

1.3 Defect Summary

Acceptance Testing identified the 8 defects outlined in the table below, all have been closed. It is recommended to release Early BCU Changes with November 2020 Release.

Jira #	Summary	Severity	Priority	Resolution/Comment	Status
BCU-85	Nov Rel - State/province/region field from Online application is NOT populated in XRM (BirthCountryRegionStateText), DB16 and AMS(StateProvinceOfBirth)	3 Moderate	P3 Low	This is an existing issue from the AED project(existing production behaviour IM-1351)	Closed
BCU-86	NovRel - tIdentityOtherCitizenship.ID is not in order	4 Minor	P3 Low	This is not a defect. SQL caches upcoming ID numbers for performance.	Closed
BCU-87	Nov Rel - Identity not created in AMS when submitting a Daon Enrol with 30 Additional Citizenships or more	3 Moderate	P3 Low	This is not a defect. There is incorrect reference data in DAON Enrol.	Closed
BCU-88	NovRel - Adding Additional Citizenship from AED is not getting saved in tIdentityOtherCitizenship	2 Major	P2 Medium	DXC fixed and was retested and passed	Closed
BCU-89	NovRel - Addtl citizenship in tIdentityOtherCitizenship remains 'Inactive' after adding additional citizenship that was previously deleted in AED	3 Moderate	P3 Low	DXC fixed and was retested and passed	Closed
BCU-90	NovRel - Image does not sync to AMS when submit applications from IGMS Online	3 Moderate	P2 Medium	UAT environment issue. DXC has identified certificate has expired. Vodafone fixed and passed	Closed
BCU-91	Nov Rel - Updates from AED not reflected in AMS and can no longer be updated when adding TD Expiry to an identity that comes from DAON with Additional citizenship	3 Moderate	P3 Low	Existing production behaviour(IDMEONE-561)	Closed
BCU-92	NovRel - Online IGMS application not syncing in AMS	1 Critical	P1 High	Preprod environment issue. Datcom fixed and passed	Closed

1.4 Approvals



Early BCU changes
Test summary report



Early BCU changes
Test summary report



**MINISTRY OF BUSINESS,
INNOVATION & EMPLOYMENT**
HĪKINA WHAKATUTUKI

Test Exit Report

3285: BCU – Biometric Capability Update

Early Migration Business Context (DB16)

Release – 1.2

Version: V1.0 – Final

Date: 13th September 2021



1 Document Control

Document Information

Document Name:	MBIE BCU Release 1.2_ Test Exit Report
Contact Person:	s 9(2)(a)
Status:	V1.0

Document History

Author	Description of Change	Date	Version
s 9(2)(a)	Draft	26/08/2021	V0.1
	Updates after merge deployment into Pre prod	06/09/2021	V0.1
	Updates after merge deployment into Production	10/09/2021	V1.0 Final

Reviewed by

The following people have a formal quality assurance role with respect to this document.

Name	Role	Date
s 9(2)(a)		9/9/21
		9/9/21
		9/9/21
		9/9/21
		9/9/21
		9/9/21
		9/9/21
		9/9/21



Document Approval

Signatory	Signature	Date
s 9(2)(a)	 RE MBIE BCU Early Pre-Migration Business	13/09/2021
s 9(2)(a)	 RE MBIE BCU Early Pre-Migration Business	17/09/2021



2 Contents

1	Document Control	2
3	Introduction	5
3.1	Overview	5
3.2	Background.....	5
4	Executive Test Summary	6
4.1	Evaluation.....	6
4.2	High Level View	6
4.3	In Scope	7
4.3.1	Functional Requirements	7
4.4	Out of Scope for this document.....	8
5	Test Results	9
5.1	Overall Test Execution status	9
6	Defect Management	9
6.1	Defect status	9
7	Appendix	10
7.1	Test Results –Test Execution result details	10



3 Introduction

3.1 Overview

This document provides a summary of the tests that has been undertaken for the BCU Release 1.2 which is the combined IGMS and AMS changes. It is intended to summarise the

- Results of the Test Execution
- Issues discovered during the Test Phase

3.2 Background

Below is the high-level scope for BCU Release 1.2

As part of the early pre migration release the following code change required for Migration of the business context data from IGMS to AMS. Testing was completed against the combined IGMS and AMS changes.

The DB16 (Create Identity in AMS via IGMS) shall provide the relevant Business Context for each Identity created via the IGMS Online or ETA channels. The relevant Business context is as follows:

- Border - Referral
- Client Present – Lodgement
- Client Not Present
- Online Application
- New ETA



4 Executive Test Summary

The following section documents at a high-level view on the testing activities and responsibilities undertaken to test the BCU Release 1.2

4.1 Evaluation

The evaluation of the BCU Project test outcomes detailed in this document indicates that defined Test Exit Criteria as documented and agreed in the BCU Test Plan have been met as follows,

SIT Exit Criteria	Met/Not met	Comment/s
All planned tests have been executed.	Met	All planned functional Tests have been exercised at least once in one of the following environments UAT and Pre-Prod environments.
No open severity 1 or 2 defects.	Met	No open defects
Any remaining unresolved defects have been reviewed by the project team and business owners and an action plan put in place to accept or remediate.	Met	No open defects
Sev-3 aggregate impact overall is deemed acceptable	Met	No open defects
Test Summary Report completed	Met	This document

4.2 High Level View

- All planned functional Tests have been exercised at least once in one of the following environments UAT and Pre-Prod environments.
- Daon specific business context validation was run through test automation.
- Regression testing on the merged code with ADEPT was successfully tested in UAT and Pre-prod.
- No open defects
- SIT backfill deployment planned along with ADEPT release at a later stage.



4.3 In Scope

Below is the list of Requirements that will be delivered as part Release 1.2.

4.3.1 Functional Requirements

Requirement ID	Title
BCU-IGMS-FR15	Pass Business Context to AMS
ID2-028	Business context

4.3.1.1 Detail

The DB16 (Create Identity in AMS via IGMS) shall provide the relevant Business Context for each Identity created via the IGMS Online or ETA channels. The relevant Business context is as follows:

IGMS (BusinessContextTypeLookup)		AMS (tTriageSubmissionChannelType)
Description	s 6(c)	Description
Border - Referral		Border Referral
Client Not Present		NIST Upload
Client Present - Lodgement		In Person Enrolment
New ETA		New ETA
Online Application		Online Application



4.4 Out of Scope for this document

- Functional Requirements that are not part of the release 1.2
- Non-Functional Requirements not In Scope for Release 1.2.
- Security testing

5 Test Results

The table below represents the test cases prepared and executed and includes the results of the test execution activities.

5.1 Overall Test Execution status

Description	Test Type	Total	Planned	In progress	Passed	Failed	Blocked	Deferred	Not Run
BCU Release 1.2 - UAT	SIT	6	6	0	6	0	0	0	0
BCU Release 1.2 – Pre-Prod	SIT	6	6	0	6	0	0	0	0
Code Merge Redeployment with ADEPT Regression Testing – Pre-prod/UAT	SIT	12	12	0	12	0	0	0	0

6 Defect Management

6.1 Defect status

No Open Defects

7 Appendix

7.1 Test Results –Test Execution result details



Test Results_ Early
Release Pre-Migrator



**MINISTRY OF BUSINESS,
INNOVATION & EMPLOYMENT**
HĪKINA WHAKATUTUKI

Test Exit Report

3285: BCU – Biometric Capability Update

BCU and ADEPT code merge

Release – 2.0.0

Version: V0.1

Date: 17th November 2021



1 Document Control

Document Information

Document Name:	MBIE BCU Release 2.0.0_ Test Exit Report
Contact Person:	s 9(2)(a)
Status:	V1.0

Document History

Author	Description of Change	Date	Version
s 9(2)(a)	Drafted and issued for approval	17/11/2021	V0.1

Reviewed by

The following people have a formal quality assurance role with respect to this document.

Name	Role	Date
s 9(2)(a)		



Document Approval

Signatory	Signature	Date
s 9(2)(a)	 RE_APPROVAL PLSE_MBIE AMS-BCL	7/12/2021
s 9(2)(a)	 RE_APPROVAL PLSE_MBIE AMS-BCL	8/12/2021



2 Contents

1	Document Control.....	2
3	Introduction	5
3.1	Overview	5
3.2	Background.....	5
4	Executive Test Summary	6
4.1	Evaluation.....	6
4.2	High Level View	6
4.3	In Scope	7
4.3.1	Functional Requirements deployed and Feature flag set to enabled.....	7
4.3.2	Functional Requirements deployed and Feature flag set to disabled	25
4.4	Out of Scope for this document.....	40
5	Test Results	47
5.1	Overall Test Execution status	47
6	Defect Management	48
6.1	Defect status	48
6.2	Open Defect List.....	48
7	Appendix	49
7.1	BCU Test DashBoard – Azure Dev Ops	49



3 Introduction

3.1 Overview

This document provides a summary of the tests that has been undertaken for the BCU Release 2.0.0. It is intended to summarise the

- Results of the Test Execution
- Issues discovered during the Test Phase

3.2 Background

Below is the high-level scope for BCU Release 2.0.0

As part of the pre migration release following high level functionalities were deployed and tested in MBIE Non Production environments

- Channel Identity Creation for all identified business contexts
- DB 16 new data changes and AMS client update
- Fingerprint override settings
- Parse given name data rules
- Travel document type implementation

The functionalities deployed for this release have relevant feature flags set as below

Enabled – Code development completed, deployed into MBIE Non Production environment with the Feature flag set to “Enabled” i.e. the functionality is available to the end user and for testing.

Disabled - Code development completed, deployed into MBIE Non Production environment with the Feature flag set to “Disabled” i.e. the functionality is not available for the end user and cannot be tested.



4 Executive Test Summary

The following section documents at a high-level view on the testing activities and responsibilities undertaken to test the BCU Release 1.2

4.1 Evaluation

The evaluation of the BCU Project test outcomes detailed in this document indicates that defined Test Exit Criteria as documented and agreed in the BCU Test Plan have been met as follows,

SIT Exit Criteria	Met/Not met	Comment/s
All planned tests have been executed.	Met	All planned functional Tests have been exercised at least once in one of the following environments UAT and Pre-Prod environments.
No open severity 1 or 2 defects.	Met	No open Sev 1/2
Any remaining unresolved defects have been reviewed by the project team and business owners and an action plan put in place to accept or remediate.	Met	Defect S6(C) to AMS client performance is currently under monitoring with DXC
Sev-3 aggregate impact overall is deemed acceptable	Met	Defect to be assessed after performance test outcome scheduled under ADEPT project
Test Summary Report completed	Met	This document

4.2 High Level View

- All planned functional tests have been exercised at least once in one of the following environments SIT,UAT and Pre-Prod environments.
- Regression testing on the merged code with ADEPT and Residency Visa was successfully completed in Pre-prod.
- Functionalities with feature flag set to disabled will be tested in future BCU release when enabled.

4.3 In Scope

Scope items for this deployment is split into feature flag set to Enabled and Disabled

4.3.1 Functional Requirements deployed and Feature flag set to enabled

Requirement ID	Description	Feature Flag
s 6(c)	Biographics Definition For the purposes of other requirements Biographics is defined as any data within the s 6(c) tables within AMS	Enabled
	Travel Document Definition For the purposes of other requirements Travel Document is defined as any data within the s 6(c) tables within AMS	Enabled
	Address Definition For the purposes of other requirements Address is defined as any data within the s 6(c) table within AMS	Enabled
	Family Relationships Definition For the purposes of other requirements Family Relationships is defined as any data within the s 6(c) table within AMS	Enabled
	Family Text Definition For the purposes of other requirements Family Text is defined as any data within the s 6(c) table within AMS	Enabled

s 6(c)	New Data in DB16 from IGMS s 6(c)	Enabled
	Town/City of Birth Passed to AMS from IGMS s 6(c)	Enabled
	Other Citizenships Passed to AMS from IGMS s 6(c)	Enabled
	Province/State of Birth Passed to AMS from IGMS s 6(c)	Enabled
	Display of Identity Data s 6(c)	Enabled



s 6(c)	AMS Image Capture Edit s 6(c)	Enabled
	AMS Image Capture Addition or Deletion s 6(c)	Enabled
	Edit Identity Data Security Settings s 6(c)	Enabled
	Identity Delete Verification s 6(c)	Enabled

s 6(c)	Visa Application Creation from IGMS s 6(c)	Enabled
	Additional Fields from IGMS s 6(c)	Enabled
	Create Identity via IGMS s 6(c)	Enabled
	Client Number Response to IGMS s 6(c)	Enabled
	Identity Fingerprint Flag Removal s 6(c)	Enabled



Error! Unknown document property name.

s 6(c)	New AMS Officer for IDme System Use s 6(c)	Enabled
--------	---	---------

s 6(c)	Ineligibility Status Additions s 6(c)	Enabled
	Ineligibility Status per Identity s 6(c)	Enabled
	Ineligibility Status Reasons s 6(c)	Enabled
	Ineligibility Status Schema s 6(c)	Enabled
	Online Application Channel Identity Creation s 6(c)	Enabled

s 6(c)	MFAT Channel Identity Creation s 6(c)	Enabled
	MFAT Channel Identity Creation Trigger s 6(c)	Enabled
	Online Services Channel Identity Creation s 6(c)	Enabled
	Online Services Channel Identity Creation Trigger s 6(c)	Enabled
	ETA Channel Identity Creation s 6(c)	Enabled
	ETA Channel Identity Creation Trigger s 6(c)	Enabled

s 6(c)	Citizenship Confirmation Channel Identity Creation s 6(c)	Enabled
	Citizenship Confirmation Channel Identity Creation Trigger s 6(c)	Enabled
	Interpol Alerts Channel Identity Creation s 6(c)	Enabled
	Interpol Alerts Channel Identity Creation Trigger s 6(c)	Enabled
	Passport Scan Channel Identity Creation s 6(c)	Enabled
	Passport Scan Channel Identity Creation Trigger s 6(c)	Enabled

s 6(c)	Border Referral Channel Identity Creation s 6(c)	Enabled
	Border Referral Channel Identity Creation s 6(c)	Enabled
	NIST Upload Channel Identity Creation s 6(c)	Enabled
	NIST Upload Channel Identity Creation Trigger s 6(c)	Enabled
	ADEPT Channel Identity Creation s 6(c)	Enabled
	ADEPT Channel Identity Creation Trigger s 6(c)	Enabled
	IGMS Business Context Mapping s 6(c)	Enabled

s 6(c)	AMS New Identity Channel Identity Creation s 6(c)	Enabled
	AMS New Identity Channel Identity Creation Trigger s 6(c)	Enabled
	In Person Enrolment Channel Identity Creation s 6(c)	Enabled
	In Person Enrolment Channel Identity Creation Trigger s 6(c)	Enabled
	Border Movement Channel Identity Creation s 6(c)	Enabled
	Border Movement Channel Identity Creation Trigger s 6(c)	Enabled



s 6(c)	BDC Bulk Upload (VACs) Channel Identity Creation s 6(c)	Enabled
	BDC Bulk Upload (VACs) Channel Identity Creation Trigger s 6(c)	Enabled
	Multiple Client Movements s 6(c)	Enabled
	Fingerprint Override Security Setting s 6(c)	Enabled
	Fingerprint Override Verification s 6(c)	Enabled

s 6(c)	Fingerprint Override Execute Move s 6(c)	Enabled
	Fingerprint Override Cancellation s 6(c)	Enabled
	<u>Fingerprint Override Invalid User</u> s 6(c)	Enabled
	Fingerprint Override Not Set in DB17 s 6(c)	Enabled
	Fingerprint Override Move from DB17 s 6(c)	Enabled
	Client Move Advice to IGMS s 6(c)	Enabled

	S 6(c)	
S 6(c)	Parsing Given Name Data from 4 to 3 Fields S 6(c) 	Enabled
	Parsing Given Name Data Rules S 6(c) 	Enabled
	Given Name Data Truncation S 6(c) 	Enabled



Error! Unknown document property name.

S 6(c)	Remove the Reference to IGMS from Warning Descriptions S 6(c)	Enabled
	Travel Document Type Selectable S 6(c)	Enabled

s 6(c)	Receive Travel Document Type from IGMS s 6(c)	Enabled
	Receive Travel Document Type from IGMS - Update s 6(c)	Enabled



s 6(c)	Send Travel Document Type to IGMS s 6(c)	Enabled
	Searchable Image Dialog Screen Wording Change s 6(c)	Enabled
	Fingerprint Identities Security Setting s 6(c)	Enabled

s 6(c)	Fingerprint Identity Edit Invalid User s 6(c)	Enabled
	Fingerprint Identity Edit/Link Security Setting Request s 6(c)	Enabled
	Feature Flags/Switches for IGMS/NEC s 6(c)	Enabled

s 6(c)	Feature Flags/Switches for AMS s 6(c)	Enabled
	Feature Flags/Switches for Redirection to IGMS s 6(c)	Enabled
	Feature Flags/Switches for Change History Viewing s 6(c)	Enabled

4.3.2 Functional Requirements deployed and Feature flag set to disabled

Following requirements were deployed in the MBIE Non Production environment with the Feature Flag set to disabled and hence not tested. These functional requirements will be tested on the Feature Flag is set to Enabled.

Functional Requirement	Description	Code State
s 6(c)	Client Details Editing s 6(c)	Disabled
	Travel Document Editing s 6(c)	Disabled

	s 6(c)	
s 6(c)	Travel Document Double Click s 6(c)	Disabled
	Address Editing s 6(c)	Disabled
	Address Double Clicking s 6(c)	Disabled
	Family Details Editing s 6(c)	Disabled

s 6(c)	Face Image Loading s 6(c)	Disabled
	Non Passport Scan Face Images to EAG s 6(c)	Disabled
	Images from Passport Scans s 6(c)	Disabled
	Images Failing PQC s 6(c)	Disabled
	Images for AMS Display s 6(c)	Disabled
	Town/City of Birth Addition s 6(c)	Disabled

	s 6(c)	
s 6(c)	Town/City of Birth Editing s 6(c)	Disabled
	Other Citizenships Addition s 6(c)	Disabled
	Remove an Other Citizenship s 6(c)	Disabled



Error! Unknown document property name.

	s 6(c)	
s 6(c)	Adding an Other Citizenship s 6(c)	Disabled

	s 6(c)	
s 6(c)	Cancel Adding an Other Citizenship s 6(c)	Disabled
	Province/State of Birth Addition s 6(c)	Disabled

s 6(c)	Province/State of Birth Editing s 6(c)	Disabled
	Add Face Image through Image Manager s 6(c)	Disabled
	Identity Deletion Message to EAG s 6(c)	Disabled
	Identity Creation Message to EAG s 6(c)	Disabled
	New Identity Creation Message from IPE s 6(c)	Disabled
	s 6(c)	Disabled
	New Identity Images s 6(c)	Disabled
	DB02 API Call to EAG s 6(c)	Disabled



Disabled

6(c) of the OIA

	s 6(c)	
--	-------------------	--

s 6(c)	Logical Identity Deletion s 6(c)	Disabled
	Create Identity via AMS s 6(c)	Disabled
	New Fields to NEC s 6(c)	Disabled
	New Fields API Schema s 6(c)	Disabled
	Identity Updates via AMS s 6(c)	Disabled
	Client Linking via AMS s 6(c)	Disabled

s 6(c)	Client Linking via IDMe to IGMS s 6(c)	Disabled
	Identity Resolution Status s 6(c)	Disabled
	Client Linking from Identity Resolution s 6(c)	Disabled
	Inconclusive Identity Resolution Warning s 6(c)	Disabled
	Stop Travel Document Deletion Ending s 6(c)	Disabled

s 6(c)	Suspected Fraudulent Identity Warning Ending s 6(c)	Disabled
	Passport Scan Result Update Warning Ending s 6(c)	Disabled
	6(c) of the OIA	Disabled
	Update Identity Details Ending s 6(c)	Disabled
	Image Sharing Ending s 6(c)	Disabled
	Identity Audit Trigger s 6(c)	Disabled
	Identity Audit Data s 6(c)	Disabled

s 6(c)	Online Application Channel Identity Creation Trigger s 6(c)	Disabled
	Channel Identity Creation to EAG s 6(c)	Disabled
	"Stickiness" Rules Removal s 6(c)	Disabled
	Client Move Advice to NEC and IGMS s 6(c)	Disabled
	Block ETA Identities from Being Edited s 6(c)	Disabled



s 6(c)	Identity Change History Data Access s 6(c)	Disabled
	Identity Change History Data Viewing s 6(c)	Disabled
	Identity Change History Data Viewing - No Data Editing s 6(c)	Disabled
	Identity Change History Data Viewing - Default Browser s 6(c)	Disabled



4.4 Out of Scope AMS requirements for this release

Below AMS Functional Requirements are Not In Scope for this release and will be part of the future planned release.

No	Description
s 6(c)	Travel Document Editing Data Validation
	s 6(c)
	Address Editing Data Validation
	s 6(c)
	Image Sizing
	s 6(c)
	Image Caching
	s 6(c)

s 6(c)	Image Sizing - Remove Restriction s 6(c)
	Non Passport Scanned Images s 6(c)
	Additional Image Types s 6(c)



s 6(c)	Fingerprints Not Displayed s 6(c)
	Primary Image Management s 6(c)
	Image Display Management s 6(c)
	Other Citizenships not Primary Citizenship s 6(c)
	Edit a Face Image Meta Data s 6(c)
	Image Type Change - Face to Non-Face s 6(c)
	Image Type Change - Non-Face to Face s 6(c)

s 6(c)	Delete a Face Image located in IDMe s 6(c)
	Image Type Change - Confirmation s 6(c)
	New Identity Creation Message from IPE - Format s 6(c)
	In Person Enrolment Biometric Capture Note Type s 6(c)
	IPE Step Skip Reason Note s 6(c)
	Client Number Provision for IPE and Fingerprint Identities s 6(c)
	Application Numbers to NEC s 6(c)
	API Call Ordering from AMS to NEC s 6(c)

s 6(c)	s 6(c)
	API Call Ordering from AMS to NEC same API Call Type
	s 6(c)
	DB02 Deletion API Call to EAG
	s 6(c)
	Handling of API Error Responses
	s 6(c)
	Handling of Identities Created from a DB16a Message
	s 6(c)
	Image Deletion Upon Identity Resolution
	s 6(c)
	Task Number Included in Identity Resolution Message
	s 6(c)
	Multiple Identity Resolution Messages
	s 6(c)

s 6(c)	DB01 Message Replication s 6(c)
	Add Identity Fingerprint Flag Ending s 6(c)
	Ineligibility Status Country Field Transformation s 6(c)
	Ineligibility Status Additional Fields Changes s 6(c)
	Identity Image Meta Data Audit Trigger s 6(c)
	Identity Image Add/Delete Audit Trigger s 6(c)
	Edit Identity Channel s 6(c)

s 6(c)	Edit Identity Channel Trigger s 6(c)
	Include NEC Task Number in Warning Note s 6(c)
	ETA Identities Message s 6(c)

5 Test Results

The table below represents the test cases prepared and executed and includes the results of the test execution activities.

5.1 Overall Test Execution status

Description	Total	Passed	Failed	Blocked	Deferred	Not Run
BCU Release 1.2 - UAT	126	81	0	0	0	45
Regression Test	6	5	1	0	0	0
Total	132	86	1	0	0	45

All No Run Test cases are related to the Functional Requirements with Feature flags set to disabled.

6 Defect Management

6.1 Defect status

Below table represents the defects raised during release 2.0.0 and its current state

Row Labels	3 - Medium	4 - Low	Grand Total
Closed	12	1	13
Proposed	1		1
Grand Total	13	1	14

6.2 Open Defect List

Defect ID	Type	Description	Status	Severity	Priority
s 6(c)					

s 6(c)

7 Appendix

7.1 BCU Test DashBoard – Azure Dev Ops

6(c) of the OIA

7.2 BCU Test cases and results

6(c) of the OIA

7.3 BCU AMS Requirement -> Test Case Traceability report



BCU AMS Test Case -
Requirement traceability

7.4 All Defect list – Release 2.0.0

ID	Work Item Type	Title	State	Severity	Priority
s 6(c)					

s 6(c)



s 6(c)





**MINISTRY OF BUSINESS,
INNOVATION & EMPLOYMENT**
HĪKINA WHAKATUTUKI

IN-CONFIDENCE



3644 Biometric Capability Update

Non-Functional Test Plan

Version 1.1

Date: 07 March 2023



Contents

Contents.....	2
Document control.....	3
1.1. Version history.....	3
1.2. Approved by	3
1.3. Reviewed by	3
1.4. Distribution.....	4
1.5. Reference documents	4
2. Project Overview	6
Biometric Capability Update (BCU)	6
3. Test Scope.....	8
3.1. In Scope	8
3.2. Out of scope requirements	20
4. Test Approach	23
4.1. High Level Test Approach	26
4.2. Architecture / Design Verification	41
4.3. Process Verification	41
4.4. Verification of System Behaviour	41
4.5. Test Traceability	44
5. Entry, Exit and Suspension Criteria	45
5.1. Entry Criteria	45
5.2. Exit Criteria	46
5.3. Suspension Criteria.....	48
5.4. Test support.....	48
6. Defect Management	49
7. Assumptions, Dependencies & Risks	51
8. Test environments	53
8.1. Identity Test Environment Usage	53



Document control

1.1. Version history

Date	Version	Author	Description of change
17/12/2021	0.1	s 9(2)(a)	Initial creation
10/10/2022	0.2		Update In Scope Items
13/10/2011	0.3		Review and Update Test Approach and NFR Treatments
26/10/2022	0.4		Added some more NFRs & reference from NEC IPE Hardware Requirement
28/11/2022	0.5		Moved NFR10, NFR11, NFR12, NRF13 & NFR20 from "Out of scope" to "In scope"
13/12/2022	1.0		Final
06/03/2023	1.01		Incorporated review comment from Bob Marshall
07/03/2023	1.1	s 9(2)(a)	Signed off – Final version

1.2. Approved by

Name	Role	Organisation	Date	Signature
s 9(2)(a)		MBIE	06/03/2023	 RE_ Reminder_ BCU Non -Functional Tes
		MBIE	22/12/2022	 RE_ BCU Non -Functional Test Plai

1.3. Reviewed by

The following people have a formal quality assurance role with respect to this document.

