Inland Revenue
Te Tari Taake

Business Transformation

Inland Revenue

Gateway Services onboarding: Accounting Income Method

Version: v0.8
Date: 11/09/2017

IN CONFIDENCE

About this document

This document is the onboarding guide for service providers to guide them step-by-step through the process of consuming Inland Revenue's (IR) new Gateway Services. It focuses on core business such as prerequisites, testing activities, organisation contact lists etc.

There is also a Return service build pack document that lists the technical requirements and specifications, solution design and other bi-directional information sources between IR and external clients.

A link to an AIM Overview document will be added.

Document control

File Name and Path	TBC
Contact Person	SoftwareDevelopersLiaisonUnit@ird.govt.nz
Status	DRAFT ~~| REVIEW | FINAL~~

Contents

1 Overview 4
2 Path to production 5
2.1 Registration prerequisites 5
2.2 Supporting your software development lifecycle 5
2.3 Testing phase and environment information 5
2.3.1 Data allocation 6
2.3.2 Test scenarios 7
3 Business use cases 8
3.1 Confirm user's eligibility to use AIM service 9
3.2 Submit a new Statement of Activity 11
3.3 Retrieve the status of previously submitted Statement of Activity and next filing obligation 14
3.4 Retrieve previously-submitted Statement of Activity 16
3.5 Amend and submit a Statement of Activity 18
4 Testing 21
4.1 Prerequisites 21
4.2 Data management 21
4.3 Test execution 22
4.4 Test exit report 23
5 Production support 23
5.1 Service hours 23
5.2 Service provider support 23
6 Appendix A—Build pack references 24
6.1 Return service build pack 24
6.2 Identity and Access services build pack 24
7 Appendix B—Glossary 25

1 Overview

Inland Revenue has a range of digital services that facilitate secure and efficient business interactions between itself and its customers. Inland Revenue's Gateway Services provide a suite of services, including the returns service for the Accounting Income Method (AIM), that allow customers to file returns electronically through this gateway.

This document should be read in conjunction with the relevant legislative overview (to be supplied) and technical build packs (see appendix A).

The diagram below shows how the Onboarding and Build packs link together.

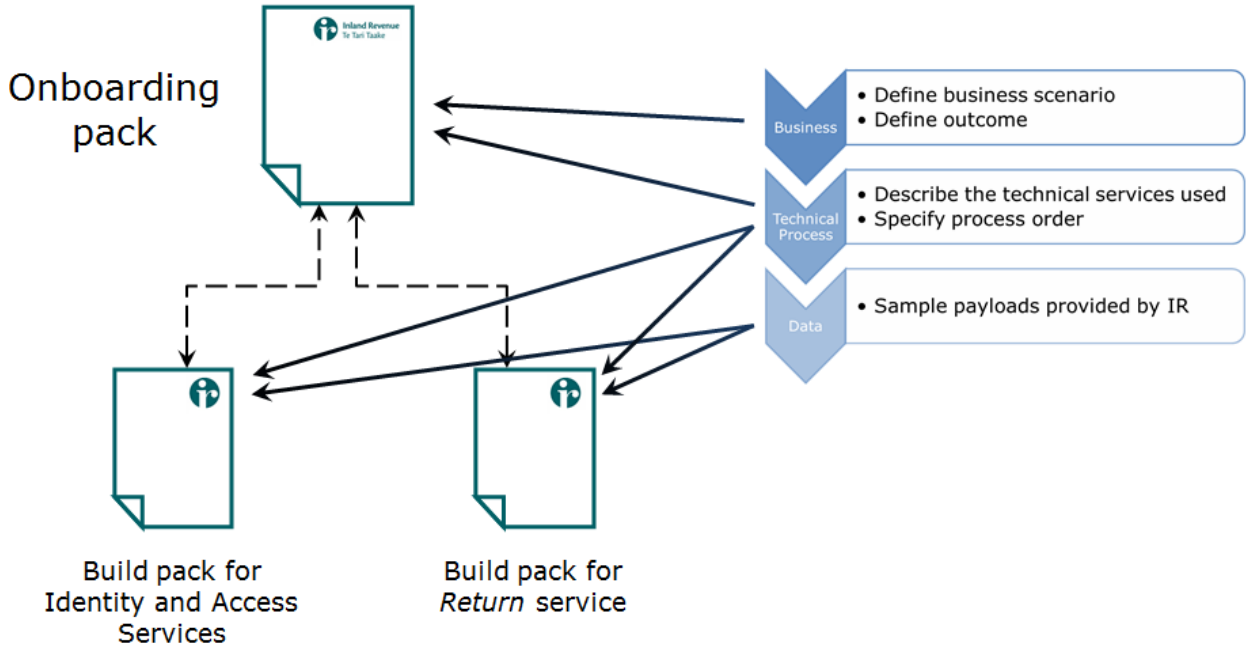


Figure 1: Onboarding and build pack structure

2 Path to production

2.1 Registration prerequisites

Details on the supporting legislation for AIM are summarised here http://taxpolicy.ird.govt.nz/publications/2016-commentary-bteirm/accounting-income-method. It is important to note that <<summarise key parts of the *AIM providers approval and revocation* section>>.]

Service Partner registration requests should include information about the entity requesting access, the system(s) that will integrate with Inland Revenue (examples include software products to market and in-house software) and the intended use of Gateway Services and the data exchanged (customer reach, customer segmentation, expected volumes, etc).

Before committing effort to building AIM-capable software, a Service Provider must be aware that prior to entering production a signed, statuary declaration confirming software confirms to legislation is required. Inland Revenue has a legislative duty of care for treating all tax payer and business information as confidential. Inland Revenue will complete due diligence which your Relationship Manager will discuss with at the time of registration.

