise the treatment of security threats aligned with the INZ Risk framework.	30 Nov 2020
SC7	Make templated responses available to staff to notify migrants of screening decisions and their rights when refused a visa or entry into NZ.	30 Nov 2020
SC8	Implement changes to adapt National Security assessments and treatments to changes in threat levels/new threats.	31 May 2021
SC9	Clarify how exceptions and escalations are made for staff treating migrants that are a potential threat to National Security	31 March 2021
SC10	Design and implement approach to audit, track and review performance indicators used to assess the effectiveness of National Security threat screening.	30 Nov 2020
SC11	Implement system rules to detect threat indicators in migrant Visa applications and identify required screening actions for staff to complete.	30 Nov 2020
SC12	Track updates to screening and Visa application status and automate the communication of changes.	31 March 2021
SC13	Measure and report the performance of screening steps and volumes of migrants processed with potential threat indicators that inform future improvements and forecast impacts from proposed changes.	31 March 2021
SC14	s6(a), s6(c) [redacted]	30 Nov 2020
SC15	Implement digital forms to automate the capture of data from migrants where there are gaps in information provided in their applications.	31 March 2021
SC16	Make digital forms available for INZ staff to request information from migrants where there are gaps in information provided in their physical application forms.	31 March 2021
SC17	AMS changes to prevent Visas being issued when screening is in progress.	31 March 2021
SC18	s6(a), s6(c) [redacted]	31 May 2021
SC19	s6(a) [redacted]	31 May 2021
SC20	s6(a), s6(c) [redacted]	30 Sep 2021
SC21	s6(a), s6(c) [redacted]	30 Sep 2021
SC22	Decommission old NSC systems.	30 Sep 2021
SC23	Revisions to INZ/NZSIS direct access agreements to include new systems and information sources.	31 May 2021

Released under the Official Information Act 1982

Timeline and Key Milestones

An indicative timeline for all stages is included below. Timelines for stages 2-4 are based on effort estimates and key dependencies a further validation of timeline assumptions are needed for these stages.



Released under the Official Information Act 1982

Assumptions

#	Assumption	Impact if Assumption does not hold	Validated by	Validation date	Notes
AS01	s6(a)	[redacted]	NZSIS	Stage 3	s6(a) [redacted] [redacted]
AS02	s6(a)	s6(a)	Part A solution design	Stage 3	s6(a)
AS03	The direct access agreement to share data with NZSIS will be revised.	INZ exposes itself to reputation risk	Security Architect	Stage 3	Project will need to obtain an approval at Cabinet Minister level noting supporting legislation is already in place. This is covered by NZISM to the restricted level. Details are at: NZISM section 2.3 s 6 (a)

Released under the Official Information Act 1982

#	Assumption	Impact if Assumption does not hold	Validated by	Validation date	Notes
AS04	Operational efforts saved through efficiency can be balanced by increased effort in treating threats or other immigration risks. Effort is focused where the threat is greatest.	Additional operational resourcing to manage backlog or discussion with branches to reduce costs through reduction of staff where activities are reduced is completed separately		Stage 3	Currently there is limited ability to estimate efficiency gains and the operational impacts from changing screening actions to treat the threats. Improvements in forecasting will be introduced early and decisions to change resourcing levels made later if required.
AS05	Sizing for changes to move screening logic from AMS is similar in scale to a similar implementation as part of the Triage project.	Increase in cost	s9(2)(j)	[redacted]	s9(2)(j) This has been reviewed and the effort is expected to be lower.
AS06	The Risk Analytics Platform will be used to provide data modelling capability to inform rules. RAP will provide the standards for modelling and a platform for analytics.	A smaller range of datasets will be available to analyse data patterns to assess rules and threats.	Project Brief	Stage 4	Use of RAP is optional and included in the 4th stage enabling time for the project to establish model standards and capabilities.
AS07	Automated Decision Assist (ADA) will provide a new forms product to capture data from migrants that will be assessed for National Security threats.	Increased timeline and operating costs using different technologies	Project Brief	Stage 2	Design estimates are based on using separate tools. Review of ADA requirements of Vendors will highlight if the product fits the needs of both projects.

Released under the Official Information Act 1982

#	Assumption	Impact if Assumption does not hold	Validated by	Validation date	Notes
AS08	s6(a)	s6(a)		Stage 3	A consistent risk model will be used to assess threat levels, treatments controls and improvements. The duration of effort for each is likely to average out to a similar level but involve different threat specialists. Efficiencies are expected addressing several threats in parallel.
AS09	s9(2)(j)	s9(2)(j)		Stage 2	s6(a) This is covered in the NZISM section 2.3: s 6 (a) The direct access agreement between NZSIS and INZ will be updated.
AS10	Lead times to engage ICT resources are less than 3 months duration	Timeline delays.		Stage 1	This may be reduced by using Vendors and staff moving off other projects that have been placed on hold.
AS11	Threat criteria will be developed working with partner agencies using DPMC methodologies.	INSS threat criteria will not align with National Security and Intelligence Priorities		Stage 1	These methodologies were employed to identify the first priority risk indicators

Released under the Official Information Act 1982

Constraints

#	Constraint	Impact	Validated by	Validation date	Notes
Con01	s6(a), s6(c) [redacted]	[redacted]	Data scientist in RAP	Stage 4	Data modelling using statistics to measure likelihood of a risk requires data examples to prove the risk is more than coincidence
Con02	[redacted]	[redacted]	The Service	Stage 3	s6(c), s6(a) [redacted]

Released under the Official Information Act 1982

Interdependencies and Project Relationships

#	Description the dependency	Name of project dependent on	Dependency In or Out?	Milestone impacted	Impact Assessment	Date required to be delivered
Dep01	ADA choice of tooling for data capture capability and workflow	2974 – Automated Visa Approval	In	Stage 2	Triggers for automated workflow processes (sequencing) to enable our design options. May leverage online forms technology for data capture improving data quality and targeting.	30 June 2020
Dep02	Service improvements to National Security Screening	The Service	Both	Stage 3 Aligned treatment	Advice on current threat/ context for immigration National Security. s6(a) [redacted] [redacted]	Stages 2&3

Released under the Official Information Act 1982

Tolerances

The table below lists the permissible deviations from the project targets than can be managed without raising a Change Request.

Project level tolerances

Time and Cost project tolerances comply with the MBIE standard. Zero Scope Tolerance is the INZ standard and by default also includes Benefits. Risk and Quality Tolerances have been agreed with the Business Owner.

The Project Manager will inform the Business Owner and Project Sponsor as soon as it becomes apparent that tolerance will be used. Where it is forecast that there will be a deviation beyond the agreed tolerance level a Change Request will be raised. A Change Request is not required where a project delivers ahead of schedule.

Tolerance criteria	Description	Tolerance Settings default
Time[1]	+/- time on target completion date	3 weeks over the agreed target completion date
Cost	+/- amount of approved budget	5% over budget or $150k whichever is the less
Scope	permitted variation of the scope of a solution	Zero: All "Must have" (MVS) requirements met
Risk	limit on the aggregate value of threats; limit on any individual threat	All RED risks to have treatment plans
Quality	target range, set at the product level	No show stoppers
Benefits	target benefits defined as a range	All Must have and Should Have Requirements met

Delivery Assurance Plan

- The INSS project will follow the Immigration NZ Project Governance Framework.

A link to the framework is below

s 6 (a)

- Decisions outside of tolerance will be made by the Business Reference Group and Business Change Board.
- ICT governance processes will be followed for all technology deliverables.

Released under the Official Information Act 1982

[1] 3 weeks slippage applies to the project completion date. For a large project, 3 week slippage for a milestone may be absorbed and recovered and may not impact the overall end date.

Exception and Change Control process

Upon approval of this business case, the project plan will be baselined, after which all project changes will come under formal change management. A Project Change Request will be raised for any proposed changes to scope, schedule and/or financials and approval sought from INZ governance for the changes.

In addition, the following project reporting and assurance activities will be carried out:

Assurance[5] activities	Mandatory/Optional/ Recommended	Frequency -
Business owner meetings	Mandatory	Weekly
Project status reporting for the business owner	Mandatory	Weekly
INZ Change Portfolio status reporting in Project server for INZ governance (report can be used for the business owner)	Mandatory	Weekly
Interagency Project Steering group meetings	Optional	Monthly and as required to review key deliverables/decisions
MBIE Privacy Threshold Assessment (PTA)	Mandatory	One-off assessment.
Privacy Impact Assessment	Required by PTA	Assessment in initiate phase with review when the design is endorsed.
INZ Change portfolio related project collaboration session	Optional	Fortnightly
Project Risk Assessments using the MBIE standard	Mandatory	Throughout the project lifecycle
Compliance with INZ Change Portfolio Project Management framework, processes, governance and quality assurance	Mandatory	Throughout the project lifecycle
Compliance with INZ Change Portfolio project health checks, including Benefits checks	Mandatory	As required, throughout the project lifecycle
Compliance with INZ Business Change and Integration processes	Mandatory	As required, throughout the project lifecycle
Business Acceptance	Optional	Through interagency working group and steering as required /on milestone deliverables
External Assurance activities (as required)	Optional	Independent Quality Assurance review as mandated

Released under the Official Information Act 1982

[5] INZ projects are selected at random for external assurance reviews.