Name	Role	Organisation
s 9(2)(a)		MBIE



Name	Role	Organisation
s 9(2)(a)		MBIE
		MBIE
		MBIE
		MBIE

1.4.Distribution

The following people / groups have been sent a copy of this document (list excludes approvers, reviewers, and consulted).

Name	Role	Organisation	Date and Version
All Vendors			
s 9(2)(a)			

1.5. Reference documents

The following documents contain the detailed migration requirements, which are not repeated in this document.

Title	Version	Date	6(c) of the OIA
NEC BCU Non-Functional Requirements v1.0 APPROVED	1.0	04/05/2021	
NEC BCU NFR Support Data	1.0	04/05/2021	
MBIE BCU Functional Test Plan	1.0	27/10/2022	
Nagios Operating System Monitoring Profiles		05/09/2022	
MBIE NEC IDME Solution Design Document		18/08/2022	
MBIE IPE Detailed System Design Document	3.7	12/08/2022	



6(c) of the OIA

Title	Version	Date
In-Person Enrolment (Part A) FINAL	1.3	23/04/2020
BCU Architectural Solution Design Part A – FINAL	1.5	10/08/2021
BCU Infrastructure Design (Part B)	4.0	3/08/2022
NEC IPE Hardware Requirements	2.2	17/03/2022
Disaster Recovery Plan (Pending)		
Technical Operation Manual		
Support Operation Manual		
Security Test Plan/Approach		
BCU Performance Test Plan		

Note: The highlighted documents are not available at the time of finalizing this document.



2. Project Overview

Biometric Capability Update (BCU)

The Identity Management solution (IDme) provides INZ with the capability to be the authoritative source of identity information for all non-New Zealanders.

The Biometric Capability Update has been designed to address INZ projects needs and future known capability by upgrading the versions of biometric, biographic matching and management platforms, rationalising, and simplifying the platform to reduce on-going cost and improving the flexibility and utility of the system in the process. This is a core capability for INZ's future protection in an environment where identity fraud, terrorism and other sources of harm are prevalent and increasingly diverse and sophisticated, and this upgraded capability is crucial to achieving that future.

s 6(c)

Identity Management Components





3. Test Scope

3.1. In Scope

s 6(c)



3.1.1. Requirements

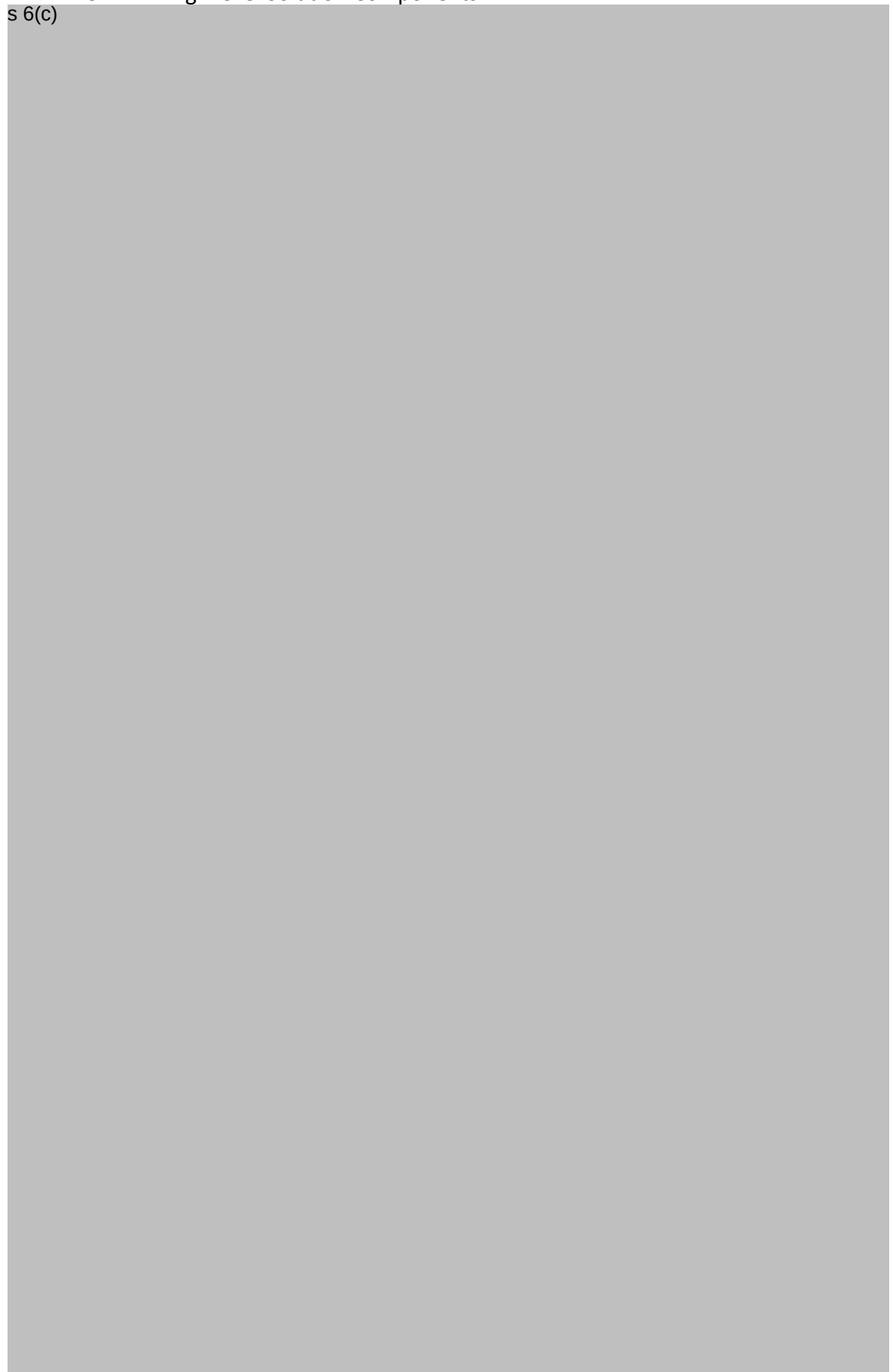
s 6(c)





3.1.2. High level Solution Components

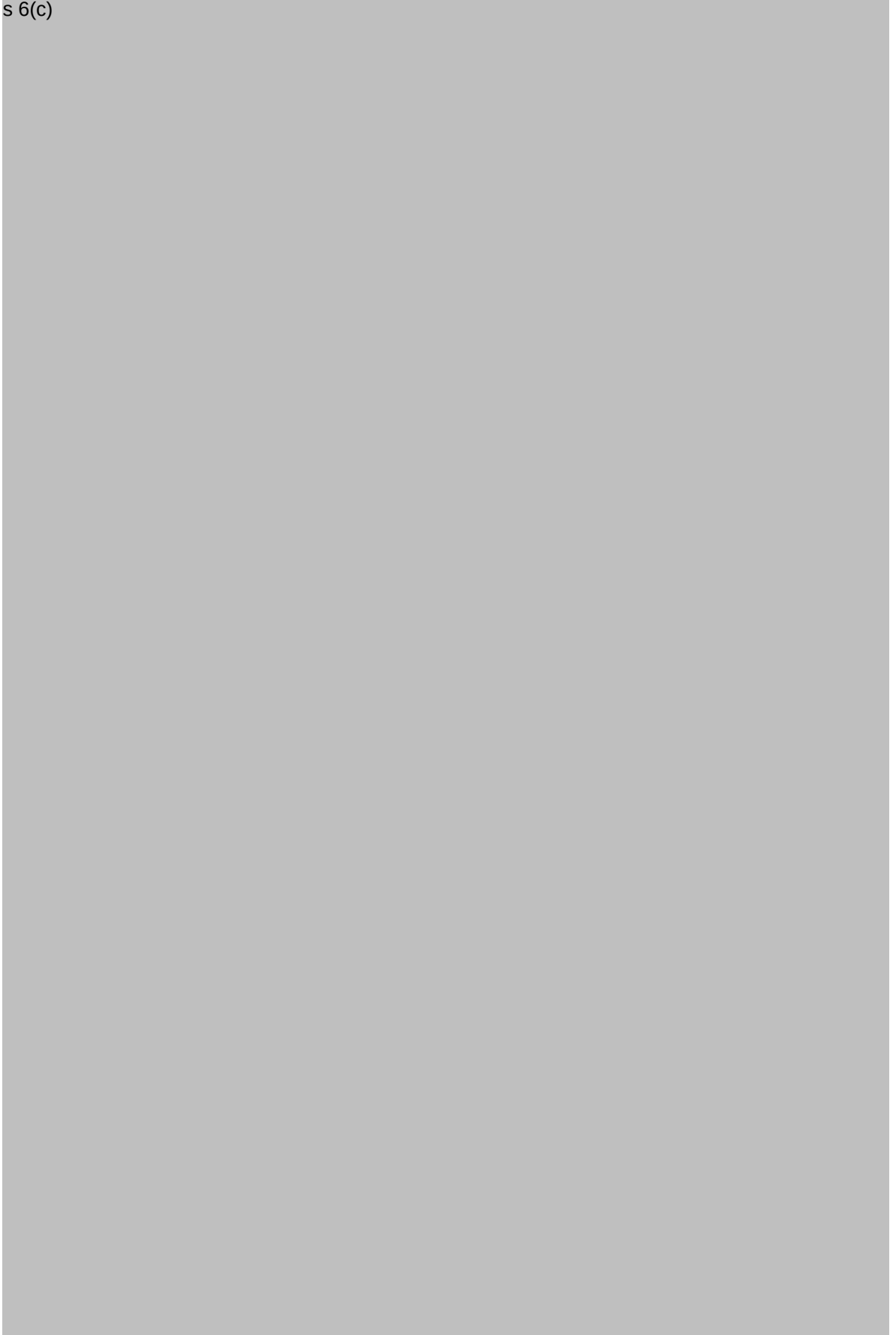
s 6(c)





3.1.3. System Integration

s 6(c)





3.1.4. Test Phases

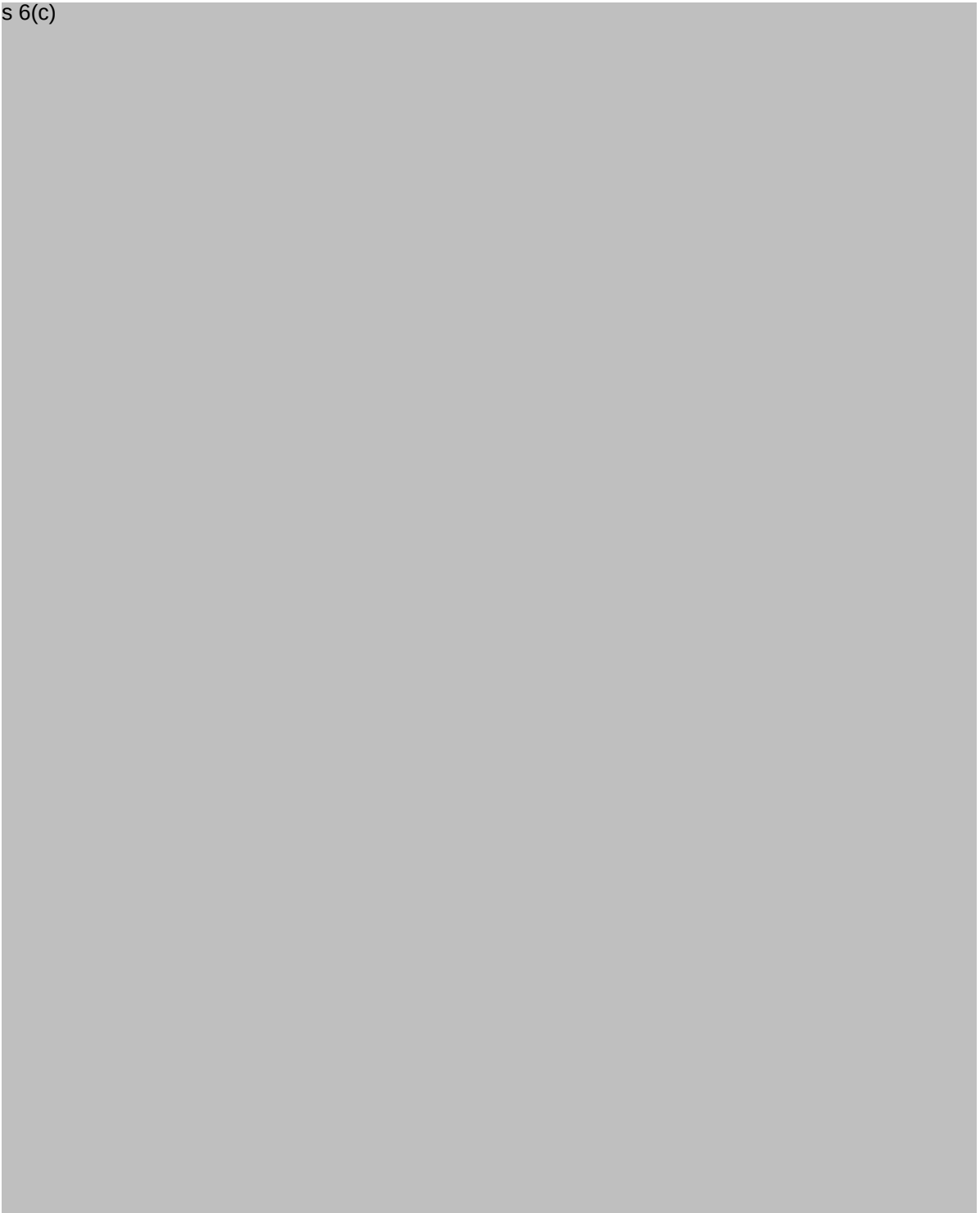
The table below describes each of the test phases included within the scope of testing. The different test types are discussed in detail in Section 3.3.3.

Test Phase	Description
Systems Integration Testing	NFR testing is to be undertaken on an integrated environment – UAT Environment. Evidence of test results from this stage will be presented for approval. More details about test phases and environment details are covered in section 6.1



3.2. Out of scope requirements

s 6(c)





4. Test Approach

This section describes the overall testing approach to be undertaken for Non-Functional testing that will be performed on items within the scope defined.

The figure below presents an overview of the process in which NFRs are progressively addressed through the project life cycle to the High-Level Test Approach.

- NFRs are built into the Architecture and Design Artefacts, where NFR Treatments are defined.
- For each of the treatments, work has been undertaken to identify an appropriate NFR Acceptance Approach.
- Following on from this, a High-Level Test Approach has been defined for each of the treatments, aligned with the relevant acceptance approach.
- For context, the high level NFR Acceptance activity is also shown.

The following sections provide further details around these activities, including details of test scenarios within each of the high-level test approaches and the expected approach to acceptance.

s 6(c)



For each of the relevant NFRs identified within the scope of BCU Solution, a solution treatment will be implemented / applied to satisfy the NFR.



4.1.High Level Test Approach

s 6(c)





4.2. Architecture / Design Verification

s 6(c)



4.3. Process Verification

s 6(c)



4.4. Verification of System Behaviour

s 6(c)





4.5. Test Traceability

Test scenarios will be traced back to the detailed non-functional requirement document. Below is the link for the Non-Functional Test Team's test scenario matrix:



BCU NFR Test
Traceability Report.x



5. Entry, Exit and Suspension Criteria

The following table describes the quality controls that will be implemented via the agreed entry and exit criteria for BCU Non-Functional Testing.

5.1.Entry Criteria

Short Description	Long Description
NEC Solution Design Documents Sign-off	The NEC Solution Design Documents must be approved prior to NFR testing
Approved Non-Functional Requirements	Non-Functional requirements must be approved prior to NFR testing.
MBIE Architecture Specs Sign-off	The MBIE Architecture specs- Part A/B, Infrastructure specs must be approved prior to NFR testing
NFR Test Plan Sign-off	The NFR test plan must be approved prior to NFR testing
DR Test Plan Sign-off	The DR test plan must be approved prior to DR Testing
Security Test Plan Sign-off	The Security test plan must be approved prior to starting Security Testing
Performance Test Plan Sign-off	The Performance test plan must be approved prior to starting Performance Testing
Test Cases Completed	Test cases associated with testing have been completed
Test Environments	Test environments are available and have passed smoke testing.
NFR Traceability	Evidence of traceability of NFR requirements – currently expected to be represented by Requirement to Test case links in MBIE ADO .
NEC Systems Testing	In scope NFR test execution has been completed. Defects associated with NFRs are clearly presented, including their impact to the solution, and compliance to Project NFR requirements.
Hardening	Application / Platform Security hardening has been completed prior to start of NFR testing.
Defects associated to Functional testing	All Sev 1 & Sev 2 defects have already been fixed prior to start of NFR testing.



Short Description	Long Description
System Traceability Testing	System Traceability, including logging, auditing, and exception handling design is defined and implemented, and tested/verified.
Test Resource Availability	Appropriate business resources are available
	Appropriate technical resources are available
Technical / Operational Procedures Supporting Test Execution	DR Technical Run plan should be available and approved prior to DR Testing. Change & Release Management Procedures should be available prior to Deployment Testing. Backup & Restore Procedures should be available prior to Backup & Restore Testing.
BCU Project Environment Handover Checklist	BCU Project Environment Handover Checklist is complete and provided to the Non-Functional Test team.

5.2.Exit Criteria

The following conditions will need to be met for test execution to be considered complete:

Short Description	Long Description
Test Coverage	100% coverage of agreed non-functional testing completed as outlined in the test plan. Where certain tests are not executed, a gap analysis is completed to identify and assess risks and a solution is agreed.
Test Results	All test results, supporting artefacts, defects and issues have been recorded and clearly presented to all appropriate parties for review and analysis against acceptance criteria
Defects	100% resolution of severity 1 & 2 non-functional testing defects
	An agreed action plan is completed for non-critical non-functional testing failures
Test Results Approval	The Project Stakeholders have approved testing outcomes and that that no further testing is required





5.3.Suspension Criteria

The following conditions define circumstances when test execution may be suspended:

Short Description	Long Description
Environment Availability	The application/environment is identified as unstable, or unavailable
Significant Defects/Rework	Incorrect functionality/configuration of a core component, that requires significant investigation, prevents further testing
	Significant design changes are required that prevent further testing
Resource Availability	Absence of critical technical / support resource or SME to resolve an issue or a defect.

Testing will resume when the condition(s) encountered above is/are resolved.

5.4.Test support

Non-functional testing activity will need support for the following activities

- Infrastructure Support team to take certain server administrator level action e.g., take some server down, failover the server, etc.
- Support from Solution Architect (MBIE and Vendors) to determine / identify issues, in some cases.
- Disaster Recovery setup is only available in Production environment and hence it will be exercised in Production environment prior to Go-Live. This activity will rely on support from Infra support team and Architect. This exercise depends on the Disaster Recovery Plan document (waiting for document to be produced).



6. Defect Management

Defect Management processes will follow MBIE BCU Defect management process

All open System defects from the vendors will be logged in MBIE ADO repository when MBIE SIT testing commences.

MBIE defects will be logged into ADO with Severity and Priority ratings. When the defect is reviewed by the Defect Triage Committee the ratings may be reset. Defect meetings will be scheduled by the BCU Test Manager and will be run twice a week

6.1. Severity

Severity level refers to the degree that the defect impacts or affects the system.

The impact of the defect on the application (system-wide, one module, single function) as well as the impact on the business or technical environment is also considered when assigning a severity.

Defect Severity Level	Description
Critical	A termination of the complete system or one or more components of the system and causes extensive corruption of the data. The failed function is unusable and there is no acceptable alternative method to achieve the required results.
Major	A termination of the complete system or one or more components of the system and causes extensive corruption of the data. The failed function is unusable but there exists an acceptable alternative method to achieve the required results.
Moderate	A defect that does not result in the termination, but causes the system to produce incorrect, incomplete or inconsistent results then the severity will be stated as moderate.
Minor	A defect that does not result in termination and does not damage the usability of the system and the desired results can be easily obtained by an acceptable work around.
Cosmetic	A defect that is related to the enhancement of the system where the changes are related to the look and feel of the application then the severity is stated as cosmetic.



6.2. Priority

Priority defines the order in which we should resolve defects. It is set by the tester as an indication of how quickly a resolution is required, usually to support the test execution timeframes.

Priority	Description	Response Time
High	Must be resolved as soon as possible because the defect is severely affecting the application or the product or business reputation. The system cannot be used until the repair has been done.	2 hours
Medium	The defect should be resolved in the normal course of development activities. It can wait until a new build or version is created.	New release
Low	The defect is an irritant which should be repaired, but repair can be deferred until after more serious defects have been fixed.	Planned release



7. Assumptions, Dependencies & Risks

The following assumptions, dependencies and risks have been considered in the production of this Test Plan:

Assumptions

No.	Assumptions	Impact
1	Testers will have sole use of test environment for duration of the testing schedule, unless specifically agreed by the project and Test Manager. In case of unavailability of the environment, testing may need to be performed outside normal office hours.	Other testing may impact NFR test results so must not occur while NFR test is under way. Testing outside normal working hours would add cost to project and restricts testing progress.
2	Resource availability – from MBIE test team, NEC, Datacom, Vodafone, Argonaut, Intech, Theta and DXC teams are available throughout testing window	Resource unavailability may mean delays to test schedule
3	The IGMS system & AMS are not within the scope of NFR Testing under this test plan. However, the performance impact on those systems is to be included under the Performance Test Plan.	This assumption controls test scope
4	Any required access to test environments will be provisioned before NFR testing is scheduled to start	Lack of access will introduce delays to NFR testing

Dependencies

No.	Dependencies	Consequence
1	System testing has met the agreed acceptance criteria	Delay to test schedule
2	A stable test environment	Delay to the test schedule while corrective action is made
3	Available time to work on project deliverables	Delay to completion of project deliverables
4	Environment / Server access for test resources	Delay to the test schedule while access is provisioned

Risks

No.	Risk	Impact
1	Other projects impact environment availability	Delay to testing schedule
2	Late scope changes could delay timeline	Delay to testing schedule
3	Delayed completion of System Integration Testing may impact the start date of NFR testing	Delay to testing schedule
4	Support from vendors not provided or of limited availability	Possible delay to testing schedule



No.	Risk	Impact
5	Delay in Process / Policy / Operations related documents	Possible delay to testing schedule



8. Test environments

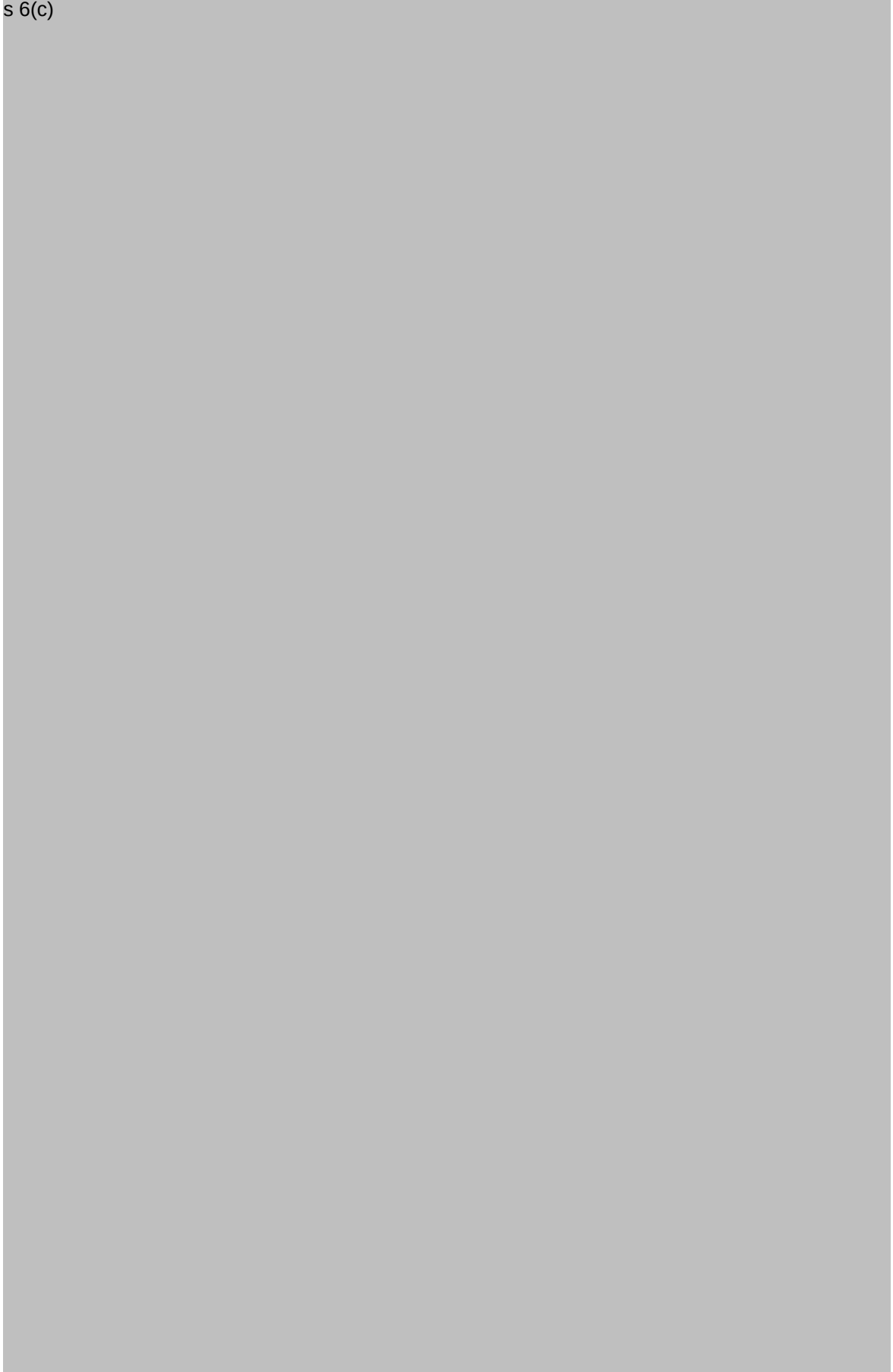
8.1.Identity Test Environment Usage

s 6(c)





s 6(c)





**MINISTRY OF BUSINESS,
INNOVATION & EMPLOYMENT**
HĪKINA WHAKATUTUKI



BCU – Biometric Capability Update

Test Strategy

Version: 2.0.1 Final

Date: 27/10/2022



1. Document control

Version history

Date	Version	Author	Description of change
23/09/2020	V1.0	s 9(2)(a)	Final
14/10/2022	V1.1		Multiple updates across the document after Requirements are finalised
27/10/2022	V2.0		Updated with review MBIE review Feedback. Final
2/05/2023	V2.0.1		Corrected date on cover pages. (was showing as approved in 2023) – Not needing redistribution

Reviewed by

The following people have a formal quality assurance role with respect to this document

Name	Role	Date
s 9(2)(a)		7/10/2022
		7/10/2022
		7/10/2022
		7/10/2022
		7/10/2022

Note: Due to the change in approach the Test Strategy has been resent out for a full review. The dates above reflect this date.