2.2 Supporting your software development lifecycle

Your Inland Revenue Relationship Manager will support the entire software development lifecycle including the journey from initial registration, testing, deployment to production and managing the on-going relationship in a BAU environment. Your Relationship Manager will ensure access to the latest documentation and Inland Revenue non-production environments.

The design and build phase of your software development lifecycle is supported by Inland Revenue on-boarding documentation and associated build packs listed in the appendix. This document links the business overview with the technical information contained in the associated build packs. Build packs describe the technical interactions for services, lists of response codes and provide links to schemas, WSDLs and the like. Emulated services may be available to support early development effort while the testing phase, test planning and Inland Revenue test environments are described in section 2.3. Your Relationship Manager will work with you on go-live and production support. Re-certification should be included as an ongoing cost to consume Gateway Services. Your Relationship Manager will work with you to define a suitable frequency with a minimum expectation of annual re-certification or when your product has a major release.]

Inland Revenue will release minor and major upgrades to the Gateway Services from time to time. Your Relationship Manager will manage your transition and any associated certification requirements, if any.

Discussions regarding volume changes, your product roadmap(s) and innovative uses for Gateway Services should be directed to your Inland Revenue Relationship Manager in the first instance.

2.3 Testing phase and environment information

Testing with Inland Revenue will be carried out in an integrated test environment, mirroring Production. The objective of the partnership test is to allow Inland Revenue and service providers to ensure their readiness for Production.

Test duration timelines will be managed via a partnership test plan. The purpose of the partnership test plan is to provide the scope of testing, scheduled test dates, test data, test activities and responsibilities. Inland Revenue will work with you to ensure a successful conclusion to testing this service through the Test Plan. This document intentionally provides an overview of testing at a higher level.

2.3.1 Data allocation

Inland Revenue will set up and provide test data for service providers for the scenarios that are documented in section 2.3.2 (below). The test data will be refreshed in a controlled fashion during partnership testing by Inland Revenue as requested by service providers.

2.3.2 Test scenarios

The figure below lists the scenarios that have been identified for testing. The scope of these test scenarios will be managed via the partnership test plan.

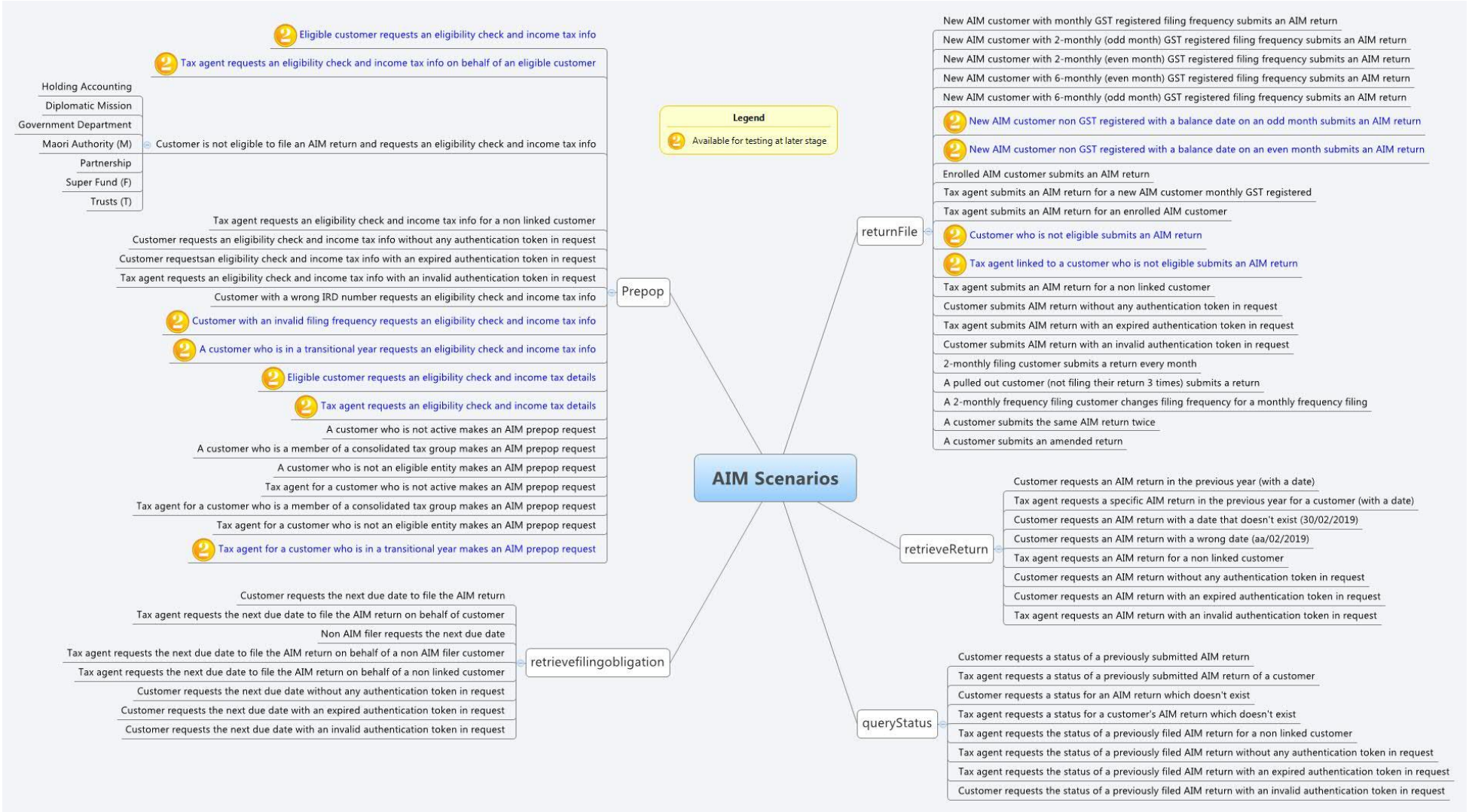


Figure 2: Test scenarios mind map

3 Business use cases

Please note the following:

1 The following use cases show sequences of Gateway Services operations that could be used to achieve a specific business outcome. They do not comprise a comprehensive list of all required business outcomes, nor are they prescriptive or intended to inhibit software innovation in any way.