Project Governance and Team Structure

Roles and Responsibilities

A working group of senior users will input into all deliverables and review for quality. Roles and responsibilities for working group are included in Appendix F

A group involving national managers of the branches impacted within Immigration and NZSIS will provide a steering group for the project. The project steering group will support the business owner and sponsor to make key project decisions and review and approve deliverables of the project.

Roles and responsibilities for the interagency project steering group are included in Appendix F.

Project roles and responsibilities (as documented by the INZ Portfolio) have been discussed with the relevant stakeholders.

The INZ Portfolio project management roles and responsibilities can be found under Cross Stage templates: s 6 (a) and used by the project manager for agreement.

Released under the Official Information Act 1982

Project team Roles and Responsibilities

Role	Name	Responsibility
Sponsor	Jacqui Ellis	The Project Sponsor is the person with overall accountability for the project. They are primarily concerned with ensuring the project delivers the agreed business benefits and they act as the champion for the project
Business Owner	9 (2) (a) s9(2)(a)	The Business Owner is responsible for the day to day oversight of the project. They also ensure the project is aligned to INZ strategy, champion the project and ensure benefits are realised.
Project Manager	[redacted]	The Project Manager has the authority to run the project on a day to day basis on behalf of the Business Owner within the constraints laid down. The Project Manager's prime responsibility is to ensure the project produces the required products within specified time, cost, quality, scope and risk. The Project Manager is also responsible for the project producing a result capable of achieving the defined Benefits.
Solution Architect	[redacted]	Leads the design of project product(s) capable of achieving the defined benefits.
Business Analysts	[redacted]	Collaborates with subject matter experts and users to define requirements and features for products to produce a result capable of achieving the defined benefits.
Business Change Manager	[redacted]	The Business Change Manager plays a key role in ensuring business change initiatives deliver value to the business by increasing adoption and usage.
ICT Lead	[redacted]	Represents ICT on the Project Steering group. Supports the project manager to manage Vendor and ICT technical resources and Technology governance.
Testing Lead	[redacted]	Assesses the features and quality of project product(s) ability to produce expected results.
Vendor Lead(s)	To be confirmed	The Supplier lead represents the interests of those designing, developing, facilitating, procuring and implementing the projects product(s). They are accountable for the quality of the product(s) and ICT or business technical integrity
Vendor Technical Lead (s)	To be confirmed	Leads the technical design of Vendor produced products.
Instructional Designer	To be confirmed	Writing of the learning module.
Technical Writer	To be confirmed	Writing of SOPs.
Risk Specialists	To be confirmed	Defining the threat assessment and evaluation processes.

Released under the Official Information Act 1982

Role	Name	Responsibility
NZSIS (project)	To be confirmed	• Subject matter experts advising and guiding development of requirements and business rules for INSS • Working group participants: review and respond in a timely manner to proposed project outcomes such as: o Requirements o Scope o Technical solution proposals o Provide formal advice to the steering group • Steering group o Assess and decide on requirements, business rules, and business case technical solution.
NZSIS (operational)		• Where NZSIS are threat specialists, provide high level threat assessment, advice and support for INZ threat specialists, immigration and border officers, support and contribute to new ICT systems, threat indicators, assessments and treatments. • s6(a) [redacted] [redacted] • Where possible and in compliance with all security requirements, support development of learning and development assets.

Released under the Official Information Act 1982

Project Risks

The following project risks have been identified and will be actively managed by the project. A link to the Project Risk Register can be found in the Reference Documents section at the beginning of this document. Risks are also entered in to project server. Where it appears that the risk will materialises as an issue, the discussion with the business owner and further escalation action may be required to be taken. Risk contingency may be required to be used and a CR.

Risk ID	Treatment Owner	Causes	Description	Impacts	Type	Controlled Likelihood	Controlled Impact	Treatment and Controls
6	Project Steering Group	Conflicting views over where the balance should be in setting the rules results in more time usage and complexity. Examples; • The INZ role in supporting service S10 collection - which will do more collection than screening. • The service advice that more info is required from ETA applicants while ETA is applying fewer (ETA vs Visa argument). • s6(c) [redacted]	Exception management dominates criteria and design discussions, driving time & complexity.	Increased time and complexity	Implementation	Possible	Moderate	Initially improve the adaptability and consistency of the processes and system based on current indicators. Prioritise changes that improve simplicity and automation first these changes are more easily accepted. Further changes can be introduced where the ability to forecast operational impacts improves. Communicate a clear process to capture proposed changes to assess when improved abilities to forecast and utilise capacity is available.

Released under the Official Information Act 1982

Risk ID	Treatment Owner	Causes	Description	Impacts	Type	Controlled Likelihood	Controlled Impact	Treatment and Controls
7	Project Steering Group	s6(c), s6(a) [redacted]	Criteria too risk adverse to be implemented effectively	Service Delivery and Customer Satisfaction	Capability and Capacity	Rare	Moderate	Assess likely improvement and impacts from proposed changes balancing both INZ and NZSIS objectives.
	Project Manager	Staff do not receive correct comms/training and don't revise the approach to assess threats. Examples; • Branches/Staff are too set in their ways to accept new processes • Training may not reach enough staff / be interpreted the correct way.	Education doesn't reach expected parties who continue with current process	People Safety and Security	People	Possible	Moderate	Engage well-resourced change management stream with learning and communication specialists. Targeted engagement through of high profile change champions in each team. Track exceptions relating to errors/misunderstanding early and address training/knowledge gaps.

Released under the Official Information Act 1982

Risk ID	Treatment Owner	Causes	Description	Impacts	Type	Controlled Likelihood	Controlled Impact	Treatment and Controls
8	Project Steering Group	Project staff that indicated their availability at start-up end-up not being available when project sessions are scheduled.	Limited access to SME resource may cause schedule delay (and therefore cost increase)	Service Delivery and Customer Satisfaction	People	Rare	Moderate	Engage wide enough steering group to request or escalate need to access SMEs in priority areas. Provide early notification of SME needs to enable scheduling to mitigate business impacts.
21	Business Owner	Different objectives and expectations exist in each agency in relation to : • Threat levels • Treatment levels and impacts to operations.	NZSIS are unable to support INZ requirements. INZ not able to support NZSIS requirements	Service Delivery and Customer Satisfaction	Dependencies	Possible	Moderate	Engage a joint agency project steering group to escalate decisions and commit changes. Prioritise changes to processes and systems that improve simplicity and automation first enabling change to be more easily accepted. Further changes can be introduced where the ability to forecast operational impacts improves.

Released under the Official Information Act 1982

Risk ID	Treatment Owner	Causes	Description	Impacts	Type	Controlled Likelihood	Controlled Impact	Treatment and Controls
	Project Steering Group	Inability to assess impacts to operations, conceptualise a completely new system and views over threat levels leading to : • Extended discussions over detailed changes upfront. • Over specification of changes upfront that doesn't deliver the expected benefit.	Delivery costs are higher than expected	Value for money	Implementation	Rare	Moderate	Prioritise changes to processes and systems that improve simplicity and automation first, enabling change to be more easily accepted. Regularly demonstrate functionality to users. Review proposed scope throughout project and submit change request to reduce or revised scope where the value of changes are no longer justified or a better approach is identified.
	Project Steering Group	Metrics on efforts for current operations are manual and limited.	Efficiency gains realised are significantly lower than forecast	Value for money	Benefits	Possible	Moderate	Prioritise changes to processes and systems that improve simplicity and automation first, enabling change to be more easily accepted. Further changes can be introduced where the ability to forecast operational impacts is improved.
	Project Steering Group	Coronavirus restrictions on travel limits the availability of Vendors	International Vendors unable to travel to NZ	Implementation	Time	Possible	Moderate	Limit travel where feasible and schedule to allow the onsite work to be completed as late as possible after lockdown restrictions ease.

Released under the Official Information Act 1982

Mandatory MBIE Risk Assessments and their Ratings are:

Risk Assessment	Rating (after assessment has been completed)
Complexity Assessment	Medium
Treasury Risk Profile Assessment (only Mandatory for High Complexity projects)	NA
Privacy Threshold Assessment	High

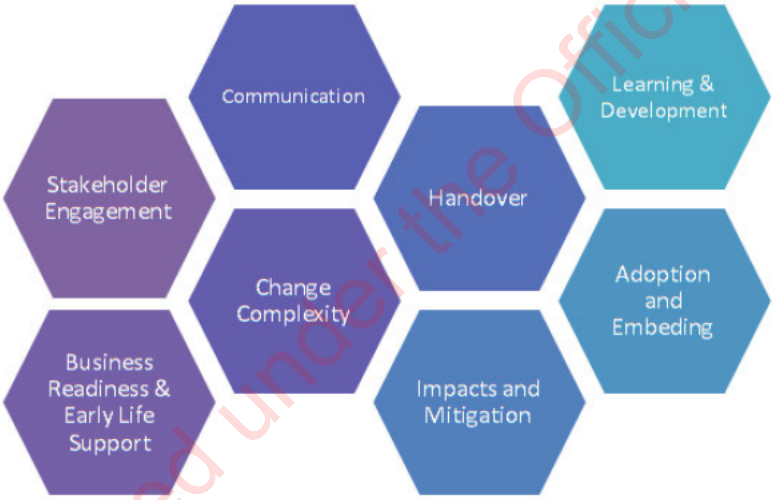
An independent privacy consultant has assessed privacy impacts during the initiation phase.