Test Strategy Signoff

The signatories below have reviewed this document and agree it is a fit-for-purpose statement of the testing objectives, processes, and strategies to be used for the Biometric Capability Update (BCU).

The following signatures indicate approval and acceptance of this document, subject to any caveats below:

Name	Title	Signed
s 9(2)(a)		Signed : _____ Date : ____ \ ____ \ ____

Distribution

The following people/groups have been sent a copy of this document (list excludes approvers, reviewers, and consulted):

Name	Role	Date
s 9(2)(a)		



Name	Role	Date
s 6(c)		

Contents

1. Document control	2
Version history.....	2
Reviewed by	2
Test Strategy Signoff.....	2
Distribution.....	2
2. Overview	6
Purpose.....	6
Context	6
Documents Referenced	6
Project Overview.....	7
3. Test Overview	11
Objectives of Testing / Critical Success Factors	11
Test Principles	11
4. Test Scope	12
Test Level and Types	12
End to End BCU IDmes Solution	13
In Scope	14
Out of Scope	19
5. Test Approach.....	20
Smoke testing.....	24
System Testing	27
Migration.....	29
System Integration Testing.....	33
Performance Testing	39
Business Acceptance Testing	40
Business Verification Testing.....	41
Test Management Tools	42
Test Execution Schedule.....	42
Test Wrap up.....	42
Deliverables.....	42
Test Suspension Criteria	43
6. Test Team Structure and Roles	44
Roles and Responsibilities.....	44
7. Testing Schedule and Environments	47
Testing Milestones	47
Test Environments	47
8. Test Management Procedure	49
Test Progress Reporting	49
Defect Management.....	49
9. Assumptions & Dependencies; Risks and Issues	51
Assumptions	51
Dependencies	51
Risks	51



Issues	53
Appendix A: Test Types	54
Appendix B: Functional Requirements In-Scope	56

2. Overview

Purpose

This document contains details of the testing to be completed for BCU and IPE. It should be used to inform relevant parties of testing details to review and understand the involvement from the different teams, resources, vendors and expected artefacts and deliverables for the project.

This is a static document to provide information at this stage of project planning. All changes during the execution phases of the project will be managed by the project using accepted change processes. Changes to testing will be logged and recorded in the Test Summary/Exit reports at the end of Test Execution.

Context

This Test Strategy is produced as part of the ITG Project Delivery Model 'Build/Test' phase for the BCU & IPE Projects.



Documents Referenced

Further information on the project can be found as follows:

Document title	Version	Date	Location / ID
NEC IDMe Business Requirements	1.3	18/06/2021	s 6(c)
NEC IPE Functional Specification	2.4	17/05/2021	
NEC IPE Hardware Requirements	2.1	1/06/2021	
NEC BCU Non Functional Requirements	1.0	06/05/2021	
NEC BCU NFR Support Data	1.0	04/05/2021	
AMS Changes Detailed Requirements	0.7	19/07/2021	
Argonaut SRTP Business Requirements	6.8	2/07/2021	
InTech IQOffice Business Requirements	0.9	19/07/2021	
Datacom IGMS BCU Business Requirements	0.7	19/07/2021	
Theta BCU Azure Business Requirements	0.3	15/07/2021	
In-Person Enrolment (Part A) FINAL	1.3	23/04/2020	
BCU Architectural Solution Design Part A – FINAL	1.5	10/08/2021	
s 6(c)		11/08/2021	
AMS BCU External Concurrency Design	v93	08/09/2021	
AMS BCU Additional Features Design	v3	01/10/2021	
AMS BCU Detailed Design AMS and SIH	1.0	28/07/2021	
BCU Infrastructure - SIT Solution Design Infrastructure Part B	3.6	10/5/2022	



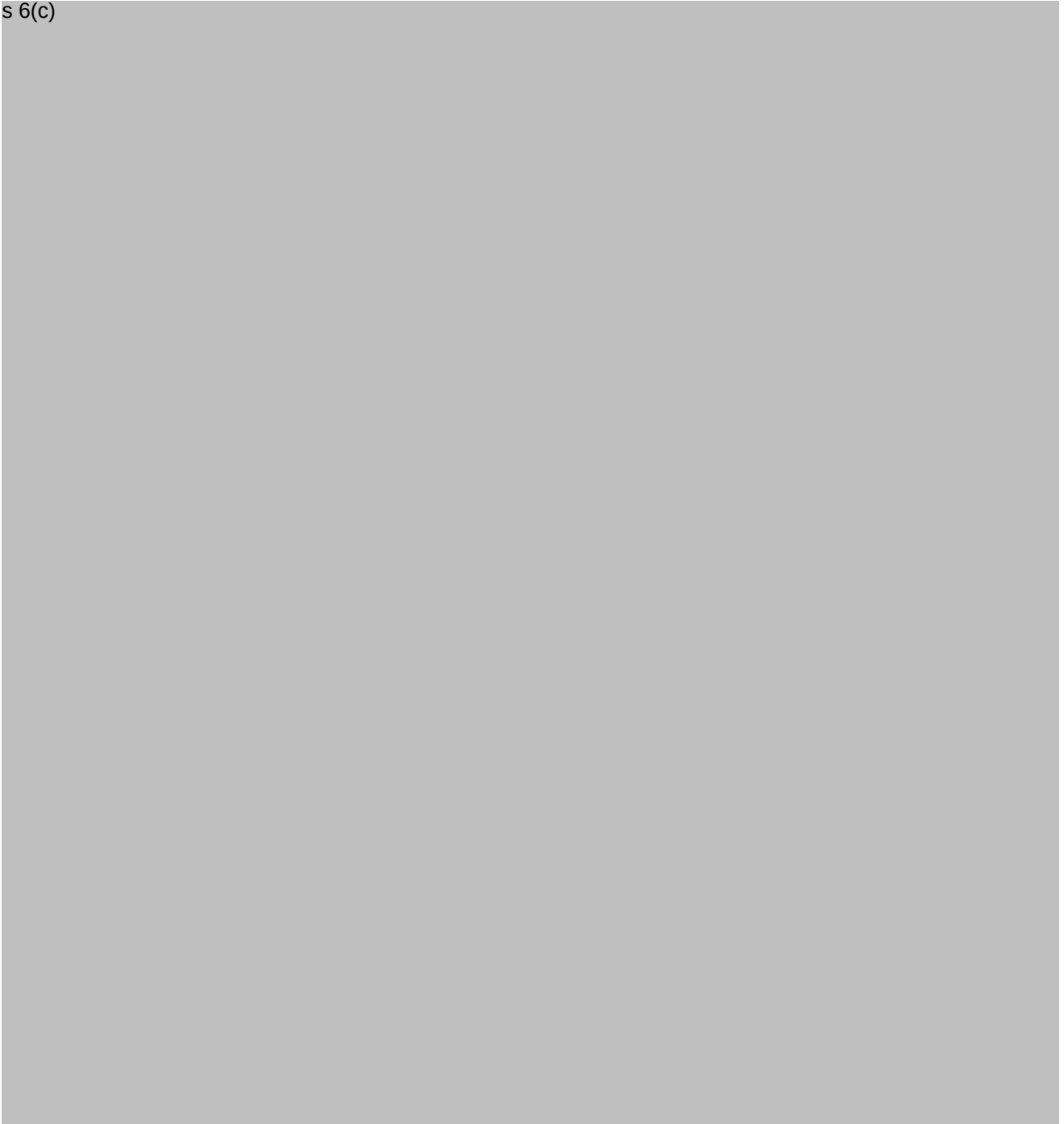
Project Overview

Biometric Capability Update (BCU)

The Identity Management solution (IDme) provides INZ with the capability to be the authoritative source of identity information for all non-New Zealanders.

The Biometric Capability Update has been designed to address INZ projects needs and future known capability by upgrading the versions of biometric matching and management platforms, rationalising and simplifying the platform to reduce on-going cost and improving the flexibility and utility of the system in the process. This is a core capability for INZ's future protection in an environment where identity fraud, terrorism and other sources of harm are prevalent and increasingly diverse and sophisticated, and this upgraded capability is crucial to achieving that future.

s 6(c)



3. Test Overview

Objectives of Testing / Critical Success Factors

Test objectives for the project are:

- To ensure the system works as specified in the Business Requirements, Non-Functional Requirements and Design Documents.
- Identify defects and associated issues and ensure they are appropriately addressed prior to implementation of the system.
- Measure quality, to provide stakeholders with sufficient information to make an informed decision about the release of the software and that the system is 'fit-for-purpose'.
- Mitigate the financial or reputational risk of deploying a system that does not meet business needs, or when implemented behaves in an undesirable or unknown way.
- To ensure that the new solution is robust, flexible and streamlined to allow for the continue tuning of the business rules.

Test Principles

The following principles have been used in formulating this Test Strategy:

- The goal of testing is to help achieve a high-quality product, while being mindful of timelines and cost.
- Each test level is planned with the knowledge and confidence as to expected coverage in previous and subsequent levels. For multiple test levels, where roles and responsibilities split between Vendor & MBIE.
- Testing will be focused to address identified stakeholder risks, both technical and reputational. Reputational risk may result in some testing requirements where little/no technical risk exists, and may include output from projects Risk Assessment or Risk Profile Spider Chart etc.
- Test early to measure quality and enable stakeholders to make informed decisions.
- Working together is the key to a successful outcome, collaboration between Business analysts, Business SMEs, vendor testers, technical specialists and the test team will help ensure a quality result.

4. Test Scope

Test Level and Types

See also [Appendix A](#) for full description of each Test Type.

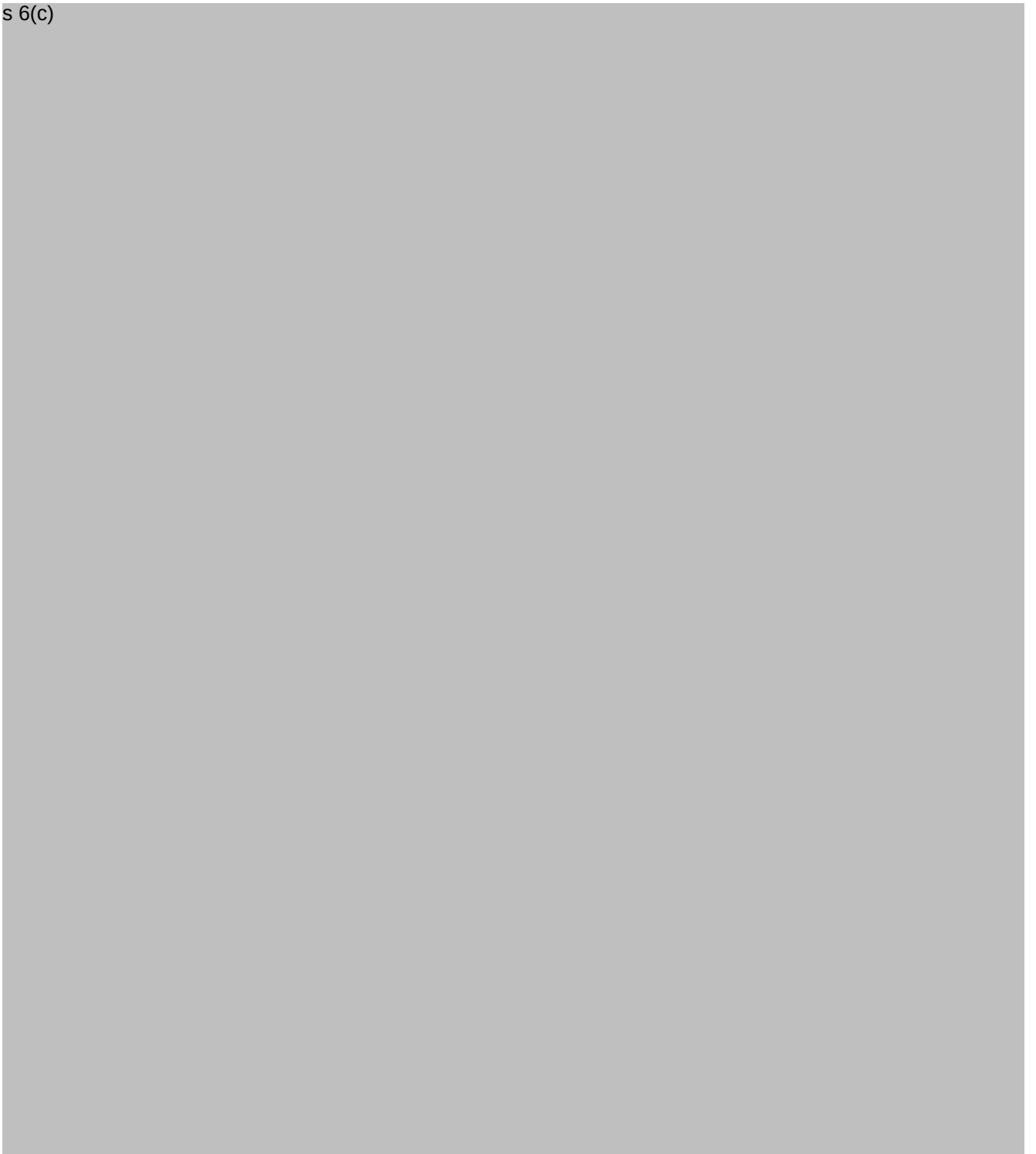
Test Level	Test Types	In Scope	Responsibility
Component/System Testing	Smoke/Shakedown	Y	Vendor Dev/Test Team
	Components	Y	Vendor Dev/Test Team
	Functionality	Y	Vendor Dev/Test Team
	Auditability	Y	Vendor Dev/Test Team
	Regression	Y	Vendor Dev/Test Team
	Integration/Interfaces	Y	Vendor Dev/Test Team
System Integration	Smoke / Shakedown	Y	MBIE BCU Test Team
	Integration / Interfaces	Y	MBIE BCU Test Team
	Connectivity	Y	MBIE BCU Test Team
	Accessibility	Y	MBIE BCU Test Team
	Usability	Y	MBIE BCU Test Team
	Auditability	Y	MBIE BCU Test Team
	Functionality	Y	MBIE BCU Test Team
	User Interface	Y	MBIE BCU Test Team
	Regression	Y	MBIE BCU Test Team
	Business Scenarios	Y	MBIE BCU Test Team
	End to End Integration	Y	MBIE BCU Test Team
	User Guides/Documentation	Y	MBIE BCU Test Team / Business Users
Performance	Performance; Load & Stress	Y	MBIE BCU Test Team
Security	Security & Penetration	Y	External Security Team
Conversion	Data Migration	Y	MBIE BCU Test Team
Business Acceptance	Functionality	Y	Business
	Functional User Security	Y	Business
	Usability	Y	Business
	Accessibility	Y	Business
	Business Process	Y	Business
Implementation	Post implementation	Y	Business/ MBIE BCU Test Team

Business includes Identity Services, Risk & Verification, Immigration Compliance, Refugee Quota Branch, Refugee Status Unit, Border and Visa Operations, Data Warehouse and NZ Police.



In Person Enrolment

s 6(c)

A large, solid grey rectangular area covering the majority of the page, indicating that the content has been redacted.



Out of Scope

Test items out of scope

The table below describes test activities that are outside the scope of the SIT Functional testing.

#	Test items	Description	Reason
1	System Testing items	Unit Testing Component Testing Field Validation UI Verification Functional Testing of Requirements	Test Activities covered under Vendor System Testing
2	Non-functional Requirements	NFRs including but not limited to system operational reporting, monitoring and alerting	Test Activities covered under NFR test scope

Functional Requirements

Detailed list of the functional requirements can be found in [Appendix B](#)

5. Test Approach

The following section details the test approach to be undertaken with the objective of covering all testable Functional Requirements within the test scope of Functional System Integration testing.

Test Approach Summary

Functional System Integration Testing will focus on functional requirements verifying that all subcomponents and external systems integrate successfully, to provide required business outcomes.

The following diagram outlines test activities within Functional System Integration testing for BCU solution:

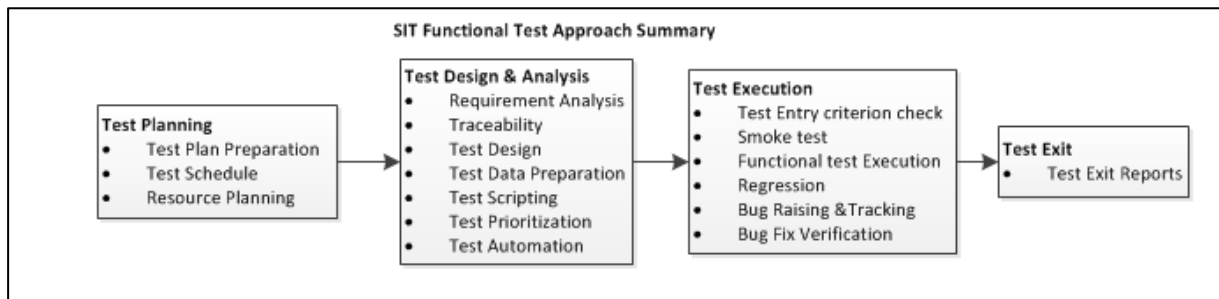


Figure 3: SIT Functional Test Approach Summary

The SIT Functional test delivery is broken down into the following test sub types:

1. Smoke
2. Functional SIT
3. Regression

The details for each test type are described in [Appendix A](#).

Functional System Integration testing will follow defined end to end business workflows. The reasoning behind this approach is to exercise in-scope workflows. In doing the testing in this manner, the environment is proofed, while the individual components are proofed indirectly through their use. Following the Usage Model approach, valid transactions will be traced through the BCU solution.

End to End Test suites are developed to validate the Automated and Maintenance Workflows which cover the Functional Requirements. Test Scenarios are designed to cover the path coverage and decision coverage of the workflows which provide a wide coverage of the business scenarios and data input.

Testing of the End-to-End business scenarios is a White Box Testing method in which test cases are defined based on flows or logical paths that can be taken through the workflows that interact with various system components i.e. AMS, Reveal, IQ Office, 6(c) of the OIA, Azure API, ADEPT, ETA, IGMS Online. The objective of path testing is to define the number of independent paths, so the number of test cases needed can be defined explicitly to maximize test coverage.

Advantages of the above Test Model are:

- It helps to reduce the redundant tests
- It focuses attention on Workflow logic
- It helps facilitates logical versus arbitrary case design
- It helps validate the integration with other solution components
- It validates the migrated data
- It proofs the integrated environment
- It achieves maximum path coverage with the least number of test cases
- Test cases which exercise basis set will execute every statement in a workflow at least once

The "Usage Model" testing strategy relies heavily on the fact that each solution components (i.e. IPE, NEC Workflow, IBW, AMS, Reveal, ISM, 6(c) of the OIA, IGMS, Azure APIM, and Data Migration) has successfully completed system



testing for each system. The goal of the strategy is to avoid unnecessary duplication of test effort, and to determine problems caused by the interaction of the various systems in the System Integrated Test environment.

The SIT functional high level test execution approach across the environments is described in the figure below. The diagram describes the SIT test types and how the tests are executed. The diagram also outlines the functional SIT test activity to be undertaken across the environments. Timelines or timeline dependencies are not explicitly represented within this high-level diagram. Arrows between the test activities represent indicative flows and dependencies.

The Number of SIT defect drops shown in the diagram below are indicative only.

The following Test phases are included:

Test Phase	Purpose	Undertaken by
System/Component/Unit Testing	Functional testing with no system integration	Vendors
System Integration Testing	MBIE's acceptance of the functionality developed System Integration Testing of all systems	BCU Test Team and Business SMEs
Migration	Verifying data has been migrated to and from MBIE's systems successfully and correctly	BCU Test Team
Performance Testing	Verify the performance of the full solution	BCU Test Team
Business Acceptance Testing	Business verifying that the solution is fit for purpose	MBIE Business Users
Operation Acceptance Testing	Technical verification that the solution has been built to MBIE's standards and meets the non-functional requirements	Architects BCU Test Team
Security Testing	Verify the solution is secure	MBIE Security Team Specialised External Security company
Production Verification	Verification that the solution was deployed correctly into the production environment	BCU Test Team MBIE Business Users

Smoke testing

s 6(c)



System Testing

Undertaken by

Vendors

- NEC
- DxC
- Datacom
- Argonaut
- In Tech
- Theta

Objective

System testing on the individual component meets functional specifications and fulfil all the specified requirements and workflows.

Test Execution Approach

Execution of the functional test cases will be completed in the system testing environment, it will cover the functionality of the application and where possible different data types. Validation and boundary testing will be executed as per business rules as defined in the specifications/design documents.

Test harnesses and stubs will be used as interfaces to the external systems as these are not available in the system test environments.

Each vendor will submit a test plan which will outline the testing methodology that they will be using and also detail the entry and exit criteria. These documents will be reviewed and accepted by the BCU Test Manager before execution starts.

Demos

Demonstrations will be completed regularly by the vendors throughout development. The team will demonstrate areas of the system that are ready for review. This will allow the project team and the business to see the solution early and enable early feedback.

Deliverables

- System Test Plan
- Requirements Traceability Matrix (Test Scripts to Functional Requirements & Rules)
- Defect Register
- Test Results
- System Test Exit Report
- Automation suite
- Walkthrough/Training of the application flow to the Test Team

Entry Criteria

- System Test Plan has been completed and signed off by MBIE
- Development is complete
- Test Environment available and configured
- Test preparation complete
- Test tools in place
- Requirements Traceability Matrix finalised



Exit Criteria

- All test cases executed (except cases that have been removed from scope after MBIE review and approval)
- No Open Severity 1 or 2 Defects
- All defects have had the severity and priority levels reviewed and agreed by MBIE
- All open defects have been reviewed by MBIE and aggregated severity 3 & 4 defects accepted with an agreed remediation plan
- All open defects have been reviewed by business representatives
- Test Exit Report completed and accepted by MBIE



Migration

Objective

Verify that data has been successfully migrated from the source system to the destination system.

Verify the migrated data is in the correct structure (Client -> Identity) in the destination system.

Verify the biometric data is associated to the correct biographic data.

Verify no degradation of the accuracy and usability of INZ data.

Verify that continuation of INZ business activities and associated transactions can be completed on the migrated data.

Test Design Technique

Test Cases will be derived from:

- Solution Architecture Design
- Business requirements
- Data Migration Approach
- Data Migration Plan

Data reconciliation reports will be provided by the vendors once the migration is completed prior to handing over to the test team.

Test Cases will be peer reviewed within the BCU Test Team, Business SMEs and Business Analysts then prioritised for execution.

Test Execution Approach

The following diagram is the high level Migration approach illustrating how migration will flow:



Performance Testing

Objective

To evaluate how the system performs in terms of responsiveness and stability under a particular workload.