2 The linking/delinking between a tax agent with their client/s is excluded from the scope of Gateway Services. This action must be done using the existing online services channel, which may take up to 48 hours.

3 The terms 'Statement' and 'Statement of Activity' are used interchangeably and represent the same intent.

4 Inland Revenue's Gateway Services will enforce the following AIM eligibility rules:

SN	Criteria	Business rule
1	User is not one of a class of customers excluded from using AIM	• User entity type **is** Company, Individual, Society/club or Unit trust. • User is not a 'look through' company
2	User is 'active'	• User is recorded as 'Active'
3	User is not a member of an income tax consolidated group.	• User's group filing indicator in FIRST is **not** 'Representative' or 'Member'
4	The tax year for which the customer wants to use AIM is not a transitional year	• User's balance date recorded in FIRST for the tax year with the provisional tax liability is the same as their balance date in the immediately preceding tax year

Table 1: Business rules for AIM eligibility

The table below summarises the business use cases and the sequence in which the Return service operations are used. The use cases are described in more detail in the following sections.

SNo	Business use cases	File	Prepop	RetrieveStatus	RetrieveReturn	RetrieveFilingObligation
1	Confirm user's eligibility to use AIM service		1			
2	Submit a new Statement of Activity (SOA)	2	1			
3	Retrieve the status of previously submitted Statement of Activity (SOA) and the next filing obligation			1		2
4	Retrieve previously submitted Statement of Activity				1	

Table 2: Summary of business use cases

3.1 Confirm user's eligibility to use AIM service

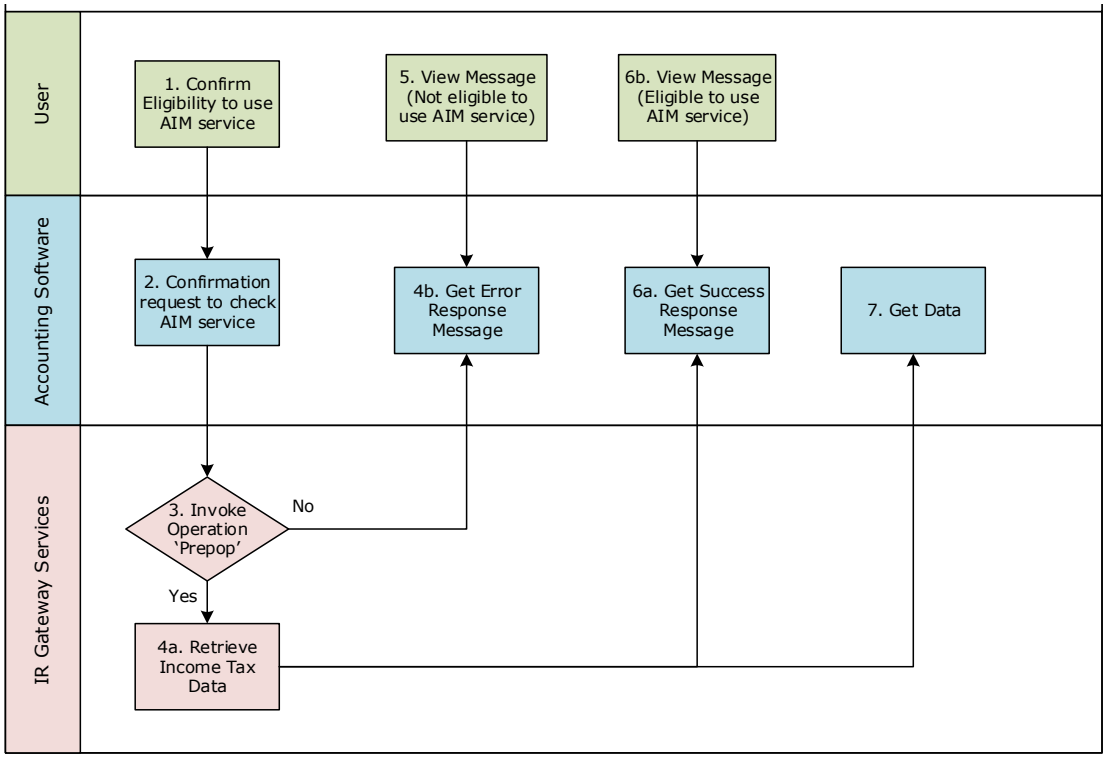
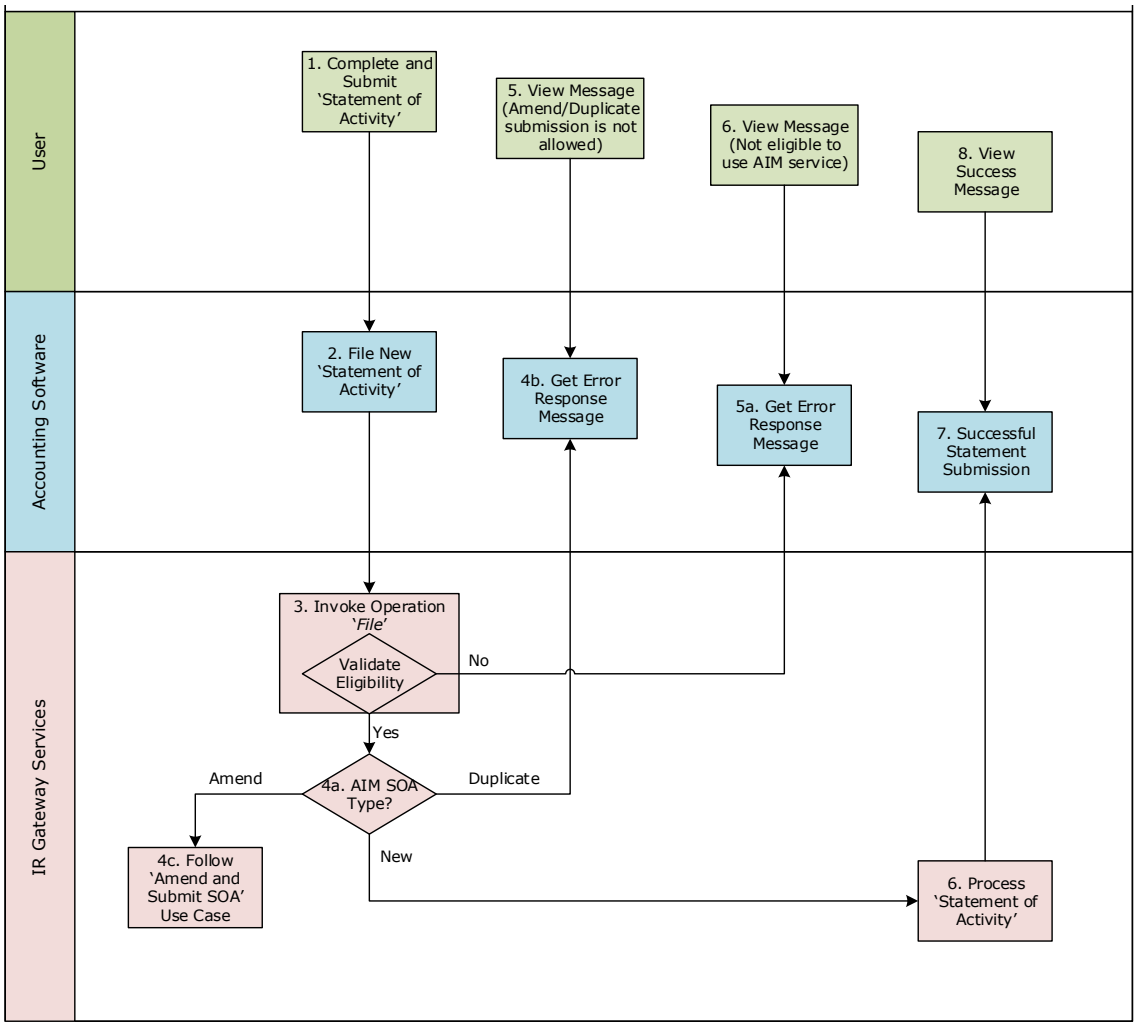