Corporate Compliance

Item	Yes / No	Comments / Link to completed document
Was a ***Privacy Impact Assessment*** required for this project	Yes	s 6 (a) Project actions in response to the impact assessment are included as an appendix.

Business Change Management

The Business Change Management strategies are outlined in the s 6 (a) document. It will apply the INZ Business Change Architecture and support the INZ Business Case.



Released under the Official Information Act 1982

Summary of the Change Management Focus Areas

Focus Areas	Priority H/M/L	Description
Change Complexity	M	Moderate change complexity with overall re-engineering of the end-to-end National Security Screening process to occur i.e. how National Security threat is assessed and managed holistically by INZ, and therefore ultimately handled by the frontline through to Threat Specialists and Intelligence teams. New systems to learn and changes to the ways of interacting with various teams and partner agencies requiring a better depth of understanding of National Security Screening as a whole. Close people impact management through delivery of communications and training, based on identification of impacts directly with the impacted people in workshop sessions. There could be a degree of media interest in the wake of the events in Christchurch on 15 March.
Stakeholder Engagement	H	There are a wide range of impacted stakeholders across the Immigration system and across multiple locations. Representatives from each impacted branch will be engaged for the INSS Working Group, to ensure the current and future states can be understood, and teams are brought on the journey. Direct engagement with stakeholders will be regular, face-to-face where appropriate (preferred) and supported by email to ensure the messages are understood.

Released under the Official Information Act 1982

Focus Areas	Priority H/M/L	Description
Impacts and Mitigations	H	Moderate overall impact to stakeholders, with changes that affect a number of teams across INZ. • Teams will need to have a more holistic understanding of the National Security Screening process to better connect with its purpose. • There will be new technology solutions to learn and use. • s6(a) • Relevant parties will need to be involved in regular review of the National Security Screening system to ensure it remains fit for purpose. No structural changes should result from this initiative or staff location changes. Future impacts to roles and responsibilities are yet to be determined, and can only be understood after some of the earlier change is implemented and realised. Culturally there will need to be a mind-set shift with emphasis on understanding the importance of National Security Screening. This will need to be championed and supported by leaders to ensure that messages are understood and the new processes stick. Generally this is about selling the value of good practice to better protect NZ from National Security risk.

Released under the Official Information Act 1982

Focus Areas	Priority H/M/L	Description
Learning and Development	H	Learning will be required for a stronger understanding of the National Security Screening processes and building a connection to its purpose. A learning module should be available to help inform and guide Immigration Officers on their role in identifying and handling National Security risk. This should be a module targeted at all frontline staff involved in National Security Screening, as a one off. It should also be integrated into new starter learning for those joining teams that handle applications associated with National Security risk. The module should be available as an ongoing refresher should anyone require it. In addition to National Security SMEs, a small cross-section of SMEs from teams that would complete this module should contribute to it and provide feedback before it is released for completion. For Technology solutions, representatives from each team should be able to take part in UAT in order to build their familiarity with new systems and act as champions for their team. Teams should also be engaged early to be involved in and understand new processes and Standard Operating Procedures, to enable smooth handover and successful adoption.
Communications	M	Communications should be leader-led and with emphasis on face-to-face communication first, supported by email where appropriate. A variety of communication needs to be done in order to ensure the messages are understood, through Business Owner and senior leaders championing the change, contextual project updates, and project meetings with impacted stakeholders, showcases and workshops.

Released under the Official Information Act 1982

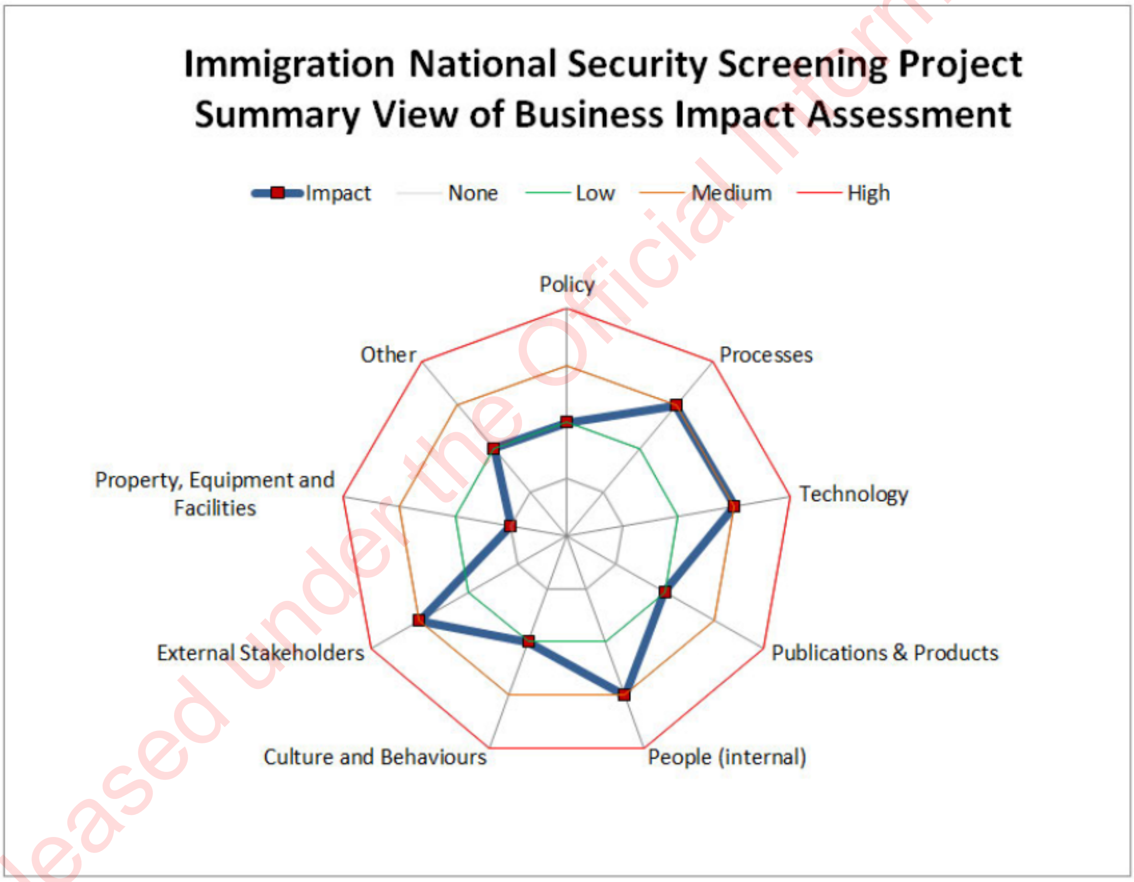
Focus Areas	Priority H/M/L	Description
Business Readiness and Early Life Support	M	Readiness checkpoints should be introduced prior to the end of each stage of the project (there are 4 core stages). This will ensure that the changes introduced as part of each stage are understood and will be adopted before moving into the next stage. Some tasks and activities that need to be assessed for readiness include: • Ability to use the new workflow tracking tool (minimal support required in order to use it) e.g. confident in finding out the security check status of an application, can see who an application is sitting with for next action • Compulsory completion of learning module for relevant staff – with a knowledge test at end of module • Teams have greater understanding/clearer interpretation of Ops Manual instructions – followed up with a survey or interview • Teams are familiar with Risk Indicators and know where to find guidance material for these Early Life Support will depend on the change occurring in each stage. Onsite support should be made available where appropriate. Change champions should be identified within the teams, who are well informed on the above readiness areas and can act as 'go-to' people in their team. Early Life Support duration will depend on the stage.
Adoption, Success & Monitoring	M	Teams who are expected to own processes and changes post-project will be involved in making the change and brought on the journey throughout the project in order to ensure adequate understanding of ownership and handover. Teams will be involved throughout the project and handover sessions will be run as the project gets closer to the close stage. Given the change is incremental the readiness checkpoints can also be used to monitor the success of the change in the previous stages. Metrics will be able to be generated and further interviews to assess the success of transition can be run in order to understand if the change has been successful.

Released under the Official Information Act 1982

Focus Areas	Priority H/M/L	Description
Handover	M	New Standard Operating Procedures (SOPs) will need to be produced, new training material will be produced and existing process maps will need to be updated. Handover over these materials will be done with the right teams and forums to ensure consistent and regular review occurs in the future as and when needed. Teams will be made aware of the expectations and a key test of handover will be through testing of the risk model.