Test Design Technique

Test scripts are designed from Non-Functional Requirements.

Test Execution Approach

Performance testing will provide details of how long a function will take between point 'a' and point 'b' with a specific number of users. A baseline will be run using the existing system and where possible compared to the new solution. Where the baseline is insufficient the business will review the results and be asked to approve the final timings.

Load testing will show how the function performs under an increasing load and determines at what point the performance becomes undesirable.

Soak testing is designed to execute load for an extended period to ensure stability and that there are no memory leaks.

Test execution of the scenarios will reflect expected performance characteristics, and will be expected to be undertaken in a production-like environment (Environment 2) in terms of

- Server and Storage capacity/compute
- Network Capability
- Database snapshot/backup
- Background processes which will run in production should run in the test environment

The following are the systems covered by this suite:

- AMS
- ETA
- Online visa applications
- ADEPT
- IPE

Entry Criteria

- Data Migration has been completed
- Latest code base has been deployed
- Test Environment available and configured
- Solution stable
- Test preparation complete
- Performance Test Plan has been completed and signed off
- Test tools in place
- All defects have had the severity and priority levels reviewed and agreed by MBIE
- All open defects have been reviewed by MBIE and aggregated severity 3 & 4 defects accepted with an agreed remediation plan

Exit Criteria

- All test cases executed (except cases that have been removed from scope after review and approval)
- No Open Severity 1 or 2 Defects
- All defects have had the severity and priority levels reviewed and agreed by MBIE
- All open defects have been reviewed by MBIE and aggregated severity 3 & 4 defects accepted with an agreed remediation plan
- Performance Test Exit Report completed and approved

Business Acceptance Testing

Objective

To assess if the system can support day-to-day business and user scenarios and ensure the system is sufficient, correct for business usage and the solution is fit for purpose.

Test Execution Approach

Each business scenario will be executed using an exploratory testing technique. This means the business user will execute the business scenario as they would during a normal working day to ensure that the solution is fit for purpose.

All steps will be documented during the test execution and logged in ADO under the project.

Test Analysts and INZ Business Analysts will be used to support the business users and ensure that all defects are analysed and prioritised appropriately.

The following business groups will be involved in the Business Acceptance testing:

- Identity Services
- Intelligence and Risk
- Border Officers
- Refugee Quota Branch - IPE
- Asylum (Refugee Status Unit) - IPE
- Compliance - IPE
- Visa Services
- NZ Police

Entry Criteria

- Test Exit report from System Integration Testing has been completed and approved
- No Open Severity 1 or 2 Defects
- All defects have had the severity and priority levels reviewed and agreed by MBIE
- All open defects have been reviewed by MBIE and aggregated severity 3 & 4 defects accepted with an agreed remediation plan
- The data migration has been completed successfully
- Test Environment available and configured
- Smoke test completed and passed
- Test preparation complete
- Test Strategy has been completed and signed off (this document)
- Test tools in place

Exit Criteria

- All test cases executed (except cases that have been removed from scope after review and approval)
- No Open Severity 1 or 2 Defects
- All defects have had the severity and priority levels reviewed and agreed by MBIE
- All open defects have been reviewed by MBIE and aggregated severity 3 & 4 defects accepted with an agreed remediation plan
- Test Exit Report completed and approved



Business Verification Testing

Objective

To verify the successful deployment of all code and data into the Production environment.

Test Execution Approach

Test Data will be created to test the various channels to ensure that the full solution has been deployed correctly and everything is up and running. Once testing is completed this data will be removed.

The testing will be executed by the project teams Test Analysts and Business representatives, they will work together to create the test cases and execute these scripts.

This testing will be undertaken by the following:

- BCU Test Team
- Business Representatives

Entry Criteria

- Test Exit reports for all test levels have been completed and approved
- CAB has approved moving into production
- Bulk data migration has been completed successfully
- BVT Test scripts complete
- Approved SOM and ORR
- No open severity 1 & 2 defects and aggregated Severity 3 & 4 defects accepted with an agreed remediation plan

Exit Criteria

- All systems are up and running.

Test Management Tools

The BCU Test Teams will use the following tools, for test planning; management; reporting and execution.

Tool	Purpose	Used by
Azure Dev Ops	Test Artefacts Test Execution scheduling and management Progress Reporting via Dashboards Test Case traceability to Business Requirements Defect Repository	BCU Test Team
Selenium	Test automation tool	BCU Test Team
Postman	API Test Automation	BCU Test Team
JMeter/Visual Studio Load Test	Performance Testing	BCU Test Team
WAVE tool (Chrome Add-on)	Usability testing. Assess the accessibility of website content	BCU Test Team
SortSite®	Automated web site testing tool for analysis of Accessibility; Usability and Web Standards	MBIE Digital Information Tools team

Test Execution Schedule

A test execution schedule will be created to ensure that all planned tests are executed within the allocated timeframe. The schedule will be used to report actual verses planned tests and give an early indication of whether the testing is on track or not. There will be no tests planned for release days as this day will be used to re-test defects and re-run the failed test cases.

Test Wrap up

The following tasks need to be completed to hand over to the BAU test team:

- Test users and set-up process documented
- INZ BAU Confluence page created and updated with testing deliverables
- Test assets handed over to INZ BAU (e.g. IPE Capture kits and laptops)
- Walk through with BAU test team
- All defects in ADO with current status, defects “Closed – Accepted by INZ” are documented.
- Regression suite updated

Deliverables

Deliverable	Responsible	Delivery Date
BCU Test Strategy	Test Manager	
Performance Test Plan	Performance Test Engineer	
BCU Non Functional Test Plan	Non Functional Test Engineer	
Test Cases	Test Analyst/s	
Traceability Matrix	(Lead) Test Analyst	
Test Results	Test Analyst/s	
SIT Test Exit Report	Test Manager	
DM Test Exit Report	Test Manager	
Performance Test Exit Report	Test Manager	
Business Acceptance Exit Report	Test Manager	
Regression Test Suite	Test Analyst/s	

Test Suspension Criteria

At any time, test execution may be suspended where:

- The severity or volume of defects is deemed sufficient to seriously jeopardise the quality and integrity of the test effort
- Continued test execution is deemed to no longer be adding value

A recommendation to suspend testing may be made by the Test Manager, but the final decision shall be made by the MBIE Project Manager and Business Owner, Systems Owner as per Roles & Responsibilities.

Testing will be suspended until the defect or other issues that led to the suspension have been satisfactorily resolved, or an acceptable workaround has been identified and implemented. In the event that this results in a change in Requirements and/or Solution Design the Project's Change Management Process is to be invoked.

Test Suspension criteria are detailed in Table below:

Short Description	Long Description
Environment Availability	The application/environment is identified as unstable, or unavailable
Significant Defects/Rework	Incorrect functionality/configuration of a core component, requiring significant investigation, prevents further testing
	Significant design changes are required that will prevent further testing
Resource Availability	Insufficient people to undertake testing, i.e. resource is required on other higher priority tasks/projects
	Absence of critical technical / support resource or SME to resolve an issue or a defect.

6. Test Team Structure and Roles

Roles and Responsibilities

Role	Responsibilities
Systems Owner	• Approver of the Test Strategy • Approver of Test Exit Report • Approver of any suspension of testing
MBIE Project Manager	• Approver of Test Strategy • Overall planning and IT resourcing of the project • Hand-over of completed solution to ICT Operations and Support • Work with INZ to assign business resources for Acceptance Testing • Member of Defect Management Committee (may delegate) • Approver of any suspension of testing • Approver of Test Exit Report • Vendor Manager
Vendor Project Manager and/or Vendor Test Manager/Lead	• Project escalation point for Vendor Test Team • Overall Vendor management of development and test activities • Member of Defect Management Committee For responsible system testing • Creation of Level Test Plans; Test Cases and Traceability Matrix • Progress reports • Test Execution • Defect management and retesting • Test Level Exit report
MBIE Solutions Architect	• Reviewer of Combined Test Strategy • Assist with definition of MBIE Test Environment/s builds • Supply Part B design doc – with test environment and interface component requirements • Member of Defect Management Committee • Consulted with prior to any suspension of testing • Approver of Non Functional Test Exit report • Review of Functional Test Exit Report • Non-functional - Technical Reviews
Security Architect	• Creator for risk assessment • Creator of Test Purpose for Security Vendor • Organize access for Security tester • Liaison between Security Vendor and project team • Attend daily security meeting
INZ Business Analyst/s	• Reviewer of Combined Test Strategy • Reviewer of Test Exit Report • Member of Defect Management Committee • Defining migration threshold's • Requirements clarification • Work with ICT Test Analysts to scope and document Business Acceptance test scenarios • Support Business Acceptance Testing • Non-functional test execution – Usability • Review test coverage via reviewing test cases • Priorities test cases in conjunction with test analysts
ICT Business SMEs	• Reviewer of Combined Test Strategy • Reviewer of Test Exit Report • Member of Defect Management Committee • Requirements clarification • Review test coverage via reviewing test cases

Role	Responsibilities
BCU Test Manager	• Manage the overall testing of the BCU and IPE testing • System Integration • Migration • Performance • Business Acceptance • Operational Acceptance (Non Functional) • Production Verification • Allocates and supports BCU test resource/s • Testing escalation point for Test Team • Creator of Test Strategy • Creator of Test Exit Report • Review Vendor test deliverables • Reports testing related risks and issues • Provides test progress report to the Project Manager • Recommends any suspension of testing • Chair of the Defect Management Committee • Manager of the Defect Process • Coordinator of Business Acceptance testing • Approve the Automation Framework
BCU SIT Test Lead	• Day to day management of SIT testing • Contributor into the Daily progress report • Contributor to the SIT Exit report • ICT Test Analysts responsibilities as below
MBIE Senior Test Analyst/s	• Create and manage MBIE test artefacts • Review Vendor test deliverables • Test execution • Defect management, including maintain defect register and retesting • Support and assist Business Acceptance Testers as required • Support and assist end/external user testing as required • Non Functional testing – usability, accessibility, audit and logging • Review existing regression suites • Regression testing of existing systems • Contributes to: • Test Strategy • Status / Progress Reports • Test Exit Report
MBIE Performance Test Engineer	• Create Performance Test Plan • Create test data • Create test scripts • Execute test scripts • Create Performance Test Exit report • Defect management, including maintain defect register and retesting
External Security Tester	• Create Security Test Plan • Create Security test scenarios • Execute test scenarios • Create Security report
Subject Matter Experts and Business Acceptance Testers	• Creation of Business scenario test cases • Execute Business Acceptance Testing • Raise defects / issues (via ICT Test Analysts) • Defining migrated thresholds • Execute Business Verification Testing in Production
MBIE Test Environment Manager & Release Planner	• Manage MBIE Test Environment requests and schedule • Manage MBIE Test Environment access • Identify and manage Test Environment conflicts with other projects • Approver of code deployments

7. Testing Schedule and Environments

Testing Milestones

For the latest testing schedule select the following mako link:
6(c) of the OIA

Test Environments

s 6(c)



Environment	Brief Specification	Activity / Test Levels
Vendor Development	Vendor hosted. Sufficient for unit testing of developed components. Integration with other components or external sub-systems may be stubbed.	Unit Testing
System Test – Vendor Environment	Vendor hosted. Integrated system components in a low performance environment. External sub-system interfaces may be stubbed	System Testing
System Integration Test (SIT) – Environment 1	MBIE hosted. A fully integrated low performance environment with real-time connectivity to, test instances of, all other internal and external sub-systems.	System Integration Testing Data Migration
User Acceptance Test (UAT) – Environment 2	MBIE hosted. Fully integrated, high performance environment with production configuration and real-time connectivity to, test instances of, all other internal and external sub-systems.	Business Acceptance Testing Data Migration Performance Testing
Pre-Production	MBIE hosted. A fully integrated, mirror of production with connectivity to all internal and external sub-systems.	Data Migration Security Testing Dress rehearsal

8. Test Management Procedure

Test Progress Reporting

Test progress reports will be available to Project and Test Management teams weekly or as required. It is anticipated that progress reporting will make use of Azure Dev Ops Report Dashboard. The test management tool that will be used for these projects is Azure Dev Ops for Test Design, Test Execution and Defect Management.

Defect Management

Defect Management processes will follow [BCU Defect management process](#)

All open System defects from the vendors will be logged in MBIE ADO repository when MBIE SIT testing commences.

MBIE defects will be logged into ADO with Severity and Priority ratings. When the defect is reviewed by the Defect Triage Committee the ratings may be reset. Defect meetings will be scheduled by the BCU Test Manager and will be run twice a week

Severity

Severity level refers to the degree that the defect impacts or affects the system.

The impact of the defect on the application (system-wide, one module, single function) as well as the impact on the business or technical environment is also taken into account when assigning a severity.

Defect Severity Level	Description
Critical	A termination of the complete system or one or more components of the system and causes extensive corruption of the data. The failed function is unusable and there is no acceptable alternative method to achieve the required results.
Major	A termination of the complete system or one or more components of the system and causes extensive corruption of the data. The failed function is unusable but there exists an acceptable alternative method to achieve the required results.
Moderate	A defect that does not result in the termination, but causes the system to produce incorrect, incomplete or inconsistent results then the severity will be stated as moderate.
Minor	A defect that does not result in termination and does not damage the usability of the system and the desired results can be easily obtained by an acceptable work around.
Cosmetic	A defect that is related to the enhancement of the system where the changes are related to the look and feel of the application then the severity is stated as cosmetic.

Priority

Priority defines the order in which we should resolve defects. It is set by the tester as an indication of how quickly a resolution is required, usually to support the test execution timeframes.

Priority	Description	Response Time
High	Must be resolved as soon as possible because the defect is severely affecting the application or the product. The system cannot be used until the repair has been done.	2 hours
Medium	The defect should be resolved in the normal course of development activities. It can wait until a new build or version is created.	New release
Low	The defect is an irritant which should be repaired, but repair can be deferred until after more serious defects have been fixed.	Planned release

Defect Management Committee Meetings

ADO will be the central defect repository and used to facilitate the management and tracking of the following:

- Defect Recording/Logging
- Defect Analysis
- Defect Tracking
- Defect Reporting

The purpose of the defect committee is to provide the project with a forum for reviewing and confirming the prioritisation of defects as well as providing information to enable the business to prepare workarounds that may be required for those defects that are not fixed prior to deployment.

During System Integration Testing and Business Acceptance testing it is anticipated these meetings will be held twice weekly, they will be facilitated by the BCU Test Manager and initiated at the commencement of test execution. If participants are not able to be on site there will be a Microsoft Teams meeting set up.

Representatives of the test team and vendor development teams will attend these meetings with support from the project management team, business owners/representatives and other project stakeholders where necessary.

The objective of the defect committee is to:

- Confirm defect severities, priorities, and resolution timeframes
- Keep the Project / Business informed and involved
- Provide a forum to talk through issues relating to the defects i.e., workarounds,
- Resolve discrepancies which may lead to the requirement for Enhancements/Change Request to be raised, and
- Make decisions as to whether testing or implementation can proceed with a particular defect present where that defect is deemed critical or important to the business and cannot be fixed and retested before exiting a test phase or implementing to production.
- Schedule defects for release

Builds/Releases

Test execution will be planned around defect builds which will contain defects fixes and no new functionality. These will be scheduled in the defect management meetings and approved by the release managers.

Each build will have a smoke test completed and testing will not commence until the smoke tests have passed.

All defect retesting will be completed on the defects, regression testing around the defect will then be executed and then the original failed test case will be re-run.

9. Assumptions & Dependencies; Risks and Issues

Assumptions

The following assumptions have been used when preparing this document:

#	Assumption	Impact if incorrect
A1	Hardware for IPE is available at the start of testing	Testing will need to start later
A2	The BCU testers have existing knowledge of the existing systems so understand the images and issues/limitations of the existing system	Testing will take longer than estimated
A2	Data Migration Reconciliation report available for the test team prior to test execution phase	Migration due to inconsistent data will have negative impact on Functional Testing
A4	At least one of the migration testers have data migration testing experience	Testing may take longer than estimated
A5	The architects will verify the non-functional requirements that do not need a test activity and review the test evidence of the other NFRs	Technical tester will need to be resourced
A6	The System Integration and Migration test phases have been estimated by the identity testers using the BCU requirements only.	Estimates will need to be reviewed
A7	BCU Test team is available to support business users during Business Acceptance testing	Estimates will need to be reviewed
A8	System Test exit reports are signed off before SIT commencement	SIT Test phase will not be able to start on schedule
A9	Defects post System Test will be managed in MBIE ADO repository	Defect Management gets difficult

Dependencies

Delivery of this testing is dependent on:

#	Dependencies	Impact
D1	The creation of the test scripts for Business Acceptance Testing is dependent on the Business processes being completed.	Business Acceptance Testing cannot start
D2	Business SMEs are available for Business acceptance testing and creation of the test cases	Project implementation date may be impacted

Risks

The following Risks, and mitigations, have been identified during the preparation of this document and will be recorded in the Projects Risk Register for visibility and management. Any further Risks identified will also be recorded and managed via the Projects register.

#	Title	Risk	Impact	Likely hood	Mitigation
R1	Hardware availability (IPE)	If the hardware (passport reader) is not available when testing starts then testing may not meet its timelines	Major	Possible	NEC are adding the testing hardware to their SOW so that it is procured early

#	Title	Risk	Impact	Likely hood	Mitigation
R2	Code Quality	If the quality of the code is not at the expected standard then testing timelines will be impacted	Major	Possible	30% defect rate has been used for testing estimates instead of the standard 15% Contingency of 20% has been added to all testing related tasks
R3	Business users not available	If the business users are not available to complete Business Acceptance testing then the implementation will be impacted	Major	Likely	Business User reference group has been created Schedule to be published to the business user group to help plan resources
R4	Requirements clarity	If the requirements are not documented at a detailed level then there is the possibility that the delivered solution will not fully meet the needs of the business, and the gaps will not be identified prior to production implementation.	Moderate	Likely	Business Analysts will review test cases for coverage Test Analysts will review requirement documents Architect to review the requirements to ensure that they meet the proposed design
R5	Business processes	If the business processes are not completed before the User acceptance testing starts then this test phase will not start	Moderate	Unlikely	Change Manager to monitor progress
R6	s 6(c)				
R7	Bad Data in Test Environments	Bad data in the test environment may extend the testing timeframes	Major	Almost Certain	The testers will identify the bad data scenarios as part of their test preparation The scenarios will be executed to remove the data from the migration loads
R8	Migration process	If we don't test the exact steps that will be executed during the migration process until pre-production then issues may be found that could impact the implementation date	Minor	Unlikely	Two dress rehearsals will be completed
R9	Environments	Other projects/workstreams in the test environment in parallel to BCU may impact environment availability and stability due to severity 1 defects and deployment outages	Moderate	Likely	Schedule dates given to the Environment manager as soon as possible Test Managers working together to communication potential outages

Issues

The following issues have been identified during the preparation of this document and will be recorded in the Projects Issue register for visibility and management. Any further issues identified will also be recorded and managed via the Projects register.

#	Title	Issue	Mitigation	Status
I1				
I2				

Appendix A: Test Types

Test type	Description
User /Business Acceptance testing	Formal testing with respect to user needs, requirements, and business processes conducted to determine whether or not a system satisfies the acceptance criteria and to enable the user, customers or other authorized entity to determine whether or not to accept the system.
Accessibility	Testing to determine the ease by which users with disabilities can use a component or system. Includes compliance with NZ Govt. web standards. NB: See also MBIE's standard Usability checklist
Auditability	Testing to determine that that Audit requirements of the system have been met.
Back up & Recovery	The process of testing to determine the recoverability of a software product. Verifies that the system meets requirements for recovery after a failure, including ability to recover data, database, object, workspace and state; backup and recovery processes; time to recover; disruption and interference for other users.
Concurrency Testing	Testing to determine how the occurrence of two or more activities within the same interval of time, achieved either by interleaving the activities or by simultaneous execution, is handled by the component or system.
Conversion Testing (aka Data Migration)	Testing of software used to convert data from existing systems for use in replacement systems.
Configuration Testing	The process of testing to determine the portability of a software product. Verifies that the application operates successfully in all production configurations, may include: • Browser (type and version) • DBMS • Other software and version dependencies (e.g. MS-Office applications, data access components, drivers, add-ins, Citrix) • Hardware • Deployment method and process
Content Management	Process to verify that the content to be published in production ready. For MBIE, this should be managed by the Business / Content Managers and may include reviews by policy and legal teams.
Documentation Testing	Testing the quality of the documentation, e.g. user guide or installation guide. Applicable methods will be Inspection, Reviews etc.
Functional Testing	Testing based on an analysis of the specification of the functionality of a component or system. Verifies that the application is usable, works correctly, completely and as specified. If applicable, test requirements will include workflow (business scenarios – alternative flow of events) which might cross use case boundaries, or which represent special test requirements, i.e. transaction level tasks, business cycle functions, data processed. Test design should include coverage of both valid and invalid scenarios and would typically employ black-box testing techniques such as boundary value analysis; equivalence partitioning. Where applicable, testing shall include 'in-flight' and 'new' data
Graphical User Interface (GUI)	Testing performed by interacting with the software under test via the user interface. Includes testing areas such as: • Mandatory data / fields • Field picklists & dropdowns • Field and screen navigation
Integration Testing	Testing performed to expose defects in the interfaces and in the interactions between integrated components or systems.
Interface Testing	An integration test type that is concerned with testing the interfaces between components or systems.

Maintenance Testing (including Warranty Testing)	Testing the changes to an operational system or the impact of a changed environment to an operational system. Includes data-fix testing.
Operation Acceptance Testing	This testing evaluates operational readiness for a software application prior to the release to the production. Operational Acceptance Testing ensures system and component compliance in the application's standard operating environment (SOE). The testing is based off the Non-functional requirements.
Performance Testing	The process of testing to determine the performance of a software product. Can include Stress, Volume, Load and Soak testing
Production Acceptance Testing (aka Deployment Test)	Testing conducted to evaluate a component or system in its operational environment. Also known as Operational Acceptance and Production Installation Verification (PIV) testing.
Regression Testing	Testing of a previously tested program following modification to ensure that defects have not been introduced or uncovered in unchanged areas of the software, as a result of the changes made. It is performed when the software or its environment is changed.
Reports Testing	Testing to determine that report content, format and output meets requirements. Where applicable, shall include testing against production configuration and hardware.
Security Testing	Testing to determine the security of the software product; generally at a functional or user level rather than penetration by "hackers" via the internet
Smoke Testing	A subset of all defined/planned test cases that cover the main functionality of a component or system, to ascertaining that the most crucial functions of a program work; but not bothering with the finer details. A daily build and smoke test is among industry best practices.
System Testing	The process of testing an integrated system to verify that it meets specified functional and non-functional requirement.
System Integration Testing	Testing the integration of systems and packages.
Unit/Component Testing	The testing of individual software components.
Unit/Component Integration testing	Testing performed to expose defects in the interfaces and interaction between integrated components.
Usability	Including compliance with: • Government web standards • Identity and Branding NB: Guided by MBIE's standard Usability checklist

Appendix B: Functional Requirements In-Scope

The functional requirements for BCU are detailed in the documents in the list below (all of which are listed in the document reference in this document also). Key additional/new functional requirements added by BCU are listed below.

BCU requirements documents:

Document title	Version	Location / ID
NEC IDMe Business Requirements	1.3	s 6(c)
NEC IPE Functional Specification	2.4	
NEC IPE Hardware Requirements	2.1	
NEC BCU Non Functional Requirements	1.0	
NEC BCU NFR Support Data	1.0	
AMS Changes Detailed Requirements	0.7	
Argonaut SRTP Business Requirements	6.8	
InTech IQOffice Business Requirements	0.9	
Datacom IGMS BCU Business Requirements	0.7	
Theta BCU Azure Business Requirements	0.3	
In-Person Enrolment (Part A) FINAL	1.3	
BCU Architectural Solution Design Part A – FINAL	1.5	
s 6(c)		
AMS BCU External Concurrency Design	v93	
AMS BCU Additional Features Design	v3	
AMS BCU Detailed Design AMS and SIH	1.0	
BCU Infrastructure - SIT Solution Design Infrastructure Part B	3.6	



**MINISTRY OF BUSINESS,
INNOVATION & EMPLOYMENT**
HĪKINA WHAKATUTUKI



3644 BCU – Biometric Capability Update

Test Plan

Version: 2.03

Date: 09/June/2023



1. Document control

Version history

Date	Version	Author	Description of change
23/09/2020	V1.0	s 9(2)(a)	Final
14/10/2022	V1.1		Multiple updates across the document after Requirements are finalised
17/10/2022	V2.0		Final
24/04/2023	V2.01		Minor updates around Test User Setup (AD and KeyCloak)
23/05/2023	V2.02		Adding User Role mapping and AD group requirements (Appendix D)
9/06/2023	V2.03		Adding more detailed and updated timeline.

Reviewed by

The following people have a formal quality assurance role with respect to this document

Name	Role	Date
s 9(2)(a)		7/10/2022
		Not Yet
		Not Yet
		7/10/2022
		7/10/2022
		7/10/2022
		7/10/2022

Test Plan Signoff

The signatories below have reviewed this document and agree it is a fit-for-purpose statement of the testing objectives, processes, and strategies to be used for the Biometric Capability Update (BCU).