Figure 3: Confirm user's eligibility to use AIM service

Use case: Confirm user's eligibility to use AIM service	
Primary actor	• User
Secondary actors	• Accounting software • Gateway Services
Description	• The goal of the user is to confirm the eligibility to use AIM service
Pre-conditions	• User is logged-in to accounting software • User has used their IR online services credential to grant accounting software consent to access their information • In cases where user is a tax agent or an intermediary, they must have delegated access from the customer
Post-conditions	• User views request to check the eligibility to use AIM service and
Constraints	• The request must be sent using user's accounting software • At the time of any service request the accounting software must hold a valid access token for the user
Use case scenarios	
1. Normal flow	1.1 User submits a request in accounting software to confirm the eligibility of using AIM service 1.2 Return Service '*Prepop*' operation is invoked 1.3 Return service validates user's eligibility to use AIM service (please refer eligibility rules in Table 1). Once user is found eligible, Return service retrieves user's income tax data* and a successful response is returned to accounting software 1.4 User views the success message 1.5 Use case ends. *Note that income tax data includes: • IRD number • Filing frequency • Aim statement type • Balance date • Transitional year • Residual income tax • Losses carried forward.
2. Exception flow: User is not eligible to use AIM service	2.1 Return service validates user's eligibility to use AIM service (please refer eligibility rules in Table 1) and finds user not eligible to use AIM service 2.2 Return service returns an error message to accounting software 2.3 Accounting software displays the error message with an intent that user is not eligible to use AIM service. 2.4 User views the error message 2.5 Use case ends.

Use case: Confirm user's eligibility to use AIM service	
3. Exception: Authentication token is expired	3.1 Identity and Access service validates and finds authentication token expired due to inactivity (Please see section 5.1 'Response codes' in the Return service build pack) 3.2 Identity and Access services validate credentials and generates new token 3.3 Identity and Access services record new token generation request 3.4 Use case ends.
4. Exception: User is not authorised to use Service	4.1 The user is valid, however doesn't have the correct permissions to use this service 4.2 Identity and Access service responds to third party payroll software with appropriate error message (Please see section 5.1 'Response codes' in the Return service build pack) 4.3 Identity and Access services record access attempt 4.4 Use case ends.