Business Change Impacts

A high level impact assessment was conducted with the INS project team using the INZ high level change impact tool and then validated with the reviewers of this document. The impacts were noted across a range of impact areas and the validated findings are shown below by the blue line.



Communications

A separate Communications Plan will be developed as part of the Change Management Plan post Business Case. However, an initial assessment has been completed; refer to Defining the Change.

Key messages will be distributed to the project stakeholders using a variety of mechanisms and channels.

Released under the Official Information Act 1982

What is the message?	Who is delivering the message?	What is the channel?	Stakeholder Group	Frequency
National Security screening will be fit for purpose and efficiently delivered by INZ.	Project, Leaders & Business Owner where appropriate.	Email, face-to-face, workshops/meetings	Intelligence, Data & Insights Border & Visa Operations Verification & Compliance Refugee Migrant Services	Minimum monthly (but more frequently as required)
Striking the balance in reducing the risk of National Security harms from a changing threat landscape, while facilitating entry of the people New Zealand needs over the border.	Project, Leaders & Business Owner where appropriate.	Email, face-to-face, workshops/meetings	Intelligence, Data & Insights Border & Visa Operations Verification & Compliance Refugee Migrant Services	Minimum monthly (but more frequently as required)
Leveraging new data analytics, digitisation and automation technologies to improve consistency, reduce risk and help make our jobs easier and more effective.	Project, Leaders & Business Owner where appropriate.	Email, face-to-face, workshops/meetings	Intelligence, Data & Insights Border & Visa Operations Verification & Compliance Refugee Migrant Services	Minimum monthly (but more frequently as required)
A risk model informed by evidence with consistent processes, clear and effective quality controls and governance is being implemented.	Project, Leaders & Business Owner where appropriate.	Email, face-to-face, workshops/meetings	Intelligence, Data & Insights Border & Visa Operations Verification & Compliance Refugee Migrant Services	Minimum monthly (but more frequently as required)

The process for handling feedback will be determined as appropriate.

Released under the Official Information Act 1982

Stakeholders

The following have been identified as key stakeholders in this project:

Stakeholder name	Position	Organisation	Interest
Jacqui Ellis	GM, Intelligence, Data & Insights	Intelligence, Data & Insights, INZ	Project Sponsor
9 (2) (a)	National Manager, Targeting, Analytics & Insights	Intelligence, Data & Insights, INZ	Business Owner
s9(2)(a)	National Manager, Risk & Verification	Verification & Compliance, INZ	Business Fit
[redacted]	National Manager, Enablement	Enablement	Business Fit
[redacted]	Manager Risk Assessment	Verification & Compliance, INZ	Business Fit
NZSIS	-	NZSIS	Business Fit – Partner Agency
s9(2)(a)	Manager Operational Policy	Enablement, INZ	Policy and Legislation impacts
[redacted]	Manager ICT Systems	Enablement, INZ	Business Fit
[redacted]	Business Advisor	Border & Visa Operations, INZ	Business Fit
[redacted]	INZ Enterprise Architect	Technology, Strategy and Architecture, MBIE	Strategic Fit
[redacted]	Business Analytics & Targeting Manager	Intelligence, Data & Insights, INZ	Business Fit
[redacted]	Senior Business Advisor (Systems)	Verification & Compliance	Business fit
[redacted]	Visa Operations Manager (Beijing)	Border & Visa Operations	Business Fit
[redacted]	Manager Refugee Quota	Refugee & Migrant Services, INZ	Business Fit
[redacted]	Technical Advisor	Border & Visa Operations, INZ	Business Fit
[redacted]	Head of Border Operations	Border & Visa Operations, INZ	Business Fit

Released under the Official Information Act 1982

Stakeholder name	Position	Organisation	Interest
s9(2)(a) [redacted]	Immigration Manager	Border & Visa Operations, INZ	Business Fit
[redacted]	Head of Operations, NADO	Border & Visa Operations, INZ	Business Fit
[redacted]	Senior Solicitor	Legal Services, Corporate Governance & Information	Legislative impacts and legal advice.
[redacted]	Business Architect	Operations, Tasking & Improvement, INZ	Compatibility with INZ Risk Model.
[redacted]	Principal Policy Advisor	Labour, Science & Enterprise, Labour & Immigration Policy	Policy and legislation Impacts.
[redacted]	Acting Intelligence Manager Wellington	Intelligence, Data & Insights, INZ	Business Fit
[redacted]	Senior Advisor Privacy	Legal Services, Corporate, Governance & Information	Privacy Impacts
NZ Police	-	NZ Police	Business Fit – Partner Agency
NZ Customs	-	NZ Customs	Business Fit – Partner Agency
MFAT	-	MFAT	Business Fit – Partner Agency
Maritime NZ	-	Maritime NZ	Business Fit – Partner Agency

Released under the Official Information Act 1982

s9(2)(g)(i), s9(2)(a)

[redacted]

Released under the Official Information Act 1982

Appendix A – Detailed Financial Breakdown

Asset Management

New asset	***Yes***
Replacement Asset	***Yes***

Summary of business capital and operational costs including out years

Summary of capital and operational costs including out years

	Current FY 19/20	FY 20/21	FY 21/22	FY 22/23	FY 23/24	FY 24/25	Total
Total project delivery capex expenditure	47,062	2,778,186	353,072	s9(2)(j) [redacted]	[redacted]	[redacted]	[redacted]
Total project delivery opex expenditure	-	10,000	35,000	[redacted]	[redacted]	[redacted]	[redacted]
Estimated on-going business opex (excluding depreciation)	-	-	-	[redacted]	[redacted]	[redacted]	[redacted]
Estimated on-going ICT opex (excluding depreciation)	-	-	193,888	[redacted]	[redacted]	[redacted]	[redacted]
Whole of Life costs (capex + opex + on-going costs[6])	47,062	2,788,186	581,960	[redacted]	[redacted]	[redacted]	[redacted]
Net cash flow (Benefits less Total Costs)	-47,062	-2,788,186	-581,960	[redacted]	[redacted]	[redacted]	[redacted]
Depreciation			403,607	[redacted]	[redacted]	[redacted]	[redacted]

Released under the Official Information Act 1982

ICT capital and operational costs

The Capex costs in addition to on-going ICT operational support costs are detailed in the following table(s).

Summary of capital and operational costs including out years						
	FY 20/21	FY 21/22	FY 22/23	FY 23/24	FY 24/25	Total
s9(2)(j)	92,888.00	92,888.00	s9(2)(j)			
s9(2)(j)	96,000.00	96,000.00				
AMS support	5,000.00	5,000.00				
Total	193,888.00	193,888.00				

Breakdown of Capex Costs				
	Stage 1	Stage 2	Stage 3	Stage 4
InRule Environments	92,888.00			
ICT Resources	178,925.00	155,266.67	119,141.67	79,050.00
Project Resources	385,815.00	138,178.33	110,032.50	79,021.67
Vendors	405,000.00	605,000.00	635,000.00	195,000.00
Total Capex	1,062,628.00	898,445.00	864,174.17	353,071.67

Contingency: Contingency has been set by MBIE Finance in a memo dated 27 October 2016. The memo set out that:

- A standard approach to contingency be applied across MBIE projects where contingency will not be approved as part of upfront funding as the portfolio boards need to focus on mitigating risks during the life of the project
- Portfolio Boards will assess the level of contingency to ensure they are appropriate for the scale, complexity and uncertainty related to the project based on the Risk Adjustment Cost (RAC).
- A Change Request will be raised to the appropriate governance board to draw down on the contingency if required.