The following signatures indicate approval and acceptance of this document, subject to any caveats below:

Name	Title	Signed
s 9(2)(a)		Signed : _____ Date : ____ \ ____ \ ____
		Signed : _____ Date : ____ \ ____ \ ____
		Signed : _____ Date : ____ \ ____ \ ____



Distribution

The following people/groups have been sent a copy of this document (list excludes approvers, reviewers, and consulted): (Not distributed to all after the 2.02 update)

Name	Role	Date
s 9(2)(a)		26/May/2023
		26/May/2023
		26/May/2023
		26/May/2023
		26/May/2023
		26/May/2023
		26/May/2023
		26/May/2023
		26/May/2023
		26/May/2023
		26/May/2023



Contents

1. Document control	2
Version history.....	2
Reviewed by	2
Test Plan Signoff.....	2
Distribution.....	3
2. Overview	6
Purpose.....	6
Context	6
Documents Referenced	6
Project Overview.....	7
3. Test Overview	11
Objectives of Testing / Critical Success Factors	11
Test Principles	11
4. Test Scope	12
Test Level and Types	12
End to End BCU IDmes Solution	13
In Scope	14
Out of Scope	19
5. Test Approach.....	20
Smoke testing.....	24
System Testing	27
Migration.....	29
System Integration Testing.....	34
Performance Testing	39
Business Acceptance Testing	40
Business Verification Testing.....	41
Test Management Tools	42
Test Execution Schedule.....	42
Test Wrap up.....	42
Deliverables.....	42
Test Suspension Criteria	43
6. Test Team Structure and Roles	44
Roles and Responsibilities.....	44
7. Testing Schedule and Environments	47
Testing Milestones	47
Test Environments	47
8. Test Management Procedure	50
Test Progress Reporting	50
Defect Management.....	50
9. Assumptions & Dependencies; Risks and Issues	52
Assumptions	52
Dependencies	52
Risks	52



Issues	54
Appendix A: Test Types	55
Appendix B: Functional Requirements In-Scope	57
Appendix C Traceability Matrix	58
Appendix D Test User Pre-requisites and configuration	59

2. Overview

Purpose

This document contains details of the testing to be completed for BCU and IPE. It should be used to inform relevant parties of testing details to review and understand the involvement from the different teams, resources, vendors and expected artefacts and deliverables for the project.

This is a static document to provide information at this stage of project planning. All changes during the execution phases of the project will be managed by the project using accepted change processes. Changes to testing will be logged and recorded in the Test Summary/Exit reports at the end of Test Execution.

Context

This Test Plan is produced as part of the ITG Project Delivery Model 'Build/Test' phase for the BCU & IPE Projects.



Documents Referenced

Further information on the project can be found as follows:

Document title	Version	Date	Location / ID
NEC IDMe Business Requirements	1.3	18/06/2021	S 6(c)
NEC IPE Functional Specification	2.4	17/05/2021	
NEC IPE Hardware Requirements	2.1	1/06/2021	
NEC BCU Non Functional Requirements	1.0	06/05/2021	
NEC BCU NFR Support Data	1.0	04/05/2021	
AMS Changes Detailed Requirements	0.7	19/07/2021	
Argonaut SRTP Business Requirements	6.8	2/07/2021	
InTech IQOffice Business Requirements	0.9	19/07/2021	
Datacom IGMS BCU Business Requirements	0.7	19/07/2021	
Theta BCU Azure Business Requirements	0.3	15/07/2021	
In-Person Enrolment (Part A) FINAL	1.3	23/04/2020	
BCU Architectural Solution Design Part A – FINAL	1.5	10/08/2021	
S 6(c)		11/08/2021	
AMS BCU External Concurrency Design	v93	08/09/2021	
AMS BCU Additional Features Design	v3	01/10/2021	
AMS BCU Detailed Design AMS and SIH	1.0	28/07/2021	
BCU Infrastructure - SIT Solution Design Infrastructure Part B	3.6	10/5/2022	



Project Overview

Biometric Capability Update (BCU)

The Identity Management solution (IDme) provides INZ with the capability to be the authoritative source of identity information for all non-New Zealanders.

The Biometric Capability Update has been designed to address INZ project's needs and future known capability by upgrading the versions of biometric matching and management platforms, rationalising and simplifying the platform to reduce on-going cost and improve the flexibility and utility of the system in the process. This is a core capability for INZ's future protection in an environment where identity fraud, terrorism and other sources of harm are prevalent and increasingly diverse and sophisticated, and this upgraded capability is crucial to achieving that future.

s 6(c)



3. Test Overview

Objectives of Testing / Critical Success Factors

Test objectives for the project are:

- To ensure the system works as specified in the Business Requirements, Non-Functional Requirements and Design Documents.
- Identify defects and associated issues and ensure they are appropriately addressed prior to implementation of the system.
- Measure quality, to provide stakeholders with sufficient information to make an informed decision about the release of the software and that the system is 'fit-for-purpose'.
- Mitigate the financial or reputational risk of deploying a system that does not meet business needs, or when implemented behaves in an undesirable or unknown way.
- To ensure that the new solution is robust, flexible and streamlined to allow for the continue tuning of the business rules.

Test Principles

The following principles have been used in formulating this Test Plan:

- The goal of testing is to help achieve a high-quality product, while being mindful of timelines and cost.
- Each test level is planned with the knowledge and confidence as to expected coverage in previous and subsequent levels. For multiple test levels, where roles and responsibilities split between Vendor & MBIE.
- Testing will be focused to address identified stakeholder risks, both technical and reputational. Reputational risk may result in some testing requirements where little/no technical risk exists, and may include output from projects Risk Assessment or Risk Profile Spider Chart etc.
- Test early to measure quality and enable stakeholders to make informed decisions.
- Working together is the key to a successful outcome, collaboration between Business analysts, Business SMEs, vendor testers, technical specialists and the test team will help ensure a quality result.

4. Test Scope

Test Level and Types

See also 6(c) of the OIA full description of each Test Type.

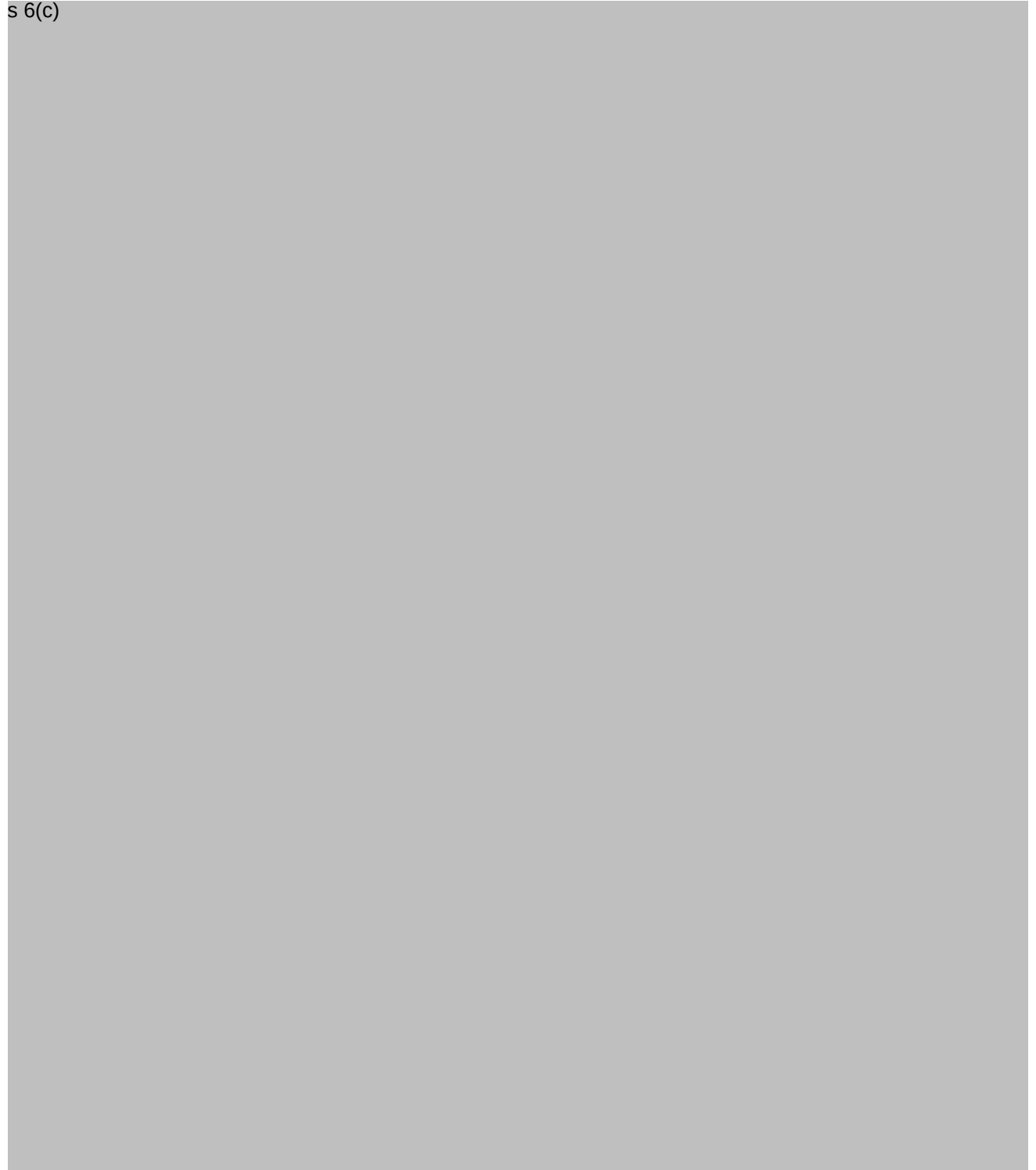
Test Level	Test Types	In Scope	Responsibility
Component/System Testing	Smoke/Shakedown	Y	Vendor Dev/Test Team
	Components	Y	Vendor Dev/Test Team
	Functionality	Y	Vendor Dev/Test Team
	Auditability	Y	Vendor Dev/Test Team
	Regression	Y	Vendor Dev/Test Team
	Integration/Interfaces	Y	Vendor Dev/Test Team
System Integration	Smoke / Shakedown	Y	MBIE BCU Test Team
	Integration / Interfaces	Y	MBIE BCU Test Team
	Connectivity	Y	MBIE BCU Test Team
	Accessibility	Y	MBIE BCU Test Team
	Usability	Y	MBIE BCU Test Team
	Auditability	Y	MBIE BCU Test Team
	Functionality	Y	MBIE BCU Test Team
	User Interface	Y	MBIE BCU Test Team
	Regression	Y	MBIE BCU Test Team
	Business Scenarios	Y	MBIE BCU Test Team
	End to End Integration	Y	MBIE BCU Test Team
	User Guides/Documentation	Y	MBIE BCU Test Team / Business Users
Performance	Performance; Load & Stress	Y	MBIE BCU Test Team
Security	Security & Penetration	Y	External Security Team
Conversion	Data Migration	Y	MBIE BCU Test Team
Business Acceptance	Functionality	Y	Business
	Functional User Security	Y	Business
	Usability	Y	Business
	Accessibility	Y	Business
	Business Process	Y	Business
Implementation	Post implementation	Y	Business/ MBIE BCU Test Team

Business includes Identity Services, Risk & Verification, Immigration Compliance, Refugee Quota Branch, Refugee Status Unit, Border and Visa Operations, Data Warehouse and NZ Police.



In Person Enrolment

S 6(c)



5. Test Approach

The following section details the test approach to be undertaken with the objective of covering all testable Functional Requirements within the test scope of Functional System Integration testing.

Test Approach Summary

Functional System Integration Testing will focus on functional requirements verifying that all subcomponents and external systems integrate successfully, to provide required business outcomes.

The following diagram outlines test activities within Functional System Integration testing for BCU solution:

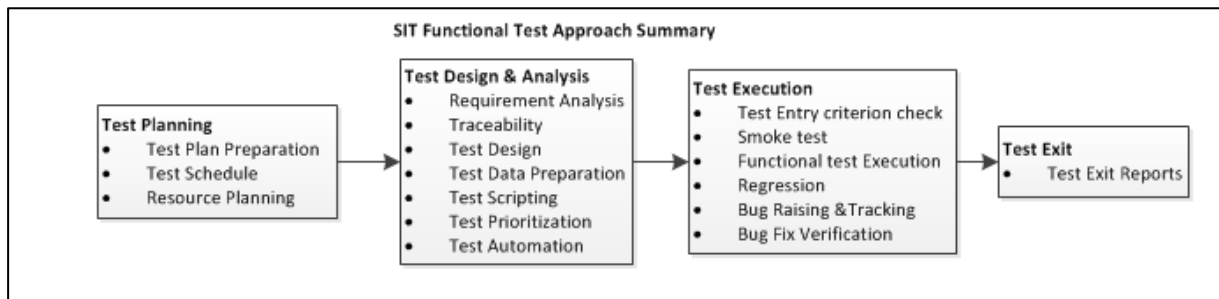


Figure 3: SIT Functional Test Approach Summary

The SIT Functional test delivery is broken down into the following test sub types:

1. Smoke
2. Functional SIT
3. Regression

The details for each test type are described in 6(c) of the OIA

Functional System Integration testing will follow defined end to end business workflows. The reasoning behind this approach is to exercise in-scope workflows. In doing the testing in this manner, the environment is proofed, while the individual components are proofed indirectly through their use. Following the Usage Model approach, valid transactions will be traced through the BCU solution.

End to End Test suites are developed to validate the Automated and Maintenance Workflows which cover the Functional Requirements. Test Scenarios are designed to cover the path coverage and decision coverage of the workflows which provide a wide coverage of the business scenarios and data input.

Testing of the End-to-End business scenarios is a White Box Testing method in which test cases are defined based on flows or logical paths that can be taken through the workflows that interact with various system components i.e. AMS, Reveal, IQ Office, IBW, 6(c) of the OIA DMS, Azure API, ADEPT, ETA, IGMS Online. The objective of path testing is to define the number of independent paths, so the number of test cases needed can be defined explicitly to maximize test coverage.

Advantages of the above Test Model are:

- It helps to reduce the redundant tests
- It focuses attention on Workflow logic
- It helps facilitates logical versus arbitrary case design
- It helps validate the integration with other solution components
- It validates the migrated data
- It proofs the integrated environment
- It achieves maximum path coverage with the least number of test cases
- Test cases which exercise basis set will execute every statement in a workflow at least once

The "Usage Model" testing strategy relies heavily on the fact that each solution components (i.e. IPE, NEC Workflow, IBW, AMS, Reveal, ISM, 6(c) of the OIA IGMS, Azure APIM, and Data Migration) has successfully completed system



testing for each system. The goal of the strategy is to avoid unnecessary duplication of test effort, and to determine problems caused by the interaction of the various systems in the System Integrated Test environment.

The SIT functional high level test execution approach across the environments is described in the figure below. The diagram describes the SIT test types and how the tests are executed. The diagram also outlines the functional SIT test activity to be undertaken across the environments. Timelines or timeline dependencies are not explicitly represented within this high-level diagram. Arrows between the test activities represent indicative flows and dependencies.

The Number of SIT defect drops shown in the diagram below are indicative only.

The following Test phases are included:

Test Phase	Purpose	Undertaken by
System/Component/Unit Testing	Functional testing with no system integration	Vendors
System Integration Testing	MBIE's acceptance of the functionality developed System Integration Testing of all systems	BCU Test Team and Business SMEs
Migration	Verifying data has been migrated to and from MBIE's systems successfully and correctly	BCU Test Team
Performance Testing	Verify the performance of the full solution	BCU Test Team
Business Acceptance Testing	Business verifying that the solution is fit for purpose	MBIE Business Users
Operation Acceptance Testing	Technical verification that the solution has been built to MBIE's standards and meets the non-functional requirements	Architects BCU Test Team
Security Testing	Verify the solution is secure	MBIE Security Team Specialised External Security company
Production Verification	Verification that the solution was deployed correctly into the production environment	BCU Test Team MBIE Business Users

Smoke testing

s 6(c)



System Testing

Undertaken by

Vendors

- NEC
- DxC
- Datacom
- Argonaut
- In Tech
- Theta

Objective

System testing on the individual component meets functional specifications and fulfil all the specified requirements and workflows.

Test Execution Approach

Execution of the functional test cases will be completed in the system testing environment, it will cover the functionality of the application and where possible different data types. Validation and boundary testing will be executed as per business rules as defined in the specifications/design documents.

Test harnesses and stubs will be used as interfaces to the external systems as these are not available in the system test environments.

Each vendor will submit a test plan which will outline the testing methodology that they will be using and also detail the entry and exit criteria. These documents will be reviewed and accepted by the BCU Test Manager before execution starts.

Demos

Demonstrations will be completed regularly by the vendors throughout development. The team will demonstrate areas of the system that are ready for review. This will allow the project team and the business to see the solution early and enable early feedback.

Deliverables

- System Test Plan
- Requirements Traceability Matrix (Test Scripts to Functional Requirements & Rules)
- Defect Register
- Test Results
- System Test Exit Report
- Automation suite
- Walkthrough/Training of the application flow to the Test Team

Entry Criteria

- System Test Plan has been completed and signed off by MBIE
- Development is complete
- Test Environment available and configured
- Test preparation complete
- Test tools in place
- Requirements Traceability Matrix finalised



Exit Criteria

- All test cases executed (except cases that have been removed from scope after MBIE review and approval)
- No Open Severity 1 or 2 Defects
- All defects have had the severity and priority levels reviewed and agreed by MBIE
- All open defects have been reviewed by MBIE and aggregated severity 3 & 4 defects accepted with an agreed remediation plan
- All open defects have been reviewed by business representatives
- Test Exit Report completed and accepted by MBIE



Migration

Objective

Verify that data has been successfully migrated from the source system to the destination system.

Verify the migrated data is in the correct structure (Client -> Identity) in the destination system.

Verify the biometric data is associated to the correct biographic data.

Verify no degradation of the accuracy and usability of INZ data.

Verify that continuation of INZ business activities and associated transactions can be completed on the migrated data.

Test Design Technique

Test Cases will be derived from:

- Solution Architecture Design
- Business requirements
- Data Migration Approach
- Data Migration Plan

Data reconciliation reports will be provided by the vendors once the migration is completed prior to handing over to the test team.

Test Cases will be peer reviewed within the BCU Test Team, Business SMEs and Business Analysts then prioritised for execution.

Test Execution Approach

The following diagram is the high level Migration approach illustrating how migration will flow:



System Integration Testing

Undertaken by –MBIE BCU Test Team with support from vendors where required.

Test Design Technique

Test Cases will be derived from:

- Architecture Solution Design
- Business Requirements
- Functional Requirements
- Vendor Design documents

Test coverage includes:

- Data validations
- UI verification
- API Integration test
- Workflows – Automated and Maintenance
- Data quality
- Configuration

All test cases will be loaded into BCU project in Azure Dev Ops and linked to the related requirements. This will allow visibility of which requirements have been tested and met. Test Cases will be peer reviewed within the BCU Test Team and Business Analysts then prioritised to ensure that the more complex areas are tested first to allow time for remediation if required.

Test Execution Approach

This testing phase will cover MBIE functional and System Integration Testing. There will also be multiple rounds of regression testing completed on all the existing systems that integrate with the identity process depending on the defect release.

Test Data

All biographic and biometric data from the existing system (IGMS) will be migrated to AMS, NEC and IQ Office which will enable the test team to test the migration and use the Test Data for Functional Testing.

Identity Process

MBIE will focus on the workflows, configuration, data types and the end-to-end process of the creation of an identity. This will include capture, match, search, manage and resolve.

In Person Enrolment (IPE)

Hardware

IPE Workstations

- S 6(c) Laptops and Handheld Tablets (MBIE build)

Enrolment equipment Standard and all in one

- Passport Scanner
- Camera
- Fingerprint readers

Physical Passports from a variety of countries.

Execution

The testing completed by NEC will focus on the functionality of the product. The testing completed by MBIE will focus on the workflows, configuration, and data types.

Testing will ensure that the new Smartscan application:

- supports the enrolment business processes
- the processes have been configured correctly
- captures images, fingerprints, passport scans and biographic data correctly
- documents attached are associated to the correct enrolment and then stored in DMS
- integrated with BCU and sends the enrolled identity for matching.

High priority test cases will be the enrol process that covers all the functions, and the other processes will be considered medium and will be executed after all the high priority test cases are executed.

Hardware testing

Each of the hardware above will be tested to ensure that they meet the hardware requirements and work as expected with the support from Business SMEs.

Reveal

Reveal is a COTS product that will be configured to reflect MBIE's requirements.

The application is used to allow the user to resolve any matches that need manual intervention. Specific testing will be completed on the following functions, all other testing will be covered in the resolution process above.

Tasks

- Task consolidation
- Multiple Matches
- Task filtering and self-assign

Administration - Insights

- Reports
- Update to business rules
- Add and update users roles
- Adjust queues
- Update urgency level
- Update priority levels
- Update capping rules
- Optimise capping rule
- Task/queue prioritisation

Ad hoc search

Search will be moved to Reveal and IBW, this will allow users to complete a search without having to create an identity. The face images that will be used have been obtained from the production image set which have been through the test harness and reviewed by the Identity services team. Fingerprint images will be obtained from an existing fingerprint test file that has been provided to the team. The following will be covered during the search testing:

- Load NIST files - IBW
- Load JPEG files - Reveal
- Search via Biographic - Reveal

IBW - Integrated Biometric Workstation

IBW will be used for all fingerprint analysis. The tool will be used by Identity service and Police to quality check all INZ fingerprint. Testing will cover:

- Workflows associated with fingerprint
- Loading of fingerprints
- Searching fingerprints
- Quality check the fingerprints



- Editing fingerprints
- Delete Fingerprints
- Upload NIST file
- Create NIST file
- Extract Fingerprints

AMS

AMS is being changed to now be the master of the biographic rather than IGMS, so the Add, Edit and delete functionality will be reinstated in AMS. Changes will be made so that all images will be pulled from the NEC rather than AMS.

Early AMS Release

Due to the risk of issues happening when syncing data from IGMS to AMS then to NEC it was decided to look into completing the changes to AMS to include the additional fields and ensure that the data from IGMS is updated to these fields. It was found that these additional fields are already in the Databroker messages and only changes to SIH and AMS were required.

Regression

The following systems/applications have been identified as interfacing with the new IDME system but do not need changes so a regression will be run over each of them, to ensure that the BCU changes have not impacted them.

The following will be executed in Environment one:

- Mobile Regulator
- EOI
- ETA
- AMS
- ADEPT
- IGMS Online
- Other AMS file uploads
- DMS

The following will be executed in Pre-Production as they do not reside in either of the lower environments:

- APP (SITA)
- CUSMOD
- Movement Record System (MRS)

6(c) of the OIA



Thresholds

During SIT testing a set of base thresholds will be used to test the matching decision process. Testing will verify that the thresholds can be changed easily and that the changes are implemented correctly.

Usability

A round of usability testing will also be completed during this test phase to ensure that the application meets the usability Non-Functional requirements.

Also the business SMEs that represent the business will complete user testing to ensure that the solution is ready to be moved to the business acceptance testing phase.

Business users will be involved earlier during the SIT phase to get early feedback on the solution particularly around IPE and Reveal workflow.

Demos

Regular demonstrations will be completed by the BCU Test team to the Business stakeholders. The team will demonstrate areas of the system that are ready for review. This allows the users to see the solution early and enable early feedback.

Active Directory

User access testing will be completed ensuring that solution is using the correct active directory user groups. Testing will add and remove users from different AD groups and ensure that the users can only access the functions relating to the AD groups.

For IPE testing there will need to be further testing as there is another layer of access that is managed in LMS by an administrator. This functionality will be documented, and testing will confirm that the user only has access to the screen and workstations authorities in LMS.

Audit logging

The test analysts will check the logs to ensure that the auditing requirements are met across all the BCU Solution components.

Test Tools

- Azure Dev Ops
- Microsoft SQL Server - Database verification
- Selenium - Automation
- SortSite - Accessibility

Deliverables

Reporting dashboard will be set up in ADO to have the visibility on the Test execution progress and test status.

- Test Scripts
- Test Results
- SQL queries
- Test Exit Report
- Requirements traceability Matrix

Entry Criteria

- Test Exit reports from all System Testing components have been completed and approved
 - NEC
 - DxC
 - In Tech



- Argonaut
 - Datacom
 - Theta
- Requirements traceability matrix updated with MBIE test cases
- No Open Severity 1 or 2 Defects from System test
- Test Environment available and configured
- Test data has been created
- Smoke tests completed and passed
- Test preparation complete
- Test Plan has been completed and signed off
- All defects have had the severity and priority levels reviewed and agreed by MBIE
- All open defects have been reviewed by MBIE and aggregated severity 3 & 4 defects accepted with an agreed remediation plan
- All open defects have been reviewed by a business representative

Exit Criteria

- All test cases executed (except cases that have been removed from scope after review and approval)
- No Open Severity 1 or 2 defects
- All defects have had the severity and priority levels reviewed and agreed by MBIE
- All open defects have been reviewed by MBIE and aggregated severity 3 & 4 defects accepted with an agreed remediation plan
- All open defects have been reviewed by business/stakeholder representatives
- SIT Test Exit Report completed
- Migration Test Exit report completed

Performance Testing

Objective

To evaluate how the system performs in terms of responsiveness and stability under a particular workload.