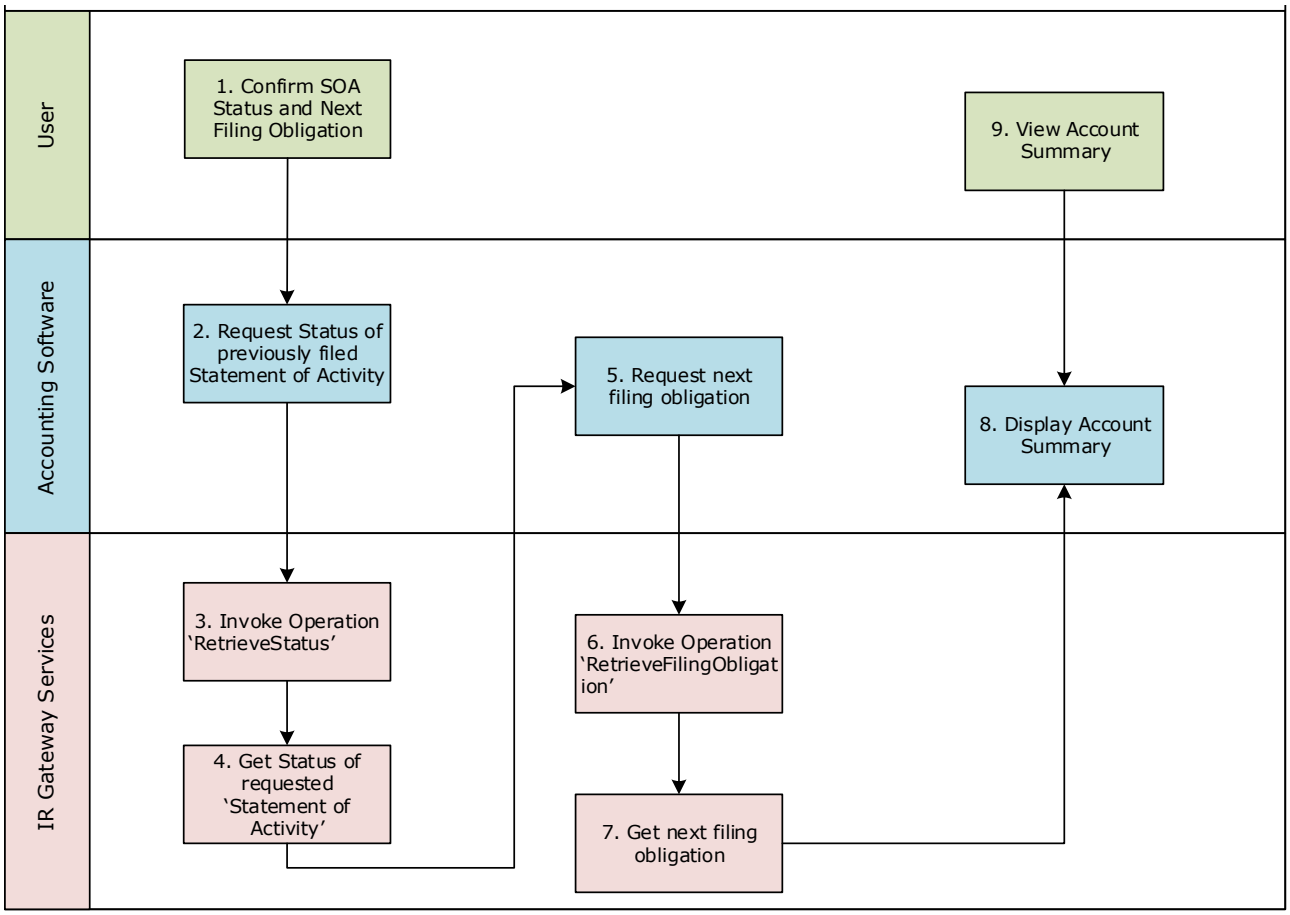
3.2 Submit a new Statement of Activity



Use case: Submit a new Statement of Activity	
Primary actor	• User
Secondary actors	• Accounting software • Gateway Services
Description	• The goal of the user is to successfully submit a new Statement of Activity (SOA)
Pre-conditions	• User is logged-in to accounting software • User has used their IR online services credential to grant accounting software consent to access their information • User is enrolled for AIM service • User is eligible to use AIM service • In cases where the user is a tax agent or an intermediary, must have delegated access from the customer
Post-conditions	• User successfully submits a new SOA in accounting software
Constraints	• The SOA must be prepared and submitted through the accounting software • At the time of any service request the accounting software must hold a valid access token for the user
Use case scenarios	
1. Normal flow	1.1 User completes and submits SOA in accounting software 1.2 Accounting software files SOA 1.3 Return service operation 'File' is invoked which validates user's eligibility to use AIM service 1.4 Once user is found eligible, Return service validates the type of Statement of Activity. Please follow exception flows if user is not eligible or Statement of Activity type is duplicate or amended 1.5 For a new Statement, Return service processes the Statement of Activity and sends a success response to accounting software 1.6 Accounting software displays the success message to user 1.7 User views the successful submission of Statement of Activity 1.8 Use case ends
2. Exception flow: The Statement of Activity is a duplicate	2.1 User is found eligible and attempts to submit a duplicate Statement of Activity 2.2 Return service returns an error message to accounting software informing that filing of a duplicate Statement is not allowed 2.3 Accounting software displays the error message 2.4 User views the error message.
3. Exception flow: The Statement of Activity is an amendment	Please follow Use case 3.5 here ('Amend and submit a Statement of Activity')
4. Exception: User is not	4.1 The user is valid, however doesn't have the correct

Use case: Submit a new Statement of Activity		
authorised to use Service		permissions to use this service
	4.2	Identity and Access services respond to third party payroll software with appropriate error message (Please see section 5.1 'Response codes' in the Return service build pack)
	4.3	Identity and Access services record access attempt
	4.4	Use case ends.
5. Exception: Authentication token is expired	5.1	Identity and Access services validate and find authentication token expired due to inactivity (Please see section 5.1 'Response codes' in the Return service build pack)
	5.2	Identity and Access services validate credentials and generates new token
	5.3	Identity and Access services record new token generation request
	5.4	Use case ends.
6. Exception flow: User is not eligible to use AIM service	6.1	Return service validates user's eligibility to use AIM service (please refer eligibility rules here) and finds user not eligible to use AIM service
	6.2	Return service returns an error message to accounting software
	6.3	Accounting software displays the error message with an intent that user is not eligible to use AIM service.
	6.4	User views the error message
	6.5	Use case ends.