Link to the memo: s 6 (a)

Released under the Official Information Act 1982

Breakdown of Vendor Costs					
		Stage 1	Stage 2	Stage 3	Stage 4
eForms(Data Capture)	s9(2)(j) [redacted]		200,000.00	30,000.00	30,000.00
Workflow and reporting	[redacted]		350,000.00	100,000.00	45,000.00
AMS Including Integration	[redacted]	350,000.00	35,000.00	35,000.00	35,000.00
Portal Tactical	[redacted]	35,000.00			
Rule Training and Design review	[redacted]	20,000.00	20,000.00	20,000.00	10,000.00
ETA Integration	[redacted]			150,000.00	
Watch list Matching	[redacted]			250,000.00	
APP integration	[redacted]				75,000.00
NSC Decommission	[redacted]			50,000.00	
Total Vendor	[redacted]	405,000.00	605,000.00	635,000.00	195,000.00

Breakdown of ICT Resource Costs Stage 1					
ICT Resource	Rate	FTE	Months	Hours	Costs
ICT Business Analyst	120	1	3	425	51,000.00
ICT Azure specialists (Deployment)	100	0.5	3	213	21,250.00
ICT Testing Lead	110	0.2	3	85	9,350.00
ICT Testing Resources	80	1	3	425	34,000.00
ICT Technical Lead	130	0.5	3	213	27,625.00
Architect	140	0.5	3	213	29,750.00
ICT Security Architect	140	0.1	3	43	5,950.00
ICT Resource Total					178,925.00

Breakdown of Project Resource Costs Stage 1					
ICT Resource	Rate	FTE	Months	Hours	Costs
Business Analysts	120	1	6	850	102,000.00
Project Co-ordinator	80	0.33	6	281	22,440.00
Project Manager	130	1	6	850	110,500.00
Business Change Manager	125	0.5	6	425	53,125.00
Learning Specialist	115	0.5	6	425	48,875.00
Technical Writer	115	0.5	6	425	48,875.00
Project Resource Total					385,815.00

Released under the Official Information Act 1982

Appendix B – Benefits Table

Benefit #	Type	Benefit Title	Benefit Description	Baseline	Target
Ben01	Reduced risk	Reduced risk of non-compliance with IA09 s16. No Visa is granted or waiver applied if the person is, or is likely to be a threat to National Security.	Improved coverage of Security threats and quality of assessments, targeting all migrants that could be a potential threat and alignment with National Security threat priorities.	s6(a) [redacted]	s6(a) [redacted]
Ben02	Reduced risk	Reduced likelihood of harm from new undetected National Security threats.	Screening coverage adapts quickly to changes in threat levels and new threats.	Unknown speed of adaption, at least 12 months is estimated.	Screening can adapt within 7 days for 90% of changes.
Ben03	Reduced risk	Increased number of security threats treated offshore.	Coverage and improved quality activities manages risk of harm to National Security for Visa Services and Border management, moving the treatment of security threats offshore.	s6(a) [redacted]	95% reduction in reactive treatment.
Ben04	Improved Responsiveness	Faster identification of threats and completion of screening assessments.	Faster more streamlined National Security screening checks within visa processing.	Manual process presently in place to measure threats. These are subjective and perceived to be slow.	Improvement measured and speed improvement identified via survey. After baseline established objective measures and performance improvement plans are tracked.

Released under the Official Information Act 1982

Appendix C – Consultation

The following stakeholders provided feedback on content used in creating this business case.

Stakeholder name	Position	Organisation	Area
Jacqui Ellis	GM, Intelligence, Data & Insights	Intelligence, Data & Insights, INZ	Project Sponsor
9 (2) (a)	National Manager, Targeting, Analytics & Insights	Intelligence, Data & Insights, INZ	Business Owner
s9(2)(a)	National Manager, Risk & Verification	Verification & Compliance, INZ	Project Steering, Benefits, Governance Decisions, Business Fit
[redacted]	Manager Risk Assessment	Verification & Compliance, INZ	Working group, Business Fit
[redacted]	National Manager, Visa	Border & Visa Operations	Project Steering, Benefits, Governance Decisions, Business Fit
[redacted]	National Manger, Immigration Enablement	Enablement, INZ	Project Steering, Governance Decisions, Business Fit
NZSIS	-	NZSIS	Working group, Requirements Feedback specialist threat knowledge.
s9(2)(a)	Manager Operational Policy	Enablement, INZ	Working group, Business Fit and Operating policy assumptions and instruction changes
[redacted]	Manager ICT Systems	Enablement, INZ	Architecture review. Ongoing technology costs
[redacted]	Business Advisor	Border & Visa Operations, INZ	Working group, Business Fit, Requirements Feedback
[redacted]	Operations Manager	Border & Visa Operations, INZ	Working Group, Business Fit
[redacted]	INZ Enterprise Architect	Technology, Strategy and Architecture, MBIE	Architecture review
[redacted]	Business Analytics & Targeting Manager	Intelligence, Data & Insights, INZ	Working group, Business Fit, Requirements Feedback

Released under the Official Information Act 1982

Stakeholder name	Position	Organisation	Area
s9(2)(a) [redacted]	Senior Business Advisor (Systems)	Verification & Compliance	Working group, Business Fit
[redacted]	Visa Operations Manager (Beijing)	Border & Visa Operations	Working group, Business Fit
[redacted]	Manager Refugee Quota	Refugee & Migrant Services, INZ	Working group, Business Fit, Requirements Feedback
[redacted]	Technical Advisor	Border & Visa Operations, INZ	Working group, Business Fit, Requirements Feedback
[redacted]	Immigration Manager	Border & Visa Operations, INZ	Working group, Business Fit, Requirements Feedback
[redacted]	Visa Operations Manager	Border & Visa Operations, INZ	Consulted on Business Fit
[redacted]	Head of Border and Visa Operations - Porirua	Border & Visa Operations, INZ	Consulted on Business Fit
[redacted]	Head of Operations, NADO	Border & Visa Operations, INZ	Consulted on Business Fit
[redacted]	Senior Solicitor	Legal Services, Corporate Governance & Information	Working group, Business Fit
[redacted]	Business Architect	Operations, Tasking & Improvement, INZ	Compatibility with INZ Risk Frameworks
[redacted]	Principal Policy Advisor	Labour, Science & Enterprise, Labour & Immigration Policy	Working group, Business Fit and Operating policy assumptions and instruction changes
[redacted]	Intelligence Manager Wellington	Intelligence, Data & Insights, INZ	Working group, Business Fit
[redacted]	Intelligence Analyst	Intelligence, Data & Insights, INZ	Working group, Business Fit
[redacted]	Principal Intelligence Analyst	Intelligence, Data & Insights, INZ	Working group, Business Fit
[redacted]	INZ Risk Manager	Assurance, INZ	Working group, Business Fit, Specialist Quality Assurance advice

Released under the Official Information Act 1982

Stakeholder name	Position	Organisation	Area
s9(2)(a) [redacted]	Senior Advisor Privacy	Legal Services, Corporate, Governance & Information	Working group overview. Privacy risks and independent review
[redacted]	Risk Profiling Analyst	Verification & Compliance, INZ	Working group, Business Fit, – Specialist advice for War Crimes
[redacted]	Analyst	Intelligence, Data & Insights, INZ	Open Source advice Specialist
[redacted]	Open Source Specialist	Intelligence, Data & Insights, INZ	Open Source Specialist

Released under the Official Information Act 1982

Appendix D Options Analysis

Option A: Status Quo

- Option A represents the counterfactual.
- Assessment work continues as it does today but
- s6(a) [redacted]
- Option A represents the cost to extend immigrations screening effort to all migrants increasing resourcing but no other changes.
- The costs for NZSIS to resource this effort are not assessed as part of this but are expected to be extensive.
- This option is not considered viable due to the costs and treatment would remain non proportional to the threat

Option B Single Refresh

- Option B represents the lowest cost investment to implement a risk and system framework to screen all migrants and provide assurance they are not likely to be a threat to National Security.
- A full review of the current threat levels and controls is undertaken with risk specialists in DPMC, NZSIS and INZ.
- A revised criterion for each threat and priority is determined with the threat specialist with assessment and treatment balanced with current objectives and resourcing constraints.
- Changes to systems policy, operating instructions, and training/education are defined to implement the changes to controls.
- A framework is defined to monitor and review risks and controls on an ongoing basis which is handed over to verification and compliance branch of Immigration. The framework would provide steps to enable changes to threat criteria through the system, policy, operating instructions and training/education materials where required.
- A system change is introduced that provides biographic information of all migrants to the security service to identify persons of concern to National Security.
- s6(a) [redacted]
- System changes are introduced to provide the criterion to identify the migrants that are a possible threat and track any assessment work required to verify the threat level. The criteria can be updated by a threat expert using business rules where policy or operating instructions are approved through the framework.
- The system in tracking assessment work provides information that can be used to monitor the assessment activity and provide metrics to inform revisions to criterion or controls for the threats.
- BAU processes could deliver any further revisions. More significant changes would be delivered by establishing another project.

Released under the Official Information Act 1982

Option C: Staged delivery longer term investment focus

- Delivers the changes described in Option B.
- Provides 2 incremental changes to the system and threat controls and system. These increments use more up to date information and analytical capabilities established in earlier stages. The efficiency of making a change is also reduced from capabilities established the earlier stages.
- Establishing the framework quickly enables a faster delivery of benefits and efficiencies without the risk of having to finalize all changes up front.
- Training would be provided to personal to have expert knowledge in the tooling, the information sources and threats to enable efficient use relevant to the threats. This replaces inefficient and inconsistent collection and assessment used currently.
- Investigates data modelling for National Security risks using existing RAP data sets. It is possible risk patterns can be identified in migrant data sets and the project provides an ability to imbed this into screening.
- Optimizes the timing and use of RAP to be efficient and minimize impact to migrants.