Test Design Technique

Test scripts are designed from Non-Functional Requirements.

Test Execution Approach

Performance testing will provide details of how long a function will take between point 'a' and point 'b' with a specific number of users. A baseline will be run using the existing system and where possible compared to the new solution. Where the baseline is insufficient the business will review the results and be asked to approve the final timings.

Load testing will show how the function performs under an increasing load and determines at what point the performance becomes undesirable.

Soak testing is designed to execute load for an extended period to ensure stability and that there are no memory leaks.

Test execution of the scenarios will reflect expected performance characteristics, and will be expected to be undertaken in a production-like environment (Environment 2) in terms of

- Server and Storage capacity/compute
- Network Capability
- Database snapshot/backup
- Background processes which will run in production should run in the test environment

The following are the systems covered by this suite:

- AMS
- ETA
- Online visa applications
- ADEPT
- IPE

Entry Criteria

- Data Migration has been completed
- Latest code base has been deployed
- Test Environment available and configured
- Solution stable
- Test preparation complete
- Performance Test Plan has been completed and signed off
- Test tools in place
- All defects have had the severity and priority levels reviewed and agreed by MBIE
- All open defects have been reviewed by MBIE and aggregated severity 3 & 4 defects accepted with an agreed remediation plan

Exit Criteria

- All test cases executed (except cases that have been removed from scope after review and approval)
- No Open Severity 1 or 2 Defects
- All defects have had the severity and priority levels reviewed and agreed by MBIE
- All open defects have been reviewed by MBIE and aggregated severity 3 & 4 defects accepted with an agreed remediation plan
- Performance Test Exit Report completed and approved

Business Acceptance Testing

Objective

To assess if the system can support day-to-day business and user scenarios and ensure the system is sufficient, correct for business usage and the solution is fit for purpose.

Test Execution Approach

Each business scenario will be executed using an exploratory testing technique. This means the business user will execute the business scenario as they would during a normal working day to ensure that the solution is fit for purpose.

All steps will be documented during the test execution and logged in ADO under the project.

Test Analysts and INZ Business Analysts will be used to support the business users and ensure that all defects are analysed and prioritised appropriately.

The following business groups will be involved in the Business Acceptance testing:

- Identity Services
- Intelligence and Risk
- Border Officers
- Refugee Quota Branch - IPE
- Asylum (Refugee Status Unit) - IPE
- Compliance - IPE
- Visa Services
- NZ Police

Entry Criteria

- Test Exit report from System Integration Testing has been completed and approved
- No Open Severity 1 or 2 Defects
- All defects have had the severity and priority levels reviewed and agreed by MBIE
- All open defects have been reviewed by MBIE and aggregated severity 3 & 4 defects accepted with an agreed remediation plan
- The data migration has been completed successfully
- Test Environment available and configured
- Smoke test completed and passed
- Test preparation complete
- Test Plan has been completed and signed off (this document)
- Test tools in place

Exit Criteria

- All test cases executed (except cases that have been removed from scope after review and approval)
- No Open Severity 1 or 2 Defects
- All defects have had the severity and priority levels reviewed and agreed by MBIE
- All open defects have been reviewed by MBIE and aggregated severity 3 & 4 defects accepted with an agreed remediation plan
- Test Exit Report completed and approved



Business Verification Testing

Objective

To verify the successful deployment of all code and data into the Production environment.

Test Execution Approach

Test Data will be created to test the various channels to ensure that the full solution has been deployed correctly and everything is up and running. Once testing is completed this data will be removed.

The testing will be executed by the project teams Test Analysts and Business representatives, they will work together to create the test cases and execute these scripts.

This testing will be undertaken by the following:

- BCU Test Team
- Business Representatives

Entry Criteria

- Test Exit reports for all test levels have been completed and approved
- CAB has approved moving into production
- Bulk data migration has been completed successfully
- BVT Test scripts complete
- Approved SOM and ORR
- No open severity 1 & 2 defects and aggregated Severity 3 & 4 defects accepted with an agreed remediation plan

Exit Criteria

- All systems are up and running.

Test Management Tools

The BCU Test Teams will use the following tools, for test planning; management; reporting and execution.

Tool	Purpose	Used by
Azure Dev Ops	Test Artefacts Test Execution scheduling and management Progress Reporting via Dashboards Test Case traceability to Business Requirements Defect Repository	BCU Test Team
Selenium	Test automation tool	BCU Test Team
Postman	API Test Automation	BCU Test Team
JMeter/Visual Studio Load Test	Performance Testing	BCU Test Team
WAVE tool (Chrome Add-on)	Usability testing. Assess the accessibility of website content	BCU Test Team
SortSite®	Automated web site testing tool for analysis of Accessibility; Usability and Web Standards	MBIE Digital Information Tools team

Test Execution Schedule

A test execution schedule will be created to ensure that all planned tests are executed within the allocated timeframe. The schedule will be used to report actual verses planned tests and give an early indication of whether the testing is on track or not. There will be no tests planned for release days as this day will be used to re-test defects and re-run the failed test cases.

Test Wrap up

The following tasks need to be completed to hand over to the BAU test team:

- Test users and set-up process documented
- INZ BAU Confluence page created and updated with testing deliverables
- Test assets handed over to INZ BAU (e.g. IPE Capture kits and laptops)
- Walk through with BAU test team
- All defects in ADO with current status, defects “Closed – Accepted by INZ” are documented.
- Regression suite updated

Deliverables

Deliverable	Responsible	Delivery Date
BCU Functional Test Plan	Test Manager	
Performance Test Plan	Performance Test Engineer	
BCU Non Functional Test Plan	Non Functional Test Engineer	
Test Cases	Test Analyst/s	
Traceability Matrix	(Lead) Test Analyst	
Test Results	Test Analyst/s	
SIT Test Exit Report	Test Manager	
DM Test Exit Report	Test Manager	
Performance Test Exit Report	Test Manager	
Business Acceptance Exit Report	Test Manager	
Regression Test Suite	Test Analyst/s	



Test Suspension Criteria

At any time, test execution may be suspended where:

- The severity or volume of defects is deemed sufficient to seriously jeopardise the quality and integrity of the test effort
- Continued test execution is deemed to no longer be adding value

A recommendation to suspend testing may be made by the Test Manager, but the final decision shall be made by the MBIE Project Manager and Business Owner, Systems Owner as per Roles & Responsibilities.

Testing will be suspended until the defect or other issues that led to the suspension have been satisfactorily resolved, or an acceptable workaround has been identified and implemented. In the event that this results in a change in Requirements and/or Solution Design the Project's Change Management Process is to be invoked.

Test Suspension criteria are detailed in Table below:

Short Description	Long Description
Environment Availability	The application/environment is identified as unstable, or unavailable
Significant Defects/Rework	Incorrect functionality/configuration of a core component, requiring significant investigation, prevents further testing
	Significant design changes are required that will prevent further testing
Resource Availability	Insufficient people to undertake testing, i.e. resource is required on other higher priority tasks/projects
	Absence of critical technical / support resource or SME to resolve an issue or a defect.

6. Test Team Structure and Roles

Roles and Responsibilities

Role	Responsibilities
Systems Owner	• Approver of Combined Test Plan • Approver of Test Exit Report • Approver of any suspension of testing
MBIE Project Manager	• Approver of Combined Test Plan • Overall planning and IT resourcing of the project • Hand-over of completed solution to ICT Operations and Support • Work with INZ to assign business resources for Acceptance Testing • Member of Defect Management Committee (may delegate) • Approver of any suspension of testing • Approver of Test Exit Report • Vendor Manager
Vendor Project Manager and/or Vendor Test Manager/Lead	• Project escalation point for Vendor Test Team • Overall Vendor management of development and test activities • Member of Defect Management Committee For responsible system testing • Creation of Level Test Plans; Test Cases and Traceability Matrix • Progress reports • Test Execution • Defect management and retesting • Test Level Exit report
MBIE Solutions Architect	• Reviewer of Combined Test Plan • Assist with definition of MBIE Test Environment/s builds • Supply Part B design doc – with test environment and interface component requirements • Member of Defect Management Committee • Consulted with prior to any suspension of testing • Approver of Non Functional Test Exit report • Review of Functional Test Exit Report • Non-functional - Technical Reviews
Security Architect	• Creator for risk assessment • Creator of Test Purpose for Security Vendor • Organize access for Security tester • Liaison between Security Vendor and project team • Attend daily security meeting
INZ Business Analyst/s	• Reviewer of Combined Test Plan • Reviewer of Test Exit Report • Member of Defect Management Committee • Defining migration threshold's • Requirements clarification • Work with ICT Test Analysts to scope and document Business Acceptance test scenarios • Support Business Acceptance Testing • Non-functional test execution – Usability • Review test coverage via reviewing test cases • Priorities test cases in conjunction with test analysts
ICT Business SMEs	• Reviewer of Combined Test Plan • Reviewer of Test Exit Report • Member of Defect Management Committee • Requirements clarification • Review test coverage via reviewing test cases

Role	Responsibilities
BCU Test Manager	• Manage the overall testing of the BCU and IPE testing • System Integration • Migration • Performance • Business Acceptance • Operational Acceptance (Non Functional) • Production Verification • Allocates and supports BCU test resource/s • Testing escalation point for Test Team • Creator of Combined Test Plan • Creator of Test Exit Report • Review Vendor test deliverables • Reports testing related risks and issues • Provides test progress report to the Project Manager • Recommends any suspension of testing • Chair of the Defect Management Committee • Manager of the Defect Process • Coordinator of Business Acceptance testing • Approve the Automation Framework
BCU SIT Test Lead	• Day to day management of SIT testing • Contributor into the Daily progress report • Contributor to the SIT Exit report • ICT Test Analysts responsibilities as below
MBIE Senior Test Analyst/s	• Create and manage MBIE test artefacts • Review Vendor test deliverables • Test execution • Defect management, including maintain defect register and retesting • Support and assist Business Acceptance Testers as required • Support and assist end/external user testing as required • Non Functional testing – usability, accessibility, audit and logging • Review existing regression suites • Regression testing of existing systems • Contributes to: • Combined Test Plan • Status / Progress Reports • Test Exit Report
MBIE Performance Test Engineer	• Create Performance Test Plan • Create test data • Create test scripts • Execute test scripts • Create Performance Test Exit report • Defect management, including maintain defect register and retesting
External Security Tester	• Create Security Test Plan • Create Security test scenarios • Execute test scenarios • Create Security report
Subject Matter Experts and Business Acceptance Testers	• Creation of Business scenario test cases • Execute Business Acceptance Testing • Raise defects / issues (via ICT Test Analysts) • Defining migrated thresholds • Execute Business Verification Testing in Production
MBIE Test Environment Manager & Release Planner	• Manage MBIE Test Environment requests and schedule • Manage MBIE Test Environment access • Identify and manage Test Environment conflicts with other projects • Approver of code deployments

7. Testing Schedule and Environments

Testing Milestones

For the latest testing schedule select the following mako link:

s 6(c)

Env	Phase		
SIT	Smoke test	3/July/2023	7/July/2023
SIT	First cycle	9/July/2023	21/Jul/2023
SIT	s 6(c)	17/Jul/2023	4/Aug/2023
SIT	Second Cycle	24/Jul/2023	4/Aug/2023
SIT	Third Cycle	7/Aug/2023	18/Aug/2023
UAT	Smoke test	21/Aug/2023	25/Aug/2023
UAT	First cycle	28/Aug/2023	15/Sep
SIT	s 6(c)	17/Jul/2023	4/Aug/2023
UAT	Second Cycle		
Pre Prod	Smoke test		
Pre Prod	First cycle		
Prod			

Test Environments

The following table summarizes at a high level the test environments that will be available for each test level. Due to the fundamental changes to the identity process each of the environments will need to be managed carefully to ensure that BCU work does not impact any new projects or BAU changes.

Environment	Brief Specification	Activity / Test Levels
Vendor Development	Vendor hosted. Sufficient for unit testing of developed components. Integration with other components or external sub-systems may be stubbed.	Unit Testing
System Test – Vendor Environment	Vendor hosted. Integrated system components in a low performance environment. External sub-system interfaces may be stubbed	System Testing
System Integration Test (SIT) – Environment 1	MBIE hosted. A fully integrated low performance environment with real-time connectivity to, test instances of, all other internal and external sub-systems.	System Integration Testing Data Migration

Environment	Brief Specification	Activity / Test Levels
User Acceptance Test (UAT) – Environment 2	MBIE hosted. Fully integrated, high performance environment with production configuration and real-time connectivity to, test instances of, all other internal and external sub-systems.	Business Acceptance Testing Data Migration Performance Testing
Pre-Production	MBIE hosted. A fully integrated, mirror of production with connectivity to all internal and external sub-systems.	Data Migration Security Testing Dress rehearsal

8. Test Management Procedure

Test Progress Reporting

Test progress reports will be available to Project and Test Management teams weekly or as required. It is anticipated that progress reporting will make use of Azure Dev Ops Report Dashboard. The test management tool that will be used for these projects is Azure Dev Ops for Test Design, Test Execution and Defect Management.

Defect Management

Defect Management processes will follow [BCU Defect management process](#)

All open System defects from the vendors will be logged in MBIE ADO repository when MBIE SIT testing commences.

MBIE defects will be logged into ADO with Severity and Priority ratings. When the defect is reviewed by the Defect Triage Committee the ratings may be reset. Defect meetings will be scheduled by the BCU Test Manager and will be run twice a week

Severity

Severity level refers to the degree that the defect impacts or affects the system.

The impact of the defect on the application (system-wide, one module, single function) as well as the impact on the business or technical environment is also taken into account when assigning a severity.

Defect Severity Level	Description
Critical	A termination of the complete system or one or more components of the system and causes extensive corruption of the data. The failed function is unusable and there is no acceptable alternative method to achieve the required results.
Major	A termination of the complete system or one or more components of the system and causes extensive corruption of the data. The failed function is unusable but there exists an acceptable alternative method to achieve the required results.
Moderate	A defect that does not result in the termination, but causes the system to produce incorrect, incomplete or inconsistent results then the severity will be stated as moderate.
Minor	A defect that does not result in termination and does not damage the usability of the system and the desired results can be easily obtained by an acceptable work around.
Cosmetic	A defect that is related to the enhancement of the system where the changes are related to the look and feel of the application then the severity is stated as cosmetic.

Priority

Priority defines the order in which we should resolve defects. It is set by the tester as an indication of how quickly a resolution is required, usually to support the test execution timeframes.

Priority	Description	Response Time
High	Must be resolved as soon as possible because the defect is severely affecting the application or the product. The system cannot be used until the repair has been done.	2 hours
Medium	The defect should be resolved in the normal course of development activities. It can wait until a new build or version is created.	New release
Low	The defect is an irritant which should be repaired, but repair can be deferred until after more serious defects have been fixed.	Planned release

Defect Management Committee Meetings

ADO will be the central defect repository and used to facilitate the management and tracking of the following:

- Defect Recording/Logging
- Defect Analysis
- Defect Tracking
- Defect Reporting

The purpose of the defect committee is to provide the project with a forum for reviewing and confirming the prioritisation of defects as well as providing information to enable the business to prepare workarounds that may be required for those defects that are not fixed prior to deployment.

During System Integration Testing and Business Acceptance testing it is anticipated these meetings will be held twice weekly, they will be facilitated by the BCU Test Manager and initiated at the commencement of test execution. If participants are not able to be on site there will be a Microsoft Teams meeting set up.

Representatives of the test team and vendor development teams will attend these meetings with support from the project management team, business owners/representatives and other project stakeholders where necessary.

The objective of the defect committee is to:

- Confirm defect severities, priorities, and resolution timeframes
- Keep the Project / Business informed and involved
- Provide a forum to talk through issues relating to the defects i.e., workarounds,
- Resolve discrepancies which may lead to the requirement for Enhancements/Change Request to be raised, and
- Make decisions as to whether testing or implementation can proceed with a particular defect present where that defect is deemed critical or important to the business and cannot be fixed and retested before exiting a test phase or implementing to production.
- Schedule defects for release

Builds/Releases

Test execution will be planned around defect builds which will contain defects fixes and no new functionality. These will be scheduled in the defect management meetings and approved by the release managers.

Each build will have a smoke test completed and testing will not commence until the smoke tests have passed.

All defect retesting will be completed on the defects, regression testing around the defect will then be executed and then the original failed test case will be re-run.

9. Assumptions & Dependencies; Risks and Issues

Assumptions

The following assumptions have been used when preparing this document:

#	Assumption	Impact if incorrect
A1	Hardware for IPE is available at the start of testing	Testing will need to start later
A2	The BCU testers have existing knowledge of the existing systems so understand the images and issues/limitations of the existing system	Testing will take longer than estimated
A2	Data Migration Reconciliation report available for the test team prior to test execution phase	Migration due to inconsistent data will have negative impact on Functional Testing
A4	At least one of the migration testers have data migration testing experience	Testing may take longer than estimated
A5	The architects will verify the non-functional requirements that do not need a test activity and review the test evidence of the other NFRs	Technical tester will need to be resourced
A6	The System Integration and Migration test phases have been estimated by the identity testers using the BCU requirements only.	Estimates will need to be reviewed
A7	BCU Test team is available to support business users during Business Acceptance testing	Estimates will need to be reviewed
A8	System Test exit reports are signed off before SIT commencement	SIT Test phase will not be able to start on schedule
A9	Defects post System Test will be managed in MBIE ADO repository	Defect Management gets difficult

Dependencies

Delivery of this testing is dependent on:

#	Dependencies	Impact
D1	The creation of the test scripts for Business Acceptance Testing is dependent on the Business processes being completed.	Business Acceptance Testing cannot start
D2	Business SMEs are available for Business acceptance testing and creation of the test cases	Project implementation date may be impacted

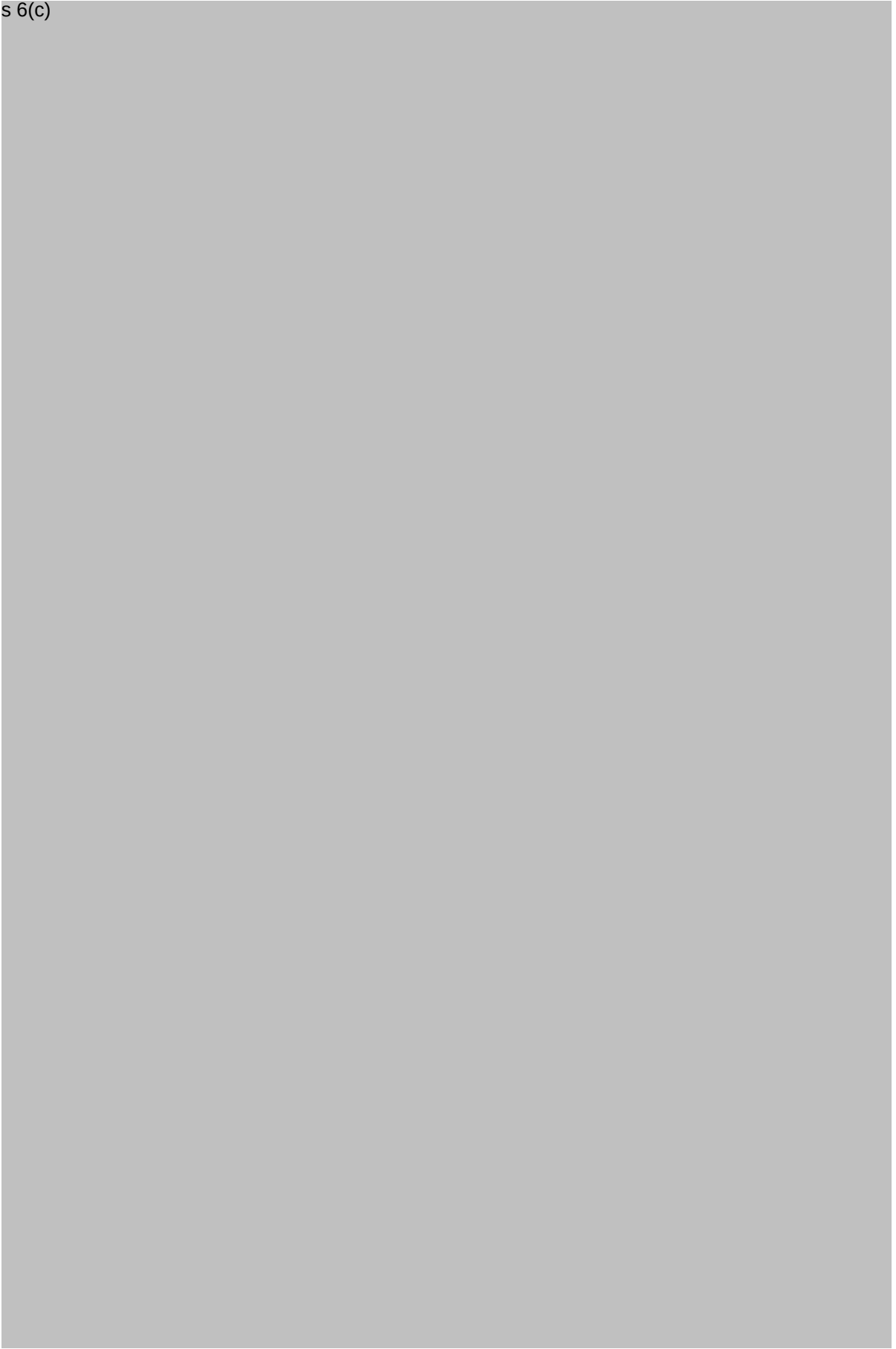
Risks

The following Risks, and mitigations, have been identified during the preparation of this document and will be recorded in the Projects Risk Register for visibility and management. Any further Risks identified will also be recorded and managed via the Projects register.

s 6(c)



s 6(c)



Issues

The following issues have been identified during the preparation of this document and will be recorded in the Projects Issue register for visibility and management. Any further issues identified will also be recorded and managed via the Projects register.

#	Title	Issue	Mitigation	Status
I1				
I2				

Appendix A: Test Types

Test type	Description
User /Business Acceptance testing	Formal testing with respect to user needs, requirements, and business processes conducted to determine whether or not a system satisfies the acceptance criteria and to enable the user, customers or other authorized entity to determine whether or not to accept the system.
Accessibility	Testing to determine the ease by which users with disabilities can use a component or system. Includes compliance with NZ Govt. web standards. NB: See also MBIE's standard Usability checklist
Auditability	Testing to determine that that Audit requirements of the system have been met.
Back up & Recovery	The process of testing to determine the recoverability of a software product. Verifies that the system meets requirements for recovery after a failure, including ability to recover data, database, object, workspace and state; backup and recovery processes; time to recover; disruption and interference for other users.
Concurrency Testing	Testing to determine how the occurrence of two or more activities within the same interval of time, achieved either by interleaving the activities or by simultaneous execution, is handled by the component or system.
Conversion Testing (aka Data Migration)	Testing of software used to convert data from existing systems for use in replacement systems.
Configuration Testing	The process of testing to determine the portability of a software product. Verifies that the application operates successfully in all production configurations, may include: • Browser (type and version) • DBMS • Other software and version dependencies (e.g. MS-Office applications, data access components, drivers, add-ins, Citrix) • Hardware • Deployment method and process
Content Management	Process to verify that the content to be published in production ready. For MBIE, this should be managed by the Business / Content Managers and may include reviews by policy and legal teams.
Documentation Testing	Testing the quality of the documentation, e.g. user guide or installation guide. Applicable methods will be Inspection, Reviews etc.
Functional Testing	Testing based on an analysis of the specification of the functionality of a component or system. Verifies that the application is usable, works correctly, completely and as specified. If applicable, test requirements will include workflow (business scenarios – alternative flow of events) which might cross use case boundaries, or which represent special test requirements, i.e. transaction level tasks, business cycle functions, data processed. Test design should include coverage of both valid and invalid scenarios and would typically employ black-box testing techniques such as boundary value analysis; equivalence partitioning. Where applicable, testing shall include 'in-flight' and 'new' data
Graphical User Interface (GUI)	Testing performed by interacting with the software under test via the user interface. Includes testing areas such as: • Mandatory data / fields • Field picklists & dropdowns • Field and screen navigation
Integration Testing	Testing performed to expose defects in the interfaces and in the interactions between integrated components or systems.
Interface Testing	An integration test type that is concerned with testing the interfaces between components or systems.

Maintenance Testing (including Warranty Testing)	Testing the changes to an operational system or the impact of a changed environment to an operational system. Includes data-fix testing.
Operation Acceptance Testing	This testing evaluates operational readiness for a software application prior to the release to the production. Operational Acceptance Testing ensures system and component compliance in the application's standard operating environment (SOE). The testing is based off the Non-functional requirements.
Performance Testing	The process of testing to determine the performance of a software product. Can include Stress, Volume, Load and Soak testing
Production Acceptance Testing (aka Deployment Test)	Testing conducted to evaluate a component or system in its operational environment. Also known as Operational Acceptance and Production Installation Verification (PIV) testing.
Regression Testing	Testing of a previously tested program following modification to ensure that defects have not been introduced or uncovered in unchanged areas of the software, as a result of the changes made. It is performed when the software or its environment is changed.
Reports Testing	Testing to determine that report content, format and output meets requirements. Where applicable, shall include testing against production configuration and hardware.
Security Testing	Testing to determine the security of the software product; generally at a functional or user level rather than penetration by "hackers" via the internet
Smoke Testing	A subset of all defined/planned test cases that cover the main functionality of a component or system, to ascertaining that the most crucial functions of a program work; but not bothering with the finer details. A daily build and smoke test is among industry best practices.
System Testing	The process of testing an integrated system to verify that it meets specified functional and non-functional requirement.
System Integration Testing	Testing the integration of systems and packages.
Unit/Component Testing	The testing of individual software components.
Unit/Component Integration testing	Testing performed to expose defects in the interfaces and interaction between integrated components.
Usability	Including compliance with: • Government web standards • Identity and Branding NB: Guided by MBIE's standard Usability checklist

Appendix B: Functional Requirements In-Scope

The functional requirements for BCU are detailed in the documents in the list below (all of which are listed in the document reference in this document also). Key additional/new functional requirements added by BCU are listed below.