3.3 Retrieve the status of previously submitted Statement of Activity and next filing obligation

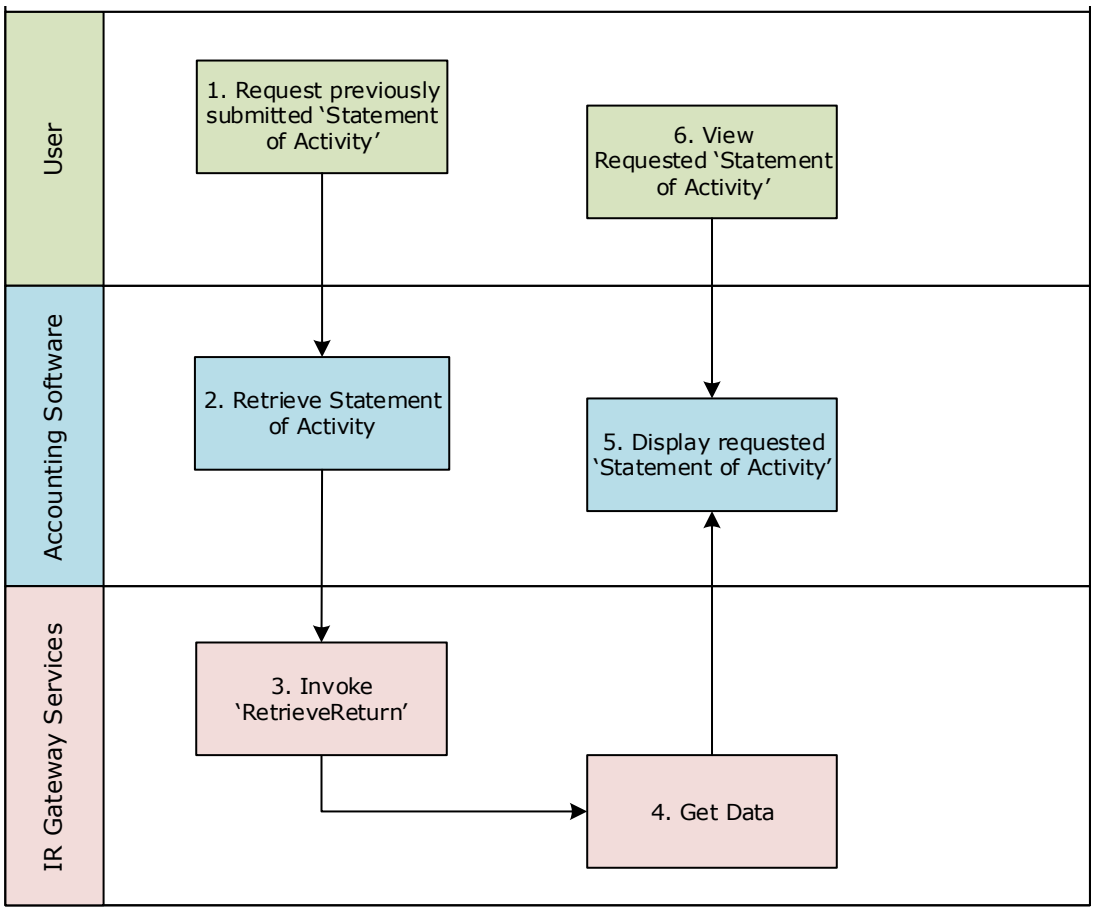


Use case: Confirm the status of previously submitted Statement of Activity and next filing obligation	
Primary actor	• User
Secondary actors	• Accounting software • Gateway Services
Description	• The goal of the user is to confirm the status of previously submitted Statement of Activity and next filing obligation
Pre-conditions	• User is logged-in to accounting software • User has used their IR online services credential to grant accounting software consent to access their information • User is enrolled for AIM service • User is eligible to use AIM service • In cases where the user is a tax agent or an intermediary, they must have delegated access from the customer • User has submitted an SOA in the past
Post-conditions	• User successfully views the status of previously-submitted SOA and next filing obligation

Use case: Confirm the status of previously submitted Statement of Activity and next filing obligation	
Constraints	• At the time of any service request the accounting software must hold a valid access token for the user
Use case scenarios	
1. Normal flow	1.1 User requests the status of previously submitted Statement of Activity and the next filing obligation. 1.2 Accounting software requests the status of previously filed Statement of Activity 1.3 Return service 'RetrieveStatus' operation is invoked 1.4 Return service retrieves the Statement status and provides it to accounting software 1.5 Accounting software requests the next filing obligation 1.6 Return service 'RetrieveFilingObligation' operation is invoked 1.7 Return service retrieves the next filing obligation and provides it to accounting software 1.8 Accounting software displays the requested data 1.9 User views the status of previously submitted Statement of Activity and the next filing obligation 1.10 Use Case Ends.
2. Exception flow: Invalid selection of Statement of Activity	2.1 The user attempts to retrieve the status of the SOA which does not exist 2.2 Accounting software generates a request 2.3 Return service '*RetrieveStatus*' operation is invoked 2.4 Return service fails to retrieve the requested Statement of Activity SOA and returns an error message to accounting software (please see section 5.1 'Response codes' in the Build Pack Returns Service) 2.5 Use case ends.
3. Exception flow: User is not eligible to use AIM service	3.1 Return service validates user's eligibility to use AIM service (please refer eligibility rules here) and finds user not eligible to use AIM service 3.2 Return service returns an error message to accounting software 3.3 Accounting software displays the error message with an intent that user is not eligible to use AIM service 3.4 User views the error message 3.5 Use case ends.
4. Exception: Authentication token is expired	4.1 Identity and Access services validate and find authentication token expired due to inactivity (Please see section 5.1 'Response codes' in the Return service build pack) 4.2 Identity and Access services validate credentials and generate new token 4.3 Identity and Access services record new token generation request

Use case: Confirm the status of previously submitted Statement of Activity and next filing obligation		
	4.4	Use case ends.
5. Exception: User is not authorised to use Service	5.1	The user is valid, however doesn't have the correct permissions to use this service
	5.2	Identity and Access services respond to third party payroll software with appropriate error message (Please see section 5.1 'Response codes' in the Return service build pack)
	5.3	Identity and Access services record access attempt.
	5.4	Use case ends.