Other options considered non-viable

- Transfer all National Security decision making to NZSIS. Considered non-viable as:
  - s6(a) [redacted]
- s6(a), s6(c) [redacted]
  - [redacted]
- Change all Visa applications to be online and provide all details to NZSIS.
  - This is not practical as many migrants don't have reliable web access, and would thus be excluded or significantly disadvantaged from applying to migrate to New Zealand.
- s6(c), s6(a) [redacted]
  - Tools such as RAP are decision support tools. We need a human to make the final decision on whether or not a migrant may enter New Zealand.
  - s6(c), s6(a) [redacted]
- s6(a), s6(c) [redacted]
  - [redacted]
- Alerting of priority threat events to NZSIS
  - Does not capture all potential threats to NZ's security.
- Increasing the availability of specialists to respond for Border screening
  - An objective of the project is to support moving the screening of migrants as far offshore as possible and to conduct assessments as early as possible. By focussing on border screening, opportunities to exclude high risk migrants before they arrive in New Zealand are lost.
  - An additional objective of the project is to utilise current staff resources. Increasing border specialists does not support this objective.
- Single agency ownership for evaluating and treating National Security threats
  - INZ and NZSIS have different, but complementary skill sets. A joint agency approach supports more effective screening while not changing staff head count.

Released under the Official Information Act 1982

- NZSIS alone identify threat priorities, criteria and sources
  - s6(a) [redacted]
  - The threat assessment model takes a whole of government approach to screening, with agencies such as DPMC, MFAT and MPI providing significant input to threat priorities, criteria and sources.
- INZ alone Identify threat priorities criteria and sources
  - s6(a) [redacted]
  - The threat assessment model takes a whole of government approach to screening, with agencies such as DPMC, MFAT and MPI providing significant input to threat priorities, criteria and sources.
- s6(c), s6(a) [redacted]
  - [redacted]
- Process changes without technology enhancements
  - Process changes offer significant benefits to treat threats, and will be a major part of the first stage of INSS’s deliver. However process change alone will not deliver all of the efficiency gains expected. Existing technology is at or beyond end of life and does not support the wider organisational technology development roadmap.
- Process or system changes without supporting learning and development
  - To gain full value from process or system changes, staff must learn how to use these new tools effectively. This will not be via a process of osmosis. Focussed learning and development will support rapid uptake and effective, efficient use of the new process and technology tools.

Released under the Official Information Act 1982

Appendix E Requirements Table

The requirements are based on the MoSCoW (Must, Should, Could, Would) Prioritisation Method for rating the projects requirements unless otherwise specifically agreed with the Business Owner and Sponsor.

Requirements shown with Removed in the Outcome(s) Supported column and Redundant in the Requirements Description column have been included to retain numbering integrity with an INZ technical document that will be updated after the COVID 19 lockdown is lifted.

Req No.	Outcome(s) Supported	Requirement Description	MoSCoW
R1	All migrants that may pose a potential National Security threat are assessed.	All migrants[7] that may pose a potential National Security threat are assessed. s6(a) [redacted]	M

[7] "Migrant" does not include New Zealand citizens.

Released under the Official Information Act 1982

Req No.	Outcome(s) Supported	Requirement Description	MoSCoW
R2	There is a shared understanding between agencies and within INZ of security threats and approach to treat them.	Risk assessment may be undertaken by INZ or NZSIS staff, to ensure the capabilities of each agency are best utilised. Initial proposed responsibility settings for risk assessment threat specialists are: • s6(a) Note that in some cases migrants may present with multiple risk indicators. s6(a) . In this case, responsibility for conducting an assessment may be shared by risk specialists in both INZ and NZSIS, or one agency may take the lead. Rules for this will be developed post-business case.	M
R3	Threat and treatment information is directed to the right people to enable action to be taken at the earliest possible time	Where an assessment indicates that a threat may be posed by a migrant, the migrant will be subject to further scrutiny which may include: • They may be required to provide additional information to facilitate the assessment • s6(a) • INZ or NZSIS security holdings may be further referenced to determine the risk status of the migrant In all cases, migrants will not be granted visas or permitted to travel to, enter or stay in New Zealand until they receive a clear security assessment.	M

Released under the Official Information Act 1982

Req No.	Outcome(s) Supported	Requirement Description	MoSCoW
R4	There is a shared understanding between agencies and within INZ of security threats and approach to treat them.	Where appropriate, formal documented agreements with partner agencies will be developed. This may include: • Standard operating procedures • Memoranda of understanding and terms of reference agreements • Service level agreements • Direct access agreements • Treaties	M
R5	Removed	Redundant	
R6	There is a shared understanding between agencies and within INZ of security threats and approach to treat them	Following assessment by threat specialists, migrant threat assessment statuses will be available to IOs.	M
R7	There is a shared understanding between agencies and within INZ of security threats and approach to treat them	NZSIS will provide a recommendation to INZ on the assessed security status of the migrant. The decision to grant entry or not resides with the Immigration Minister, and is delegated to INZ staff through the MBIE Chief Executive.	M
R8	There is a shared understanding between agencies and within INZ of security threats and approach to treat them.	An alert in a migrant's record can only be cleared following human intervention and full assessment of the risk the migrant presents. Where multiple potential threats are identified, assessments will be conducted by all relevant threat specialists.	M

Released under the Official Information Act 1982

Req No.	Outcome(s) Supported	Requirement Description	MoSCoW
R9	Governance and assurance supports clear and consistent processes and controls	Traceability of INSS systems and processes to the Immigration Act 2009 will be maintained. The traceability hierarchy is: • Legislation and regulations (primarily IA09 and IAS17, plus other Acts as appropriate) • MBIE / INZ operating instructions • MBIE / INZ Standard operating procedures (SOPs) Traceability will be formally reviewed by quality processes including quality control and quality assurance to confirm compliance with this requirement is maintained.	M
R10	There is a shared understanding between agencies and within INZ of security threats and approach to treat them.	Partner agency requirements will be considered and complied with provided they do not conflict with INSS's traceability hierarchy. This may include: • Other agency or shared training requirements • Other agency or shared technology requirements and standards	S
R11	Roles and responsibilities between agencies and within INZ are clearly defined	Where probable security risks are identified during screening checks, migrants will be referred for in-depth human assessment and, where required 2PC[8] (quality). Quality checks will be measured against performance targets.	M
R12	There is a shared understanding between agencies and within INZ of security threats and approach to treat them.	Outcomes of assessments will be timely and where practical, will be measured against performance targets.	S

[8] It is understood that second person checks ("2PC") is an older term for quality control checks, though this term is still in wide use at INZ.

Released under the Official Information Act 1982

Req No.	Outcome(s) Supported	Requirement Description	MoSCoW
R13	There is a shared understanding between agencies and within INZ of security threats and approach to treat them.	When conducting in-depth assessments on threat identified migrants, the assessment will continue until a clear determination of the threat can be made. These assessments will not be constrained by time or volume-based performance criteria.	M
R14	Roles and responsibilities between agencies and within INZ are clearly defined	The outcomes of assessments made using high side information will be provided back to immigration officers at an unclassified level in clear, unambiguous language. Wherever possible, this will be via agreed scripted responses. The intention of this requirement is to support IO decision making, not compromise secure sources or increase the workloads of threat specialists working with high side material.	M
R15	Threat and treatment information is directed to the right people to enable action to be taken at the earliest possible time	To improve the quality of information available to INZ and NZSIS staff and to support good migrant entry decision making, inputs will include: • s6(a) [redacted].	M
R16	Threat and treatment information is directed to the right people to enable action to be taken at the earliest possible time	s6(c) [redacted]	S

Released under the Official Information Act 1982

Req No.	Outcome(s) Supported	Requirement Description	MoSCoW
R17	Threat and treatment information is directed to the right people to enable action to be taken at the earliest possible time	Where practical, online forms will be optimised to collect information from migrants. The intention is to reduce rather than increase manual entry. This optimisation may include, but is not limited to: • "enter once / reuse many" information fields • Field auto – population • Ensure forms are consistent and only ask for information that is required to conduct assessments. • Forms will permit offline completion. This is to support completion of forms where internet connectivity is poor or inconsistent.	S
R18	Threat and treatment information is directed to the right people to enable action to be taken at the earliest possible time	Where online forms are provided for migrants to enter information, the forms will be clear and understandable to migrants. This includes: • Supporting guides are available in non-English languages and ethnic character sets • Forms are contextual. This means that if a question (e.g., "have you served in the military") leads to a follow up question, this question will open other response choices (e.g., "which military unit did you serve with?") • If the migrant had assistance completing the form in English (forms must be completed in English), the migrant is able to indicate this.	S
R19	Threat and treatment information is directed to the right people to enable action to be taken at the earliest possible time	Where online forms are provided for migrants to enter information, the forms will support improving information quality. This may include: • Provide the ability to upload attachments directly • Support auto-translation of non-English entry	C

Released under the Official Information Act 1982

Req No.	Outcome(s) Supported	Requirement Description	MoSCoW
R20	Threat and treatment information is directed to the right people to enable action to be taken at the earliest possible time	s6(a) [redacted]	S
R21	Threat and treatment information is directed to the right people to enable action to be taken at the earliest possible time	s6(a) [redacted]	M
R22	Threat and treatment information is directed to the right people to enable action to be taken at the earliest possible time	s6(c) [redacted]	C