BCU requirements documents:

Document title	Version	Location / ID
NEC IDMe Business Requirements	1.3	s 6(c)
NEC IPE Functional Specification	2.4	
NEC IPE Hardware Requirements	2.1	
NEC BCU Non Functional Requirements	1.0	
NEC BCU NFR Support Data	1.0	
AMS Changes Detailed Requirements	0.7	
Argonaut SRTP Business Requirements	6.8	
InTech IQOffice Business Requirements	0.9	
Datacom IGMS BCU Business Requirements	0.7	
Theta BCU Azure Business Requirements	0.3	
In-Person Enrolment (Part A) FINAL	1.3	
BCU Architectural Solution Design Part A – FINAL	1.5	
s 6(c)	2.8.2	
AMS BCU External Concurrency Design	v93	
AMS BCU Additional Features Design	v3	
AMS BCU Detailed Design AMS and SIH	1.0	
BCU Infrastructure - SIT Solution Design Infrastructure Part B	3.6	

Appendix C Traceability Matrix

[Link to SS](#)

Appendix D Test User Pre-requisites and configuration

Prerequisites:

s 6(c)





**MINISTRY OF BUSINESS,
INNOVATION & EMPLOYMENT**
HĪKINA WHAKATUTUKI



Immigration New Zealand

Biometric Capability Update (BCU) Solution

Performance Test Plan

Version: V 1.3.1

Date: 21 October 2024

Table of Contents

Table of Contents	2
1. Performance Testing Objectives	7
2. Project Overview	7
2.1 Biometric Capability Update (BCU)	7
3. Performance Testing Scope.....	8
3.1 Scope	8
3.2 Out of Scope.....	9
3.2.1 Scenarios Out of Scope.....	9
4. Performance Test Approach	9
4.1 Performance Test Principles.....	10
4.2 Performance Test Suites	11
4.3 Test Strategy.....	12
4.3.1 Performance Test Types.....	12
4.4 Test Throughput Details.....	14
4.4.1 ADEPT Load Profile Breakdown.....	14
4.4.2 AMS Load Profile Breakdown.....	14
4.4.3 NZeTA Load Profile Breakdown.....	15
4.4.4 IGMS Load Profile Breakdown.....	15
4.4.5 IPE Load Profile Breakdown	15
4.4.6 6(c) of the OIA	15
4.4.7 IDMe Load Profile Breakdown	16
4.5 Performance Metrics.....	16
4.7 Issue Analysis.....	16
5. Environments	17
5.1 Test Environments and Usage.....	17
6. Deliverables	18
6.1 Testing Schedule	19
7. Defect Tracking and Reporting.....	20
7.1 Defect Handling.....	20
8. Risks Assumptions Dependencies Constraints.....	21
8.1 Risks/Events	21
8.2 Assumptions.....	24
8.3 Dependencies.....	24
8.4 Constraints	25
8.5 Test Resources.....	25
9. Entry & Exit Criteria	26

9.1 Performance Test Entry Criteria.....	26
9.2 Performance Non-Functional Requirements	27
9.3 SIT and NFR Test Exit Report	27
9.4 Performance Test Exit Criteria	27
10. Appendix A.- Data Classes and Types.....	29
11. Appendix B.- Process Table Template	30
12. Appendix C.- Inter-component throttling values.	32
13. Appendix D.- Resource monitoring parameters and intervals by Node.	33
14. Appendix E.- List of testers for manual UI transactions while BCU system is under load. 34	
15. Appendix F.- Template for recording manual UI transactions (during performance testing) recording.	35
16. Appendix G.- List of NFRs the inform and are informed by this test	Error! Bookmark not defined.

Document Control

Document Information

Document Name:	INZ Biometric Capability Upgrade - Performance Test Plan
Contact Person:	s 9(2)(a)
Status:	V 1.3.1
Mako Ref	152725065

Document History

Author	Description of Change	Date	Version
s 9(2)(a)	Initial Draft	10/05/2024	1.1
	Review Comment Updated and Load Profile from NFR support document inserted	31/05/2024	1.2
	Responses to SME review comments	6/Aug/2024	1.2a
	Ready for signing – Feedback and response in previous version. Changes accepted	13/Aug/2024	1.2b
	Further comments accentuating the need for higher forecast volumes to be added (as per revised business forecast). And, looking for validation that submitting total volume via AMS is equivalent to submitting transactions from the ADEPT, NZeTA, igms User Interfaces	26/Aug/2024	1.2c
	Changes incorporated to reflect feedback from INZ systems Manager and INZ Business Analysts. Mako reference added to doc control panel.	20/Sep/2024	1.2d
	Additional comments responded to and minor changes made. NFRs in play appendix added.	9/Oct/2024	1.2e
	Approval email link added for INZ s 9(2)(a) Comments cleared and table of contents fully updated to deal with any shift in page spacing.	15/Oct/2024	1.3
	Added changes to the SmartScan IPE to be included in the soak test and to have 300 enrolments uploaded in each test for the offline mode.	21/Oct/2024	1.3.1

Reviewed by

Name	Role	Date	Signature
s 9(2)(a)		v1.2 – 31/05/2024	
		v1.2 – 31/05/2024	
		v1.2 – 31/05/2024	
		v1.2 – 31/05/2024	
		v1.2 – 31/05/2024	
		V1.2b – 20/08/2024	

Document Approval

Signatory	Role	Date	Signature
s 9(2)(a)		15/Oct/2024	Mako id= 164898104
		22/Oct/2024	Mako id= 165182879

Document Distribution

Name	Role
s 9(2)(a)	

s 9(2)(a)

1. Performance Testing Objectives

The objective of Performance Testing is to validate the following.

- **Current Volume Handling**

The new system performs efficiently and within acceptable ranges for the current load throughput as defined under the NFRs. This ensures that the system meets existing demand without degradation in performance.

- **Future Volume Projections**

The system's ability to handle increased volumes over the next few years, reflecting expected growth in user base, transactions and data. This will validate that the systems is scalable and prepared for future demands without a need for a significant upgrades or redesigns.

- **Peak Load Resilience**

The system's performance under peak load conditions, which simulate the maximum expected traffic or activity levels. This ensures that the system can handle occasional spikes in demand without failure or significant slowdowns.

- **Stress Testing**

Identify the system's breaking points by progressively increasing the load beyond normal operational limits until the system fails. This allows for the identification of any bottlenecks, weaknesses or areas requiring optimisation, and provides an understanding of system behaviour under stress, which in turn informs preparations for such a scenario and input for any future systems changes to compensate or improve our ability to manage the situation.

- **Impact on Integrated Systems**

Verify that other integrated systems are not adversely impacted by the new system's performance, or vice versa, ensuring that under-performance or bottlenecks in the MBIE system do not degrade the performance of these inter-dependent systems.

- **Bottleneck Identification**

Identify specific points of system degradation or performance bottlenecks. This will help in recognizing areas where improvements are needed to enhance overall system efficiency and responsiveness, and inform future system enhancement and incident management approaches.

- **Meeting Non-Functional Requirements (NFRs)**

Confirm that all performance related NFRs, including response times, throughput, and system reliability, are met under varying loads and stress conditions.

2. Project Overview

2.1 Biometric Capability Update (BCU)

The Identity Management solution (IDMeS) is a key solution supporting INZ as the authoritative source of identity information for all non-New Zealanders, the processing of visa applications and border risk management. The MBIS application provides the core functions of the new IDMeS solution. These functions include the Automated Processing and Biometric Matching sub-

functions. Other applications which are part of the IDMe solution include s 6(c), Reveal and IBW.

The Biometric Capability Update IDMe s 6(c) solution has been designed to address INZ projects needs and future known capability by upgrading the versions of biometric, biographic matching and management platforms, rationalising, and simplifying the platform to reduce on-going cost and improving the flexibility and utility of the system in the process. This is a core capability for INZ's future protection in an environment where identity fraud, terrorism and other sources of harm are prevalent and increasingly diverse and sophisticated, and this upgraded capability is crucial to achieving that future.

3. Performance Testing Scope

3.1 Scope

The following components/functions are within the defined scope of testing:

System	Functionalities
MBIS	Create/Edit Identity
SmartScan(IPE)	Enrol an Identity (Online and offline. 300 registrations bulk upload) during load and stress test phase. Also during the soak test if time allows.
Reveal	
IBW	
s 6(c) of the OIA	Capture Biometric and Biographic Data
IQ Office	Match (face finger biographics)
AMS	Adhoc Search
These listed below are not systems under test. Simply consumers of the IDMe s 6(c) services.	Visa, Travel Authority, and other applications that have identity elements associated with same applications. These systems are participant systems and while not under test, are involved in sending and receiving data from the systems in the previous row.
IGMS	
NZeTA	
ADEPT	

MBIS has integration with multiple systems and to assess the stability and performance of the system, all the integrated systems will generate transactions in parallel. Load will be generated using both manual s 6(c) and automated suites s 6(c).

Volumes (transaction per unit of time) will be as per the commercial terms, and also, the more recently revised (increased) volumes provided by INZ business staff.

The more recent production load volume analysis can be found here:

s 6(c) of the OIA

3.2 Out of Scope

3.2.1 Scenarios Out of Scope

s 6(c)



4. Performance Test Approach

The following sections describe the approach to be undertaken for performance testing.

Approach

This will be an integrated end-to-end performance test across the 6(c) of the OIA and IDMeS, DataBroker and DMS systems. Performance testing will be done to understand the transaction processing performance profile for IDMe systems and associated systems (being AMS, ADEPT, NZeTA, 6(c) of the OIA and IGMS).

Vendors, BCU Project team and ADEPT performance team will provide support during the overall performance test by running their performance scripts during each run. The manually entered ADEPT, IGMS, NZeTA and s 6(c) enrolled identities (stored offline), and AMS will be used to generate load to test the IDMe solution.

AMS will be the point of injection for the majority of the automated/harness driven load injection (ADEPT may be used if the performance test harness used by ADEPT has been updated to use compliant, well-formed identities without re-using faces with new/random biographic data). MBIE will provide a run-sheet prior to each of the test execution runs with the list of tasks

¹ Unless a cost effective method is discovered to script the loading of records into SmartScan.

to be done by each of the responsible parties. MBIE will be responsible for coordinating performance test executions. Test result details will be collected from respective vendors (Datacom, NEC, Theta, DXC and Argonaut) to analyse the performance of the systems. A dry run will be completed before the actual performance tests are run to check the connectivity and state of the environment.

4.1 Performance Test Principles

The following principles will be applied within the approach of Performance Testing:

Principle	Description
End User Perspective	- While the system is under load, stress and soak tests, users will create transactions from applications like s 6(c) 6(c) of the OIA IBW, ADEPT, AMS, IGMS, NZeTA against the systems under test. - In addition to border type IPE transactions, the upload of 300 offline In Person Enrolments will be submitted. These should also be distributed across 2 or 3 SmartScan devices operating/uploading concurrently. - A mix of (mostly script generated transactions) along with, a smaller volumes of manually entered transactions, will drive the test transaction volumes across the integrated environment.
Early Scripting	- Scripting can be developed in SIT environment and will be modified incrementally to maintain integrity as changes are made. - Scripting within the integrated environment, to allow for MBIE and Integration specific aspects within the scripts. - Scripts will then be migrated to UAT, where test execution will happen.
Production-Like Environments	Test execution of scenarios, to reflect expected performance characteristics, are expected to be undertaken in a production-like environment (UAT).
Background Processes	Background processes are built and configured during scripting in line with expected production behaviours. These processes are assumed to be running concurrently during the performance soak test execution.
Monitoring and Reporting	- s 6(c) - The NEC MBIS dashboard will provide the ability to view the status of transactions. Direct SQL queries (after the test execution run is complete) to system and audit log tables will be used to complement the MBIS dashboard information and to confirm transaction volume processed. - Reporting on the three match result outcomes (match, undecided and new identity) as well as manual resolution workflow performance will be important to assess the validity of the performance testing.

4.2 Performance Test Suites

The below table contains the details of Performance test suite(s) which will be used for the Performance Testing.

System	New/Existing	Test Tool
ADEPT	Currently there are no automated performance suite for ADEPT that meet the project need. Transactions will be generated manually if the ADEPT team has not completed the development of suitable scripts to bypass the IDMe stub** ²	N/A
SmartScan (MBIE/IPE)	Records will be created manually from the IPE test devices during the test run. In addition to the in-person enrolment with online/real-time identity enrolment, offline capture of identity data will be entered manually and saved to be uploaded during load and stress test phases. Another upload of 300 identities may be included in the soak test phase if time and resources allow.	N/A
IBW	Manually processed IBW transactions, while the bulk of the test transactions are injected, will verify that workable response times are supported while the overall system is under load and/or stress. ³	N/A
	6(c) of the OIA	
AMS (DXC)	Existing Performance Suite with updates to accommodate BCU changes.	s 6(c)
NZeTA ⁴	Currently there is no automated performance suite for NZeTA. s 6(c) and the antivirus filescanner are also in play here and the throttle settings affect maximum test throughput.	Bulk upload via file where available
IGMS	s 6(c)	N/A

² **ADEPT has work in progress to adapt the ADEPT project's approach to performance testing. The ADEPT team is moving away from using the IDMe stub to having a portion of transactions flow to IDMe.

³ To address a question raised during review of this document. The load profiles submitted by INZ after project initiation can be found in mako doc with ID=162080878

⁴ s 6(c)

4.3 Test Strategy

4.3.1 Performance Test Types

The plan for IDMeS Performance Testing is to run the following test types representing the load expectations on the solution:

- Scenario 1 – Load Test
- Scenario 2 – Stress Test
- Scenario 3 – Soak Test

Base test transaction throughput and durations for the Load Test have been taken as a starting point from the NFR document titled “NFR Support Data for the NEC IDMeS solution”⁶. Additional (higher) test levels and longer test durations have also been included as ‘B’ tests at the request of the business review. As the ‘B’ tests are more resource intensive and take longer, there will be a cost and time impact to the project.

Performance testing scripts and execution should continue into the BAU lifecycle to support all future change to INZ systems.

Test Type	Test Description	Duration	Load
Average Load Test	The test simulates the system under normal load conditions, reflecting the average number of transactions that occur during day to day operations. The goal is to validate that the system performs within acceptable limits for response time, resource utilisation and error rates under these conditions.	2 Hours	100% average Load
Peak Load Test B	The Peak load test pushes the system to perform under maximum expected load conditions, simulating high-traffic events/peak operational periods. The aim is to ensure the system remains stable and responsive during these spikes in activity.	2 Hours	100% Peak Load
Stress Test A	This test gradually increases the system load until performance starts to degrade and to the point where the system fails. The	4 Hours	300% Peak Load

⁶ The “NFR Support Data for the NEC IDMeS solution” document (has no mako id) has been noted as being embedded in the “Non-functional Requirements for the NEC IDMeS solution” (mako link_id=111107756)

Test Type	Test Description	Duration	Load
	goal is to observe how the system handles increased pressure, identify any weak points, and understand its limits in terms of transaction volume, user concurrency and resource utilisation.		
Soak Test A	This test will simulate average daily transaction volumes for a continuous 24-hour period to detect any issues such as memory leaks, resource exhaustion, system slowdowns. The goal is to ensure the system remains stable and performs within acceptable limits for the entire duration.	24 Hours	100% Average Load
Soak Test B	The test will extend the average load scenario for a full 72-hour period. It aims to capture any long-term issues that may not surface in shorter tests, such as gradual memory leaks or resource depletion.	72 Hours	100% Average Load
Soak Test C	This test will simulate peak operational loads for a 24-hour period. The goal is to ensure the system can handle maximum expected traffic continuously for a full day without degradation.	24 Hours	100% Peak Load
Soak Test D	This test will push the system to maintain peak load for 72 hours continuously. The goal is to ensure the system can handle sustained high traffic without performance degradation or system failure over multiple days.	72 Hours	100% Peak Load

4.4 Test Throughput Details

IDMe Concurrent Throughput Details:

Source	Action	100% Average Hourly Load (24 hours)*	100% Peak Hourly Load (24 hours)*
AMS	DB15 API messages are sent from AMS for create or an edit identity. This will include all identities captured from an Online application (IGMS and ADEPT), and NZeTA and within AMS. Return Final DB01 message from MBIS.	s 6(c)	
	A DB18 message is accepted into IDMe with instructions to move an identity.		
	6(c) of the OIA		
IQ Office	Biographic matching		
MBIS**7	Biometric matching (Total/No match)		
SmartScan(IPE)	Individual submission (border ops)		
	Bulk Enrolment submission(from offline enrolment)		

*Revised volumes (above originally contracted) have been interpreted from the document provided by INZ- stored in mako at this link: The more recent production load volume analysis can be found here:

6(c) of the OIA

4.4.1 ADEPT Load Profile Breakdown

s 6(c)

4.4.2 AMS Load Profile Breakdown

Source	Action	100% Average Hourly Load (24 hours)	100% Peak Hourly Load (24 hours)
AMS	Create/Edit Identity	s 6(c)	
	Move Identity		

Transactions will be injected via AMS as the main source of load to MBIS. The channel value in each transaction record will be portioned to emulate the various transaction's source. i.e. if 50%

⁷ Test users will carry out typical tasks, in particular on litmus points concurrently with the load, stress and soak tests times to observe and measure UI response times.



4.7 Issue Analysis

Additional deep dive analysis will be carried out by project team where transactions are aborted or failed during the performance run. Resolution/mitigations will be investigated with any un-resolvable issues requiring business acceptance prior to go-live. Any fixes may require functional testing prior to further performance retesting.

The tests may need to be re-run, because of issue analysis findings, that require either; a code change, Database index adjustments or configuration changes (or any combination of these 3).

⁸ These values (for all the table) will need to be adjusted given the numbers altered by the business in other sections.

⁹ Source data capture during each test run will allow further statistical analysis to determine if a normal distribution is appropriate or if some other distribution profile better informs the test acceptance party

5. Environments

This section provides information about environments required for performance testing.

5.1 Test Environments and Usage

The following table summarises test activities undertaken within the test environments:

Environment	Usage
SIT (AMS UAT1)	• Performance Scripting
UAT (AMS UAT2)	• Performance script updates • Performance test execution

6. Deliverables

Descriptions of deliverables for the Performance Testing activity are as follows:

Deliverable	Description
Performance Test Plan	Performance testing plan (this document) describing performance testing approach.
Run Summary report	Findings will be reported as and when applicable relative to findings. Any areas of concern or failures will be reported as and when they occur. This will facilitate discussion around outcomes at post-execution meetings/walkthroughs.
Final Report	A summary report formally documenting the findings of the testing. This will be the test-exit report highlighting whether exit criteria have been met and will be signed by relevant parties representing the business. Performance test exit report with Business owner's acceptance/approval.

6.1 Testing Schedule

Test Tasks	Target Start Date	Target End Date	w1	w2	W3	W4	W5	W6	W7	W8	W9
Performance Test Plan	23/04/2024	9/10/2024									
Scripting**	31/05/2024	30/07/2024									
Harvest and prepare any additional (If required) test input data (face and biographic data) from AMS for the extended tests.	30/09/2024	26/10/2024									
Identify UI manual testers and assign roles in UAT – Appendix E.	30/10/2024	18/10/2024									
Dry run for manual testers in Appendix E. Recorded results may serve as a primary baseline and a set of results for case of the system being under negligible load.	7/10/2024	26/10/2024									
** dry run (demo) of transaction injection scripts and rate and interval control and resource consumption level capture and record and presentation of results.	30/07/2024	26/10/2024									
Performance Test execution (with draft results report -lite – high level through put results and main bottlenecks (if any) identified. Tuning opportunities – low hanging fruit and main defects identified).	27/10/2024	8/11/2024									
Tuning period and performance defect repair	9/10/2024	15/11/2024									
Final acceptance Perf Test Execution	16/Nov/2024	22/Nov/2024									
Performance Test Report(draft)	18/Nov/2024	30/Nov/2024									
Performance Test Report (Final)	1/Dec/2024	10/Dec/2024									

7. Defect Tracking and Reporting

7.1 Defect Handling

As per current defect management processes in the project, the following applies.

ADO will be used to manage defects raised during performance test execution and assigned to the UAT test Environment.

Defects will be logged in ADO with performance tag and will be assigned to the respective team at the triage meeting. The same process will be followed as for defects processed during the SIT functional test phase.

8.2 Assumptions

The following table summarises the assumptions associated with performance testing:

ID	Assumptions
A01	Stable build will be deployed to UAT in time for full execution all necessary testing and analysis before go-live.
A02	The Performance testing environment will be available at 3pm daily and over weekends for testing.
A03	Vendor support will be available to resolve issues identified during performance testing, and vendors can provide relevant performance metrics.
A04	All Integrated environments will remain active and stable during the Performance testing window, including weekends.
A05	s 6(c)
A06	Test scripts developed in SIT will be valid for execution against the UAT environment.
A07	Performance metrics (such as counts, timings, outcomes) will be provided by the respective vendors if not available from the MBIE views or UI.
A08	Resource demand and response time for generating matching scores in MBIS will be independent of the channel through which the service is accessed (e.g. matching times for identities from ADEPT will be the same as those from NZeTA)
A09	Test data that differs from production data will not skew test results, whether optimistically or pessimistically.
A10	Test environments will closely replicate production in terms of configuration, data volumes and system integrations.
A11	Network performance (latency, bandwidth) in the test environment will be representative of the live production environment.
A12	Test Scripts and test data will reflect real-world scenarios, including edge cases, to ensure comprehensive performance validation.

8.3 Dependencies

ID	This task required	Before this task can commence
D01	SIT must be completed to a stable build, which may not be fully functional but must allow for 'happy path'	Performance scripting can begin.

	end-to-end tasks/transactions to be processed without errors.	
D02	A stable build must be deployed to UAT	Performance testing can commence
D03	Required monitoring and performance tools must be deployed and configured before performance testing begins.	Performance testing can commence
D04	Test data setup must be completed before performance testing starts, including any necessary accounts, transactions, and sample files.	Performance testing can commence

8.4 Constraints

ID	Description
C01	Performance testing may need to be conducted outside of regular business hours, requiring evening and weekend work, or the team to be on-call.
C02	Running performance tests with s 6(c) current users for Reveal and s 6(c) IBW users is not feasible.
C03	Limited availability of specific resources (e.g. databases or services) during testing hour may impact test outcomes.
C04	Any major configuration changes in the UAT environment during performance testing may affect the consistency of results.

8.5 Test Resources

Resource Name (If known)	Organisation	Role	Responsibilities
BCU Project Team	MBIE	BCU Project Team: MBIE	Generate manual load from integrated systems like ADEPT, IGMS, s 6(c), Reveal and IBW. Analyse performance outputs from test execution and advise on any degradations experienced.
s 9(2)(a)	DXC	Performance Capability: AMS	- Execute AMS performance scripts as and when required. - Provide metrics
			s 6(c) of the OIA

Resource Name (If known)	Organisation	Role	Responsibilities
Engineer	NEC	Performance Capability: IDMe systems	Analyse overall health of the IDMe solution during the peak load.
s 9(2)(a)	MBIE	Product / Business / System owner	Go/No go decision, accept/remediate performance issues if found
	MBIE	Go/no go input/doc review	Preview/review the Test Report draft
	MBIE, Datacom, NEC, DXC, Argonaut, Intech, One NZ, and Theta	Technical Consultants	- Triage of issues - Resolution identification - Implementation of optimisations/remediations
	MBIE	Solution Architect	- Triage of issues and resolution identification - Capacity and monitoring planning
	NEC, Datacom	Release Manager / Environment Manager	- Monitoring environment - Verify environment before execution.
No Appointment ¹⁰ (Test Manager will fill this function)	???	Defect Manager	Defect Recording and resolution tracking.

9. Entry & Exit Criteria

9.1 Performance Test Entry Criteria

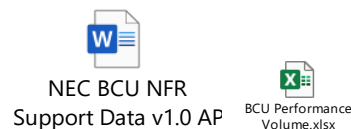
Entry Criteria
1. UAT test environment is available and stable for the full duration of the testing window.
2. There are no open Severity 1 or 2 defect from SIT that impact the performance test scripts.
3. Any unresolved defects have an agreed resolution plan in place, with assessment from the business owner and project solution architect regarding their potential impact on test results. After establishing the performance baseline, a limited re-test may be conducted to assess the effects or defect fixes.
4. Outstanding defects have been reviewed to determine their impact on system performance post-fix, and a decision has been made whether re-running test is necessary after certain defect fixes or updates.
5. All required Performance Test suites are stable, validated, and ready for execution.
6. Test data creation and maintenance processes are managed to avoid impacting test accuracy or availability.