3.4 Retrieve previously-submitted Statement of Activity

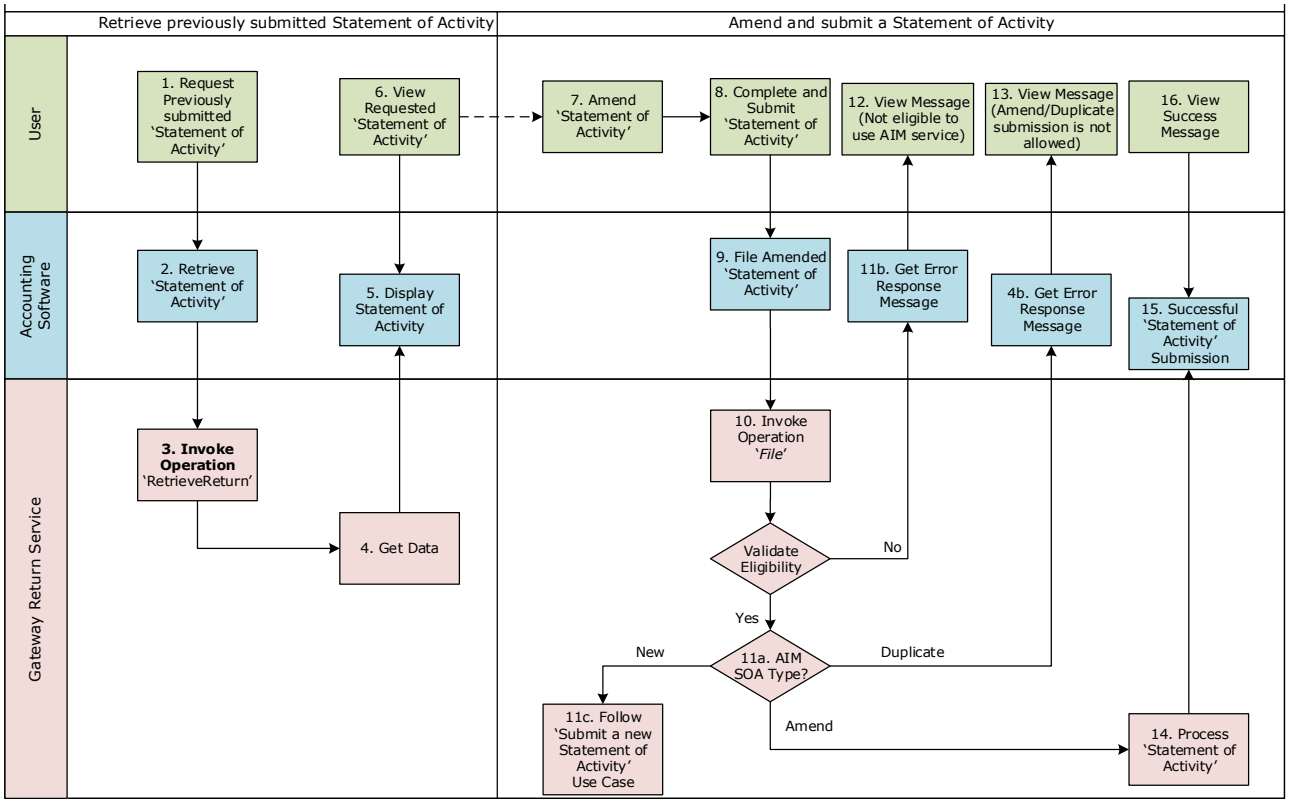


Use case: Retrieve previously-submitted Statement of Activity	
Primary actor	• User
Secondary actors	• Accounting software • Gateway Services
Description	• The goal of the user is to retrieve a previously submitted Statement of Activity (SOA)
Pre-conditions	• User is logged-in to accounting software

Use case: Retrieve previously-submitted Statement of Activity	
	• User has used their IR online services credential to grant accounting software consent to access their information • User is enrolled for AIM service • User is eligible to use AIM service • In cases where the user is a tax agent or an intermediary, they must have delegated access from the customer • User has submitted a SOA in the past
Post-conditions	• User successfully views the previously-submitted SOA
Constraints	• At the time of any service request the accounting software must hold a valid access token for the user
Use case scenarios	
1. Normal flow	1.1 User requests the retrieval of a previously-submitted SOA 1.2 Accounting software generates a request 1.3 Return service '*RetrieveReturn*' operation is invoked 1.4 Return service retrieves the data and returns it to the accounting software 1.5 Accounting software displays the requested information 1.6 User views the requested SOA return 1.7 Use case ends.
2. Exception flow: Invalid selection of Statement of Activity	2.1 The user attempts to retrieve an SOA that does not exist 2.2 Accounting software generates a request 2.3 Return service '*RetrieveReturn*' operation is invoked 2.4 Return service fails to retrieve the requested SOA and returns an error message to accounting software (please see section 5.1 'Response codes' in the Build Pack Returns Service) 2.5 Use case ends.
3. Exception flow: User is not eligible to use AIM service	3.1 Return service validates user's eligibility to use AIM service (please refer eligibility rules here) and finds user not eligible to use AIM service. 3.2 Return service returns an error message to accounting software. 3.3 Accounting software displays the error message with an intent that user is not eligible to use AIM service 3.4 User views the error message 3.5 Use case ends.
4. Exception: Authentication token is expired	4.1 Identity and Access service validates and finds authentication token expired due to inactivity (Please see section 5.1 'Response codes' in the Return service build pack) 4.2 Identity and Access services validate credentials and generate new token 4.3 Identity and Access services record new token

Use case: Retrieve previously-submitted Statement of Activity	
	generation request 4.4 Use case ends.
5. Exception: User is not authorised to use Service	5.1 The user is valid, however doesn't have the correct permissions to use this service 5.2 Identity and Access service responds to third party payroll software with appropriate error message. (Please see section 5.1 'Response codes' in the Return service build pack) 5.3 Identity and Access services record access attempt. 5.4 Use case ends.