Released under the Official Information Act 1982

Req No.	Outcome(s) Supported	Requirement Description	MoSCoW
R23	Threat and treatment information is directed to the right people to enable action to be taken at the earliest possible time	s6(a) [redacted] [redacted]	M
R24	Governance and assurance supports clear and consistent processes and controls.	For audit purposes the solution will retain all data used to inform in the INSS decision making process. Access to data will depend on security clearance of reviewers and their need to access the information. Audit logging is outlined in non-functional requirements. Data held for audit may include: • Threat assessment findings • Assessment information referenced • Decision • Open source search results Data types could include documents, images or text	M
R25	Governance and assurance supports clear and consistent processes and controls.	INSS will be provided with auditing and reporting functionality to ensure risk indicator assessments are being applied fairly and appropriately	M
R26	Governance and assurance supports clear and consistent processes and controls.	INSS screening and open source searches will be configurable by rules. • These rules will be developed by threat specialists from INZ and NZSIS. • Prior to release, rules will be subject to compliance checks. • After release, rules will be subject to governance review. • Rules will be determined post-business case.	M

Released under the Official Information Act 1982

Req No.	Outcome(s) Supported	Requirement Description	MoSCoW
R27	The INS threat framework and treatments are reviewed regularly and adapted in response to the global threat landscape	To ensure risk models are current and match evolving threats, the risk indicator management framework will be regularly reviewed and where necessary updated. Initial setting for review of the threat framework and treatments is annually.	M
R28	Threat and treatment information is directed to the right people to enable action to be taken at the earliest possible time	Low risk migrants will be quickly identified and security cleared (i.e., provided there are no other reasons to decline they will be issued a visa, able to board their craft or enter or remain in NZ).	S
R29	Removed	Redundant	
R30	Agile systems and processes, continuously refined and consistently improved	When a migrant has been assessed as a security threat, the solution will provide an alert notification. The form of this notification will be determined during technical assessment and design.	M
R31	Agile systems and processes continuously refined and consistently improved.	Linkages between INZ and NZSIS systems and processes will ensure that if a migrant application is halted, so do any checks occurring in either system. This is to ensure unnecessary effort by INZ and partner agencies is reduced.	M
R32	Agile systems and processes, continuously refined and consistently improved	Migrant application will be flagged to indicate to Immigration Officers when security assessments are in progress, and that they may not issue visas.	M

Released under the Official Information Act 1982

Req No.	Outcome(s) Supported	Requirement Description	MoSCoW
R33	Threat and treatment information is directed to the right people to enable action to be taken at the earliest possible time	To ensure migrant security assessments can be completed in a timely and effective manner, information from INZ holdings covered by direct access agreements will be available to NZSIS and other partner agencies. This information includes: • Migrant visa applications and supplemental information • Holdings from open source repositories • Holdings from closed source repositories (subject to security controls and appropriate clearances)	M
R34	Removed	Redundant	
R35	Agile systems and processes continuously refined and consistently improved.	Whenever a migrant to New Zealand interacts with INZ, their records will be updated immediately, permitting review of travel profile for that migrant. This includes all data held by INZ and / or external sources (e.g., NZSIS). When a security issue is identified with migrant, alerts will be provided in real time to appropriate INZ and NZSIS staff.	S
R36	Simple, easy processes and systems, providing clear guidance and expectations for all staff and migrants	Staff will be provided with standard operating procedures (SOPs) and workflow tools that accurately and clearly outline how they assess and decide on the security risk associated with migrants.	M
R37	Simple, easy processes and systems, providing clear guidance and expectations for all staff and migrants	INSS screening will be initiated at the migrant's first contact with INZ. Sources include: • AMS for visa applications (Covers all lodgement channels) • NZeTA for Visa waiver migrants • APP for Australian citizens or travellers returning on a valid visa • Any future state systems or processes. Future-proofing to be designed into any system or process changes developed as part of this project.	M

Released under the Official Information Act 1982

Req No.	Outcome(s) Supported	Requirement Description	MoSCoW
R38	Agile systems and processes continuously refined and consistently improved.	The solution will have a centralised business rules component with a capability of applying screening rules across all migrant entry points.	M
R39	Agile systems and processes continuously refined and consistently improved.	s6(c), s6(a)	S

Released under the Official Information Act 1982

Req No.	Outcome(s) Supported	Requirement Description	MoSCoW
R40	Threat and treatment information is directed to the right people to enable action to be taken at the earliest possible time	To support security assessments, information supplied by migrants through visa applications, NZeTA requests and other immigration process entry points will be s6(c) pre-assessed against security business rules[9]. This automatic pre-assessment will include the following features: - Preliminary indication of which threat (see R2 above) has been recorded. - s6(a) - All other cases will be routed directly to NZSIS for further assessment. This requirement will depend on development and deployment of an ICT solution which will also provide: - A repository for data relating to a migrant assessment including case notes biographical details of the migrant and outcome of human assessment. - Storage and access to assessment outcomes - Support for prioritisation of cases - Tracking for case progress - Searchable access and unique identification of cases	S
R41	Threat and treatment information is directed to the right people to enable action to be taken at the earliest possible time	Where necessary, cases and case outcomes will be shared with other INZ groups and referenced when responding to migrants' appeals.	S
R42	Removed	Redundant	

[9] These rules will be completed post-business case

[10] The term "cases" is used generically here and throughout this document.

Released under the Official Information Act 1982

Req No.	Outcome(s) Supported	Requirement Description	MoSCoW
R43	Removed	Redundant	
R44	Removed	Redundant	
R45	Agile systems and processes, continuously refined and consistently improved	The solution will facilitate interactions with NZSIS, including: • Sending referrals to NZSIS • Receiving confirmation of receipt of referral from NZSIS • Managing NZSIS Requests for additional information • Receiving responses from NZSIS security assessments	M
R46	Removed	Moved to NFRs	
R47	Agile systems and processes, continuously refined and consistently improved	In the event a visa application is cancelled, all work associated with the security check should also be cancelled and this will be identified in any ICT system developed to support this requirement. All records of the transaction will be retained and may be shared with partner agencies, subject to the terms of a Direct Access Agreement.	M
R48	Agile systems and processes, continuously refined and consistently improved	Statuses of migrant security assessments will be maintained and alerts will be provided to INZ and NZSIS staff when a status changes.	M
R49	Agile systems and processes, continuously refined and consistently improved	INZ and NZSIS staff will be able to retrieve records and outcomes of prior security assessments conducted on migrants, where these are available.	M
R50	Removed	Redundant	
R51	Removed	Redundant	
R52	Removed	Redundant	

Released under the Official Information Act 1982

Req No.	Outcome(s) Supported	Requirement Description	MoSCoW
R53	Removed	Redundant	
R54	Removed	Redundant	
R55	The INS threat framework and treatments are reviewed regularly and adapted in response to the global threat landscape	s6(a) [redacted]	S
R56	Removed	Redundant	
R57	Agile systems and processes continuously refined and consistently improved.	s6(a) [redacted]	S
R58	The INS threat framework and treatments are reviewed regularly and adapted in response to the global threat landscape	s6(a) [redacted]	S

Released under the Official Information Act 1982

Req No.	Outcome(s) Supported	Requirement Description	MoSCoW
R59	Staff operating within the system are adequately trained on roles and responsibilities	Staff will be provided with training at on boarding and receive ongoing learning and development opportunities appropriate to their needs, to build knowledge and ensure National Security screening objectives can be effectively met	M
R60	Staff operating within the system are adequately trained on roles and responsibilities	To support security assessment effectiveness, staff training will be subject to quality assurance review. This will include review of: • Initial security assessment training • Refresher security assessment training • Focussed security assessment training (e.g., new techniques, new tools) These assessments will be used to inform development of future security training.	M
R61	Agile systems and processes continuously refined and consistently improved.	Wherever possible, information will be collected once and re-used for other visa and border crossing checks.	M
R62	Simple, easy processes and systems, providing clear guidance and expectations for all staff and migrants	Information collection should be structured to capture enough information to uniquely identify migrants and to support exclusion of near-matches. This may include the capability to identify and "whitelist" migrants who have been previously screened and return false positives to security assessments.	S
R63	Removed	Redundant	
R64	Removed	Redundant	
R65	Removed	Redundant	
R66	Removed	Redundant	

Released under the Official Information Act 1982

Req No.	Outcome(s) Supported	Requirement Description	MoSCoW
R67	Removed	Redundant	
R68	Removed	Redundant	
R69	Simple, easy processes and systems, providing clear guidance and expectations for all staff and migrants	Migrants will have the ability to suspend and complete applications over several sessions.	S
R70	Removed	Redundant	
R71	Simple, easy processes and systems, providing clear guidance and expectations for all staff and migrants	Migrants will be able to easily withdraw or cancel applications. s6(c), s6(a) [redacted]	M
R72	Removed	Moved to NFRs	
R73	Removed	Redundant	
R74	Removed	Redundant	
R75	Removed	Redundant	
R76	Simple, easy processes and systems, providing clear guidance and expectations for all staff and migrants	s6(c), s6(a) [redacted]	S

Released under the Official Information Act 1982

Req No.	Outcome(s) Supported	Requirement Description	MoSCoW
R77	The system learns from itself and informs future changes/improvements	The system learns from itself and informs future changes/improvements	M

Released under the Official Information Act 1982

Appendix F Role of the Steering Group and Working Group

The Project Steering Group will support the project by:

- Providing guidance and direction to the project.
- Providing a governance group for project decision making, with the collective interest and success of the outcomes of the project in mind.
- Ensuring the initiative remains viable throughout its lifecycle.
- Ensuring acceptance of transitioned deliverables and achievement of benefits.
- Ensuring the project is aligned with wider organisational activities.
- Promoting the project within the organisations and with stakeholders.
- Identifying critical stakeholders that need to be actively engaged.
- Reviewing and agreeing change requests.
- Providing advice to the Business Owner and Project Manager.
- Making recommendations that will maximise benefits.
- Advising on project risk and issue management.
- Helping to ensure a successful handover from the project to business as usual.