¹⁰ The test manager may act in this function (time permitting)

7. The test environment is fully configured as expected, including proper setup of queue configurations, retry attempts, retry rates, and throttling levels, which impact network traffic and resource utilisation.
8. All necessary monitoring tools are in place, accessible, and fully operational.
9. Approval for any out-of-hours testing (if required) has been granted.
10. All necessary monitoring tools are in place, accessible, and fully operational.
11. All licencing and environmental scaling activities have been completed in UAT.
12. Network configurations (e.g. firewall rules, VPN access) are validated to ensure performance test can be run without connectivity issues.
13. Documentation of all configurations, test scripts, and baseline expectations is available and accessible for the testing team.

9.2 Performance Non-Functional Requirements

The two embedded documents below have been the basis for the base set of test parameters (aka volume/time).



Revised data volume profiles have been sent to the project

6(c) of the OIA . However, these have yet to be formally accepted, nor has the NFR support data document embedded in this section been revised to reflect the more recent findings.

The “BCU Performance Volume.xlsx” file in this section has been added to the BCU test planning folder with recognition that provenance of the data is not clear.

The mako link is: 6(c) of the OIA .

The “NEC BCU NFR Support Data v1.0 APPROVED.docx” file embedded in this section is/was in mako at the below link:

6(c) of the OIA

9.3 SIT and NFR Test Exit Report

TBD – Work in progress as the Functional Testing is not completed at time of writing this test plan

9.4 Performance Test Exit Criteria

- All **planned performance tests** have been executed, and the system’s measured throughput meets the agreed commercial requirements and revised load projections. The solution has been verified to handle higher throughput under scalability conditions.

- There are **no open Severity 1 or 2 defects**, including non-functional requirement (NFR) defects, with the exception of those classified as Severity 2/Priority 4 or lower.
- Any **unresolved defects** have been reviewed by the project team and business stakeholders, with an agreed action plan in place to either accept the defects or implement remediation.
- **System stability** has been demonstrated under peak load, stress, and soak test conditions, with no significant degradation in performance over the testing duration.
- **Performance metrics** (e.g. response times, transaction throughput, resource utilisation) meet or exceed the baseline performance targets and non-functional requirements (NFRs).
- **Monitoring and logging** tools have captured sufficient data to assess system behavior under load, and this data has been reviewed and validated.
- **System resource usage** (CPU, memory, disk I/O, etc) remains within acceptable thresholds during testing, with no unexpected resource exhaustion or bottlenecks.
- **Business continuity** and disaster recovery scenarios have been validated, demonstrating that the system can recover from failure events without significant performance degradation.
- **All agreed-upon performance tests** have been reviewed and approved by relevant stakeholders (project team, business owners, vendors, etc.)

10. Appendix A.- Data Classes and Types

There three main areas involved in the identity management system under test. An identity record can have any combination of face, fingerprint and biographic(written) data that can be used by MBIS to get matching scores that support the matching decisions. Full description of this matching process is found in the business requirement documents. For the purposes of this test plan the below table will help to describe test configurations.

Test Input data types and classes

s 6(c)



Legend/Key:

“T” = Templatable

¹¹ Type A records will need to be extracted from AMS+MBIS

11. Appendix B.- Process Table Template

The below table is the start of a map to assist a big picture view (or solution on one page) of the key steps in the workflow in the BCU components and participating services. Only concerned with the identity matching flow (not the visa/other application flow)

Origin	s 6(c)									
NZeTA										
IGME										
ADEPT										
AMS										

From S
6(c)



3. s 6(c)

[Redacted text block containing multiple lines of information, likely a list or table of contents, with varying levels of indentation.]

12. Appendix C.- Inter-component throttling values.

Source	Target	Throttle
PQC	Filescanner	s 6(c)
ADEPT	AMS	???
NZeTA	AMS	???

13. Appendix D.- Resource monitoring parameters and intervals by Node.

Interval for sampling and recording resource values.

Test Type	Interval for sample and record	
Load Test	Every 10 seconds	
Stress Test	Every 20 seconds	
Soak Test	Every 30 seconds	

Resource levels to be captured by Node.

Node\Parameter	CPU(% Utilisation)		Memory Usage % of allocated	Disk Write (kB/sec)	Disk Read(kB/sec)	Network In(kb/sec)	Network Out(kb/sec)
Node 1							
Node 2							
Node n.							

14. Appendix E.- List of testers for manual UI transactions while BCU system is under load.

Name	UI	Role	Email	phone
s 9(2)(a)	IBW			
	Smartscan(IPE)	Border		
BAT Tester #1	Reveal			
BAT Tester #1	IBW			

15. Appendix F.- Template for recording manual UI transactions (during performance testing) recording.

Table of Contents

Table of Contents	2
1. Performance Testing Objectives	7
2. Project Overview	7
2.1 Biometric Capability Update (BCU)	7
3. Performance Testing Scope.....	8
3.1 Scope	8
3.2 Out of Scope.....	9
3.2.1 Scenarios Out of Scope.....	9
4. Performance Test Approach	9
4.1 Performance Test Principles.....	10
4.2 Performance Test Suites	11
4.3 Test Strategy.....	12
4.3.1 Performance Test Types.....	12
4.4 Test Throughput Details.....	14
4.4.1 ADEPT Load Profile Breakdown.....	14
4.4.2 AMS Load Profile Breakdown.....	14
4.4.3 NZeTA Load Profile Breakdown.....	15
4.4.4 IGMS Load Profile Breakdown.....	15
4.4.5 IPE Load Profile Breakdown	15
4.4.6 6(c) of the OIA	15
4.4.7 IDMe Load Profile Breakdown	16
4.5 Performance Metrics.....	16
4.7 Issue Analysis.....	16
5. Environments	17
5.1 Test Environments and Usage.....	17
6. Deliverables.....	18
6.1 Testing Schedule	19
7. Defect Tracking and Reporting.....	20
7.1 Defect Handling.....	20
8. Risks Assumptions Dependencies Constraints.....	21
8.1 Risks/Events	21
8.2 Assumptions.....	24
8.3 Dependencies.....	24
8.4 Constraints	25
8.5 Test Resources.....	25
9. Entry & Exit Criteria	26

9.1 Performance Test Entry Criteria.....	26
9.2 Performance Non-Functional Requirements	27
9.3 SIT and NFR Test Exit Report	27
9.4 Performance Test Exit Criteria	27
10. Appendix A.- Data Classes and Types.....	29
11. Appendix B.- Process Table Template	30
12. Appendix C.- Inter-component throttling values.	32
13. Appendix D.- Resource monitoring parameters and intervals by Node.	33
14. Appendix E.- List of testers for manual UI transactions while BCU system is under load. 34	
15. Appendix F.- Template for recording manual UI transactions (during performance testing) recording.	35
16. Appendix G.- List of NFRs the inform and are informed by this test	35



**MINISTRY OF BUSINESS,
INNOVATION & EMPLOYMENT**
HĪKINA WHAKATUTUKI



BCU Regression Test Exit Report

Test Exit Report

Date: 17/10/2025

Document Signoff

The following signatures indicate approval and acceptance of this document, subject to any caveats

Person Name	Role	Signature	Caveats
Name	Title	Signed	
s 9(2)(a)		Signed: _____ Date: ____ \ ____ \	
		Signed: _____ Date: ____ \ ____ \	
		Signed: _____ Date: ____ \ ____ \	

Note: Electronic signature content to be emailed to all approvers

This email is confirmation of my approval as **[MBIE Project Manager]** to proceed to production.

I have reviewed the **[Project Name]** Test Exit Report that you provided on **[Date]**.

Please keep this email approval for audit purposes and embed into the approval section of the document.

Scope of this Report

The purpose of this test exit report is to document the testing executed and outcomes in preparation for the BCU Project to go-live. The purpose of this report is to provide a summary of the regression testing phase of the project.

Executive Summary

The BCU Project regression testing phase was conducted between April and October 2025. The regression phase was divided into 3 iterations due to ongoing functional changes and bug fixes.

Regression testing was conducted to verify that recent bug fixes and system updates did not adversely impact existing functionality. The regression phase confirmed that the BCU system continues to perform following these changes.

Test Results

<< This section and associated sub-sections are **MANDATORY** unless otherwise stated. >>

<<The **tables** below detail the test cases prepared and executed and include the results of the test execution activities. Based on the planned test scope, [##] test cases were prepared and [##] were executed to plan

If you are reporting using a dashboard you will need to identify the visual representation of your testing performance along with any requirements left untested>>

Test Result Summary

Regression testing was divided into three iterations of test cycles due to the ongoing delivery of bug fixes.

Iteration 1 test execution ran from 28/04/2025 to 17/07/2025.

Iteration 2 test execution ran from 18/07/2025 to 08/08/2025

Iteration 3 test execution ran from xx to xx

Test Phase (if relevant)	Prepared Test Cases	Executed (includes obsolete)	PASSED (includes obsolete)	FAILED	Not Completed	Passed with Exception	De-scoped
Iteration 1	287	258	255	3			27
Iteration 2	122	120	111	8	1		2
Iteration 3	TBC						
TOTAL							

Open/Incomplete Test Cases

<<If this section is empty and all test cases have run then leave section with N/A >>

The tests were:

- Xxxxxxx
- Xxxxxxx

Project Defect Statistics

The following table details defects identified over the duration of the “in scope” testing.

Defect Status	1– Critical	2 – Major	3 – Medium	4 – Minor/Trivial	TOTAL
OPEN					
CLOSED					
TOTAL					

Please find the below attached mako link to detailed list of the defects raised in JIRA as at [dd/mm/20yy hh:mm am/pm.]

[\[Link to defect stored as an extracted document goes in here\]](#)

Outstanding Defects

<<Add information about resolving outstanding issues post Go-Live. Or N/A if no outstanding defects>>

Test Progress Reporting

The evaluation of the BCU Project regression test outcomes detailed in this document is as follows:

Project Critical Success Factors	Acceptance Yes/No	Notes
Successful delivery and integration of BCU components to its specifications and agreed changes, within the agreed project constraints (scope, time, and quality).	Yes	
BCU components are commercially ready for use.	Yes	
The system is stable including connectivity and interfaces.	Yes	
The systems meet the documented business requirements.	Yes	
MBIE Exit Criteria	Acceptance Yes/No	Notes
All planned test cases have been executed and results documented.	Yes	All planned scripts and steps that remain in scope have been tested.
No outstanding priority 1 or priority 2 severity defects.	Yes	No outstanding priority 1 or priority 2 assessed as being required for go-live.
Acceptable levels of priority 3 and priority 4 severity defects are reviewed and agreed by MBIE prior to decision to go live.	Yes	Outstanding defects have been categorised as being required after go-live.
All defect/issues workarounds are agreed and documented.	Yes	Business processes have been established where required.
Test Exit Report issued.	Yes	



**MINISTRY OF BUSINESS,
INNOVATION & EMPLOYMENT**
HĪKINA WHAKATUTUKI



BCU Regression Test Plan

Version 1.1
Date: 21/05/2025

Document control

Version history

Date	Version	Author	Description of change
13/03/2025	Draft	s 9(2)(a)	First draft
25/03/2025	Draft		Including updates from Test Team and BA's
26/03/2025	Final		For approval
26/03/2025	Final		For approval

Reviewed by

The following people have a formal quality assurance role with respect to this document

Name	Role	Date
BCU Test Team	Senior Test Analysts	
s 9(2)(a)		

Test Plan Signoff

The signatories below have reviewed this document and agree it is a fit-for-purpose statement of the testing objectives, processes, and strategies to be used for BCU Project.

The signatories below agree to abide by the provisions, duties and the responsibilities set out in this document.

Name	Title	Signed
s 9(2)(a)		Signed: _____ Date: ____ \ ____ \ ____
		Signed: _____ Date: ____ \ ____ \ ____
		Signed: _____ Date: ____ \ ____ \ ____

Introduction

This Test Plan relates to the Biometrics Capability Upgrade (BCU) project that was established to replace the current identity management system (IDME).

This document covers the Regression Test phase of the project.

Test Approach

The regression test phase of the project will commence once System Integration Testing (SIT) has completed. The purpose of this phase is to verify that any changes implemented during the SIT phase have not introduced new bugs or broken existing functionality.

Undertaken	At each Iteration by MBIE Test Team
Objective	MBIE's project test team to verify the BCU MVP is fully functional, fit for purpose, and no regression areas are identified
Test Design technique	Test cases are designed from Functional Specs and Business Requirements to provide coverage of business requirements and rules.
Test Environment	User Acceptance Test (UAT)
Manual Test Execution Approach	- Identify the Test Scenario coverage for BCU Project and prepare required test cases using Azure DevOps Test Plan functionality to provide full traceability - The final build from System Integration Testing is expected to be deployed into the UAT environment, where a smoke test will be completed to validate the environment and deployment. - Two iterations of regression testing will be performed, in 2-week cycles with a bug fix release to be deployed after iteration 1. A second bug fix release will occur if required after iteration 2. - A 'soft start' regression week is tentatively planned. This will occur before iteration 1 and only if high severity bugs not yet resolved exist, and areas where regression testing could start, independent of the bug related areas of the system. - Each test case is executed manually, predominately with valid data, though some invalid data scenarios will be run and results details in Azure DevOps. - It should be noted that any uncompleted test scripts in an iteration will be reviewed and rescheduled for completion in conjunction with later iterations. This could impact on the testing effort required for those iterations.

Testing Resources

Resource Name	Organisation	Responsibilities
s 9(2)(a)	MBIE	Test Manager
	MBIE	Regression Testing
	MBIE	Regression Testing
	Datacom	Regression Testing
	MBIE	Regression Testing
	MBIE	Regression Testing

Test Tools

MBIE Test Team will use the following tools, for test planning; management; reporting and execution.

Tool	Purpose	Used by
Azure DevOps (ADO)	Defect Repository and Management	MBIE Project Team

Test Scope

In scope

Test Activity	Responsibility	Overall status/Commentary
Regression Testing	MBIE Test Team	Regression testing will cover the following areas and integrated components of the IDMe system. Detailed test cases can be found in ADO. - Combined Regression – with ADEPT Team and INZ BAU Team - Reveal - Ad hoc search (within Reveal) - API's / DB messages - AMS - Audit - Capping and Override (workflow related) - DMS (Document management system) - E2E flows - s 6(c) - IBW (integrated biographic workstation) - IPE / Smartscan enrolments - RBAC (role-based access) - High Risk target areas There are s 6 input channels to the system. These will be covered as part of E2E testing and Combined Regression testing with INZ BAU Team, however the focus will be on the high-volume input channels i.e. ADEPT, NZeTA, IGMS Online.

Out of scope

Test Activity	Responsibility	Overall status/Commentary
Regression Testing	MBIE Test Team	IPE – Testing will cover the submission of all Types of Transactions (ToTs) from Smartscan but not all will be processed E2E.

Test Entry and Exit Criteria

Entry Criteria

- System Integration Testing completed.
- Regression tests have been finalised.
- ‘Must-have’ bugs are closed. i.e. No open Severity 1, Severity 2 (excluding P4) defects unless reviewed and agreed by the project team
- Test Environment available with correct data loaded and required access provided.

Exit Criteria:

- Planned Regression Test execution completed.
- No Open Severity 1 and Severity 2 Defects unless reviewed and agreed by the project team
- Business consequence and impact discussed for the open Severity 3, Severity 4 Defects and appropriate workarounds exist.
- Test Exit report distributed.

Estimated Test Time frames

Activity	Start Date	End Date
<i>Soft Start Date</i>	28/04/2025	23/05/2025
Regression Test Iteration One	26/04/2025	06/06/2025
Bug fix release 1	TBC	
Regression Test Iteration Two – includes test of any regression bug fixes	09/06/2025	20/06/2025
Bug fix release 2	If required	

Test Environments

The UAT environment will be used for regression test execution.

Assumptions

None identified

Risks

R1 - Releases from NEC not delivered on time, meaning we have high severity / priority bugs still open. This will potentially impact the start date of regression testing.

R2 – s 6(c)

s 6(c)

R3 – SIT testing commenced more than two years ago. There is a risk that the scope of Regression Testing may not uncover all regressed areas of the system, given the size and complexity of the solution. This is a known risk at Senior Leadership level.



**Ministry of Business,
Innovation & Employment**

Biometric Capability Update Project

SIT Test Summary Report

Document Version 0.4

In Confidence

Document History

Version	Issue Date	Author	Changes
0.1	02/07/2024	s 9(2)(a)	Initial draft
0.2	19/08/2024		Updated draft
0.3	17/10/2025		Updated draft
0.4	17/11/2025		Updated draft

Document References

Document	Version	Link
BCU Test Plan	2.03	6(c) of the OIA

Distribution List

Name	Role	Responsibility
s 9(2)(a)		Reviewer

Document Sign-off

The following signatures indicate approval and acceptance of this document, subject to any caveats:

Role	Name	Endorsement Email / E- Signature	Caveats
s 9(2)(a)			

TABLE OF CONTENTS

Contents

1	INTRODUCTION	5
1.1	BACKGROUND.....	5
2	TEST SUMMARY	6
2.1	SYSTEM INTEGRATION TESTING.....	6
2.2	DETAILED TESTING DOCUMENTATION.....	6
3	TEST RESULTS	7
3.1	CURRENT TEST RESULTS.....	7
3.2	CURRENT TEST CASE STATUS.....	8
4	DEFECT SUMMARY	9
4.1	OUTSTANDING DEFECTS	9
5	EVALUATION	10
6	APPENDIX	11

1 INTRODUCTION

1.1 Background

The Biometric Capability Update (BCU) Project commenced in 2019. The project was established to replace the current identity management solution (IDME) which provides Immigration New Zealand (INZ) with the capability to be the authoritative source of identity information for all non-New Zealanders.

The Biometric Capability Update has been designed to address INZ project's needs and future known capability by upgrading the versions of biometric matching and management platforms, rationalising and simplifying the platform to reduce on-going cost and improve the flexibility and utility of the system in the process. This is a core capability for INZ's future protection in an environment where identity fraud, terrorism and other sources of harm are prevalent and increasingly diverse and sophisticated, and this upgraded capability is crucial to achieving that future.

The BCU project is a multi vendor project, including NEC, Datacom, Theta, Argonaut, DXC, and Intech.

This document is a summary of System Integration Testing (SIT) undertaken to date. SIT commenced in October 2023 and was concluded as per the details of this document on July 2025 - TBC

2 TEST SUMMARY

2.1 System Integration Testing

The SIT phase of the BCU project has been lengthy, with a significant number of complex test cases to execute. This SIT summary presents the facts, where SIT execution is at a point in time – at July 2025.

Testing in SIT was done until version 1.0.39. In July 2025 decision was made to use SIT for fast followers. So no active testing / releases (except fast followers) were done in SIT since July 2025. We started using UAT for active testing / releases. Tim do we have any emails/ screenshots relating to SIT agreement that I can attach to this document ?

After 1.0.39 we had 15 release done and we are upto version 1.0.39.15 in UAT.

Also note that production candidate will be from UAT and not SIT.

There is a significant backlog of defects still to be resolved. The vast majority of these defects are being worked on by NEC and MBIE is awaiting deployment of fixes for these.

Ideally, anyone referring to this test summary will have access to the [ADO test progress report](#) to obtain updated test execution and defect reports as defect retesting continues in the SIT environment.

2.2 Detailed Testing Documentation

Azure DevOps (ADO) is the selected tool for test case management and defect management. The ADO BCU project is available [here](#).

3 TEST RESULTS

The following provides an overview of SIT execution results **as at Nov 2025**.

Test cases and corresponding test results are held and managed in ADO here:

[SIT test plan](#)

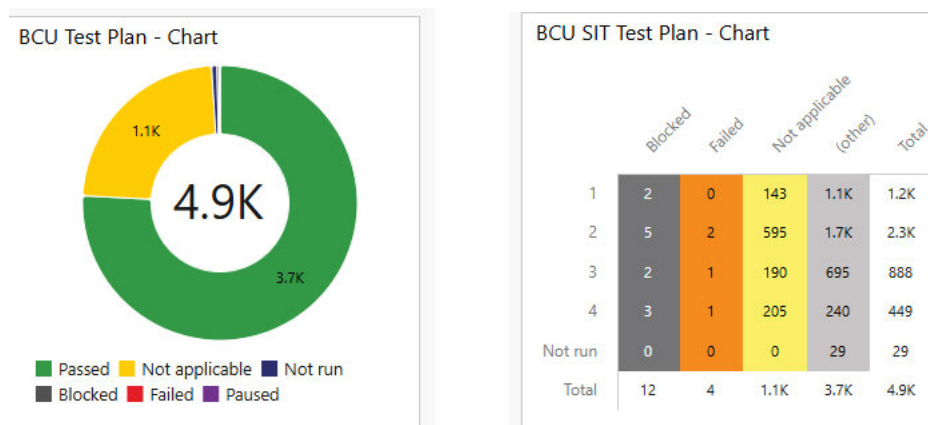
The below table represents the test cases prepared and executed, and includes the results of the test execution activities. Based on the planned test scope, test cases were prepared and executed to plan, with the exception of those test cases that were, on review, considered not applicable.

3.1 Current Test Results

The following table summarises the current SIT test results:

Will pull precise numbers from ADO for final version of document

10 Nov 2025



A significant number of test cases were considered not applicable for the following reasons:

- They were duplicates.
- They were written sometime ago when it was not clear how the system will function. On reflection it was determined that they were not needed.
- Some test cases were better suited to be executed in the User Acceptance Testing (UAT) environment.

3.2 Current Test Case Status

Below is the test case status based on priority:

BCU Test Plan - Chart					
	2	1	3	(other)	Total
Passed	1.7K	1.1K	695	240	3.7K
Not applicable	595	143	190	205	1.1K
Not run	1	1	0	29	31
Blocked	5	2	2	3	12
Failed	2	0	1	1	4
Paused	1	0	0	0	1
Total	2.3K	1.2K	888	478	4.9K

4 DEFECT SUMMARY

Defects were logged, tracked and managed via ADO.

A full list of all defects logged for the SIT environment is available in ADO:

Table as of 10th Nov 2025 (These are the defects that are filtered with a create date < currentday(-100). Security defects are excluded. This list includes defects across all priorities)

	Active	Blocked	Closed	Deferred	Proposed	Ready for Test	Resolved	Triage	Grand Total
1 - Critical	0	0	55	1	0	0	0	0	56
2 - High	24	0	573	3	1	6	6	0	613
3 - Medium	58	1	372	9	5	5	20	0	469
4 - Low	18	0	129	14	5	4	12	0	182
Grand Total	100	1	1129	27	11	15	38	0	1320

Note: Testing was stopped in SIT in July 2025. Since then SIT has been used to hold fast followers releases from NEC.

4.1 Outstanding Defects

Details of outstanding defects (S1/S2 and P1/P2/P3) is available in the Appendix. The list is correct as of Nov 2025.

5 EVALUATION

This section does not apply because this is not an exit report but a status report. Hence no evaluation will be done

Section to be removed - TBC

The evaluation of the Biometric Capability Update SIT outcomes detailed in this document indicates that defined Test Exit Criteria as documented and agreed in the Biometric Capability Update Test Plan are defined as follows:

SIT exit Criteria	Acceptance Yes/No	Notes
All test cases executed (except cases that have been removed from scope after review) (with a 95% pass rate).	No	P2, P3, and P4 test cases remain unexecuted.
No Open Severity 1 or 2 defects	No	
All defects have had the severity and priority levels reviewed and agreed by MBIE	Yes	Ongoing as part of triage, as new defects are raised
All open defects have been reviewed by MBIE and aggregated severity 3 & 4 defects accepted with an agreed remediation plan	In progress	Ongoing as defects are raised
All open defects have been reviewed by business/stakeholder representatives	In progress	Ongoing process, as new defects are raised
SIT Test Exit Report completed	In progress	This document
Migration Test Exit report completed	?	?

6 APPENDIX

Defects with Severity 1/2 and Priority 1/2/3 as of 10 Nov 2025

Defect	State	Severity	Priority	Notes
96680	Deferred	1 – Critical	1	
108165	Resolved	2 - High	3	Deferred as change request process will be tested with override rules see related bugs
109930	Resolved	2 - High	2	This is to put together Cutover defect summary
113416	Active	2 – High	3	This is linked to CR-160
117513	Resolved	2 – High	1	
118150	Deferred	2 – High	3	MBIE need to document the change release process to follow for requesting changes through service desk to NEC. This will be the same as for the override rules and business context prioritisation rules.
118151	Deferred	2 – High	3	MBIE need to document the change release process to follow for requesting changes through service desk to NEC. This will be the same as for the override rules and business context prioritisation rules.
133404	Deferred	2 – High	3	This needs adding to the list of reports you are creating.

[In Confidence]
Biometric Capability Update SIT Test Summary

143507	Active	2 – High	1	These ae currently being discussed under the data structures questions spreadsheet. Will leave this defect open in case they get pushed back to this defect.
144467	Active	2 – High	3	ADEPT to add this to their backlog
149107	Ready for Test	2 – High	3	Waiting for update from NEC
152879	Ready for Test	2 – High	2	Waiting retest
158691	Ready for Test	2 – High	2	Waiting retest