3.5 Amend and submit a Statement of Activity



Use case: Amend and submit a Statement of Activity	
Primary actors	• User
Secondary actors	• Accounting software • Gateway Services
Description	• The goal of the user is to successfully amend and submit a Statement of Activity (SOA)
Pre-conditions	• User is logged-in to accounting software • User has used their IR online services credential to grant accounting software consent to access their information

Use case: Amend and submit a Statement of Activity	
	• User is enrolled for AIM service • User is eligible to use AIM service • In cases where the user is a tax agent or an intermediary, they must have delegated access from the customer • User has submitted a SOA in the past
Post-conditions	• User successfully amends and submits an SOA
Constraints	• At the time of any service request the accounting software must hold a valid access token for the user
Use case scenarios	
1. Normal flow	1.1 User requests the retrieval of a previously submitted Statement of Activity 1.2 Accounting software generates a request 1.3 Return service '*RetrieveReturn*' operation is invoked 1.4 Return service retrieves the data and returns it to the accounting software 1.5 Accounting software displays the requested information 1.6 User views the requested Statement of Activity 1.7 User amends and submits the Statement of Activity in accounting software 1.8 Accounting software files the SOA 1.9 Return service operation 'File' is invoked which validates user's eligibility to use AIM service 1.10 Once user is found eligible, Return service validates the type of Statement of Activity. Please follow exception flows if user is not eligible or Statement of Activity type is duplicate or amended 1.11 For a new Statement, Return service processes the Statement of Activity and sends a success response to accounting software 1.12 Accounting software displays the success message to user 1.13 User views the successful submission of Statement of Activity 1.14 Use case ends
2. Exception flow: Invalid selection of Statement of Activity	2.1 The user attempts to retrieve an SOA that does not exist 2.2 Accounting software generates a request which enables Gateway Services to invoke '*RetrieveReturn*' operation 2.3 Gateway Services fails to retrieve the requested SOA and returns an error message to accounting software (please see section 5.1 'Response codes' in the Build Pack Returns Service) 2.4 Use case ends.
3. Exception flow: User is not eligible to use AIM service	3.1 Gateway Services validates user's eligibility to use AIM service (please refer eligibility rules here) and finds user not eligible to use AIM service

Use case: Amend and submit a Statement of Activity		
	3.2	Return service returns an error message to accounting software
	3.3	Accounting software displays the error message with an intent that user is not eligible to use AIM service
	3.4	User views the error message
	3.5	Use case ends.
4. Exception: Authentication token is expired	4.1	Identity and Access services validate and find authentication token expired due to inactivity (Please see section 5.1 'Response codes' in the Return service build pack)
	4.2	Identity and Access services validate credentials and generate new token
	4.3	Identity and Access services record new token generation request
	4.4	Use case ends.
5. Exception: User is not authorised to use Service	5.1	The user is valid, however doesn't have the correct permissions to use this service
	5.2	Identity and Access services respond to third party payroll software with appropriate error message (Please see section 5.1 'Response codes' in the Return service build pack)
	5.3	Identity and Access services record access attempt
	5.4	Use case ends.
6. Exception flow: The Statement of Activity is a duplicate	6.1	User is found eligible and attempts to submit a duplicate Statement of Activity
	6.2	Return service returns an error message to accounting software with informing that filing of a duplicate Statement is not allowed
	6.3	Accounting software displays the error message
	6.4	User views the error message.
7. Exception flow: User is not eligible to use AIM service	7.1	Return service validates user's eligibility to use AIM service (please refer eligibility rules here) and finds user not eligible to use AIM service
	7.2	Return service returns an error message to accounting software
	7.3	Accounting software displays the error message with informing that user is not eligible to use AIM service.
	7.4	User views the error message
	7.5	Use case ends.

4 Testing

4.1 Prerequisites

The Account Management team will ensure the following prerequisites are met by service providers:

- Test dates scheduled with Inland Revenue's Account Management team
- Environments will be booked for testing
- Test user names and data received from Inland Revenue
- Connectivity test to end point achieved
- Relevant information exchanged, such as security certificates, whitelisting IP addresses etc.

4.2 Data management

Data provision	Test data will be provisioned into Inland Revenue systems to enable end to end testing for service providers. An exclusive data set will be provided for service providers to test.
Data reset	Data will be refreshed at the partners' request and provided by Inland Revenue at an agreed time.

Table 3: Data management

Inland Revenue is obliged to maintain the secrecy of any taxpayer related information. This includes information shared between Inland Revenue and business partners during system testing.

All data used in a Test or Quality environment, should be treated as if it were Production quality, with all appropriate controls in place to ensure:

- The environment is controlled and no unauthorised individual can access the testing or staged environments
- Processes are in place to ensure that source copies of data are deleted once testing is completed
- The data used for testing is isolated to prevent accidental use
- Controls are in place to prevent contamination or accidental release to other environments.

4.3 Test execution

Test execution process	• Service providers will execute test scenarios as defined in section 2.3.2 with test data that will be provided by Inland Revenue. • Test results will be documented for each of these scenarios and compared to the expected result associated with that test. • In the event of issues, service providers can follow the issue management process.

Issue management	• Inland Revenue will execute an automated suite of tests daily to ensure the environment is available and functioning to support all external testing by service providers.
	• Disruptions in the service will be notified to service providers testing in this window by the Account Management team.
	  ○ Service providers are responsible for triaging all identified issues to establish if the root cause resides in the system calling the Inland Revenue service. Any issue that requires resolution and retest that impacts the agreed test schedule will be notified to Inland Revenue Account Management.
	  ○ Issues that are not manifested in the service providers systems will be notified to Inland Revenue to triage. Inland Revenue will initiate the automated test suite on demand to isolate and resolve issues.

Table 4: Test execution approach