Working group members are an interagency group responsible for:

- Specifying the needs of those who will use the project product(s) and monitoring that the solution will meet the needs of the users.

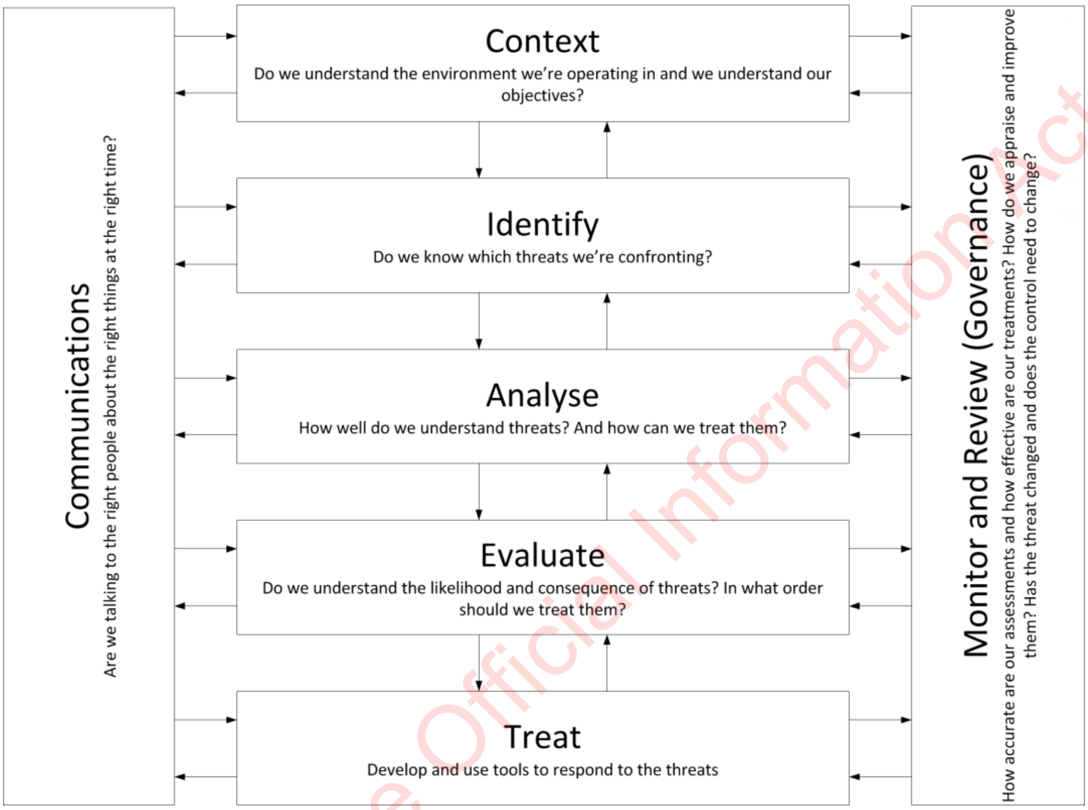
The Project Working Group will support the project by:

- Represents the interests of those who will use the project's final products (including operations and maintenance).
- Provides feedback and recommendations to the Project Manager, Business Owner and members of the Project Steering Group.
- Makes recommendations and highlights key issues to escalate to the Project Steering Group.
- Ensures that the project produces products will deliver the desired outcomes and meet user requirements.
- Contributes to the design and development of products.
- Contributes to product acceptance.
- Leads business readiness and defines operational hand-over.
- Briefs and advises the user community about the project.
- Oversees or undertakes quality assurance activities on behalf of the users.
- Participates in post implementation review.
- Identifies key decisions and issues requiring escalation to the project steering group.

Released under the Official Information Act 1982

Appendix G Model Diagrams

To aid understanding of the threat assessment model and how it works, consider the two following diagrams. Figure 1 is modified from the INZ Risk Operating Model (ROM) Framework. This high level view outlines the main components of how threats are managed. Please note this appendix is intended to provide information on how INSS will use the INZ ROM for risk modelling and how changes to risk indicators will be made. It is not intended to imply a separate risk management process to the INZ ROM process will be developed or implemented.



Communications
Are we talking to the right people about the right things at the right time?
Context
Do we understand the environment we're operating in and we understand our objectives?
Identify
Do we know which threats we're confronting?
Analyse
How well do we understand threats? And how can we treat them?
Evaluate
Do we understand the likelihood and consequence of threats? In what order should we treat them?
Treat
Develop and use tools to respond to the threats
Monitor and Review (Governance)
How accurate are our assessments and how effective are our treatments? How do we appraise and improve them? Has the threat changed and does the control need to change?

Figure 1: INSS Application of the INZ Risk Operating Model (ROM)

Context

Migrant-presented threat and NZ's response to that threat operates in a complex environment. We need to understand:

- The nature of threats presented by migrants and how those threats can be treated.
- s6(a) [redacted]
- The legal framework we operate in.
- The priority of identifying and responding to threats presented by migrants.

Identify

In order to treat a threat, that threat must first be identified. This includes:

- What is the source of the threat?
- What is the source of the information about the threat? Are the sources trustworthy / verifiable?
- Does the threat pose a security risk[11] to New Zealand or New Zealanders?

[11] As outlined under S4 and S16 of the Immigration Act, 2009

Released under the Official Information Act 1982

Analyse

After threats are identified, they must be analysed to understand:

- The nature of the threat.
- What options are potentially available to treat threat?
- What indicators are available to identify high-risk migrants?

Evaluate

Evaluation of a threat is determining how likely it is to occur and what the consequences of its occurrence are. Using this evaluation information, threats can be prioritised to inform development of candidate treatments for threats[12]. In turn, this prioritisation informs threat treatment investment decisions.

Treat

s6(c), s6(a)

[redacted]

Monitor and Review (Governance)

Governance is the monitoring and review of processes to ensure they are conducted in compliance with legislation and organisational policy and formal, delegated decision-making authority. The responsibility for INZs risk model rests with Risk and Verification and includes:

- Immediate oversight of processes by quality control of decisions made by INZ staff to ensure appropriateness and fairness of those decisions.
- Periodic quality assurance of migrant assessment processes and migrant decisions to ensure consistency.
- Regular audit of INZ processes to ensure compliance with legislation and policies.
- Decisions on changes of policies and processes to ensure fitness for purpose and compliance.

Communications

Communication is central to the success of the model shown in Figure 1 and ensures:

- Threat identification, analysis, prioritisation and treatment.
- Communications between all stakeholders is effective.

Figure 2 (below) provides a high level view of how this model works in practice. This diagram is not intended to provide a detailed view of how each step of the process works, or the define all of the system interactions planned by the project. It is intended to provide an illustrative, high level view of the interactions between INZ migrant types, processes and systems with INSS as an aid to understanding only...

[12] This process was followed in April and May in setting the initial 11 prioritised list of migrant risks to treat with INSS.

Released under the Official Information Act 1982

s 6 (a), s 6 (c)

Released under the Official Information Act 1982

Appendix I. Legislation that may have impacts on INSS

A number of Acts and Regulation has been identified that may have an impact on the future state operation of INSS. INZ must maintain compliance with these Acts.

The primary Act is the Immigration Act 2009. Other Acts that must be considered[13] are:

- Intelligence and Security Act 2017 (S13, S14, S190, Schedule 2)
- Terrorism Suppression Act 2002 (S4, S32, S38, schedules 1 – 5)
- Privacy Act 1993 (S6, S27, S57, Schedule 4A)
- Official Information Act 1982 (S6, S31)
- Customs and Excise Act 2018 (S51, S53, S207)
- Human Rights Act 1993 (S25, S129)
- Biosecurity Act 1993 (S107B, S142J)
- Policing Act 2008 (S9)
- Maritime Security Act 2004 (S59, S78)

Released under the Official Information Act 1982

[13] This list is not exhaustive, but provides a representative sample of Acts that must be complied with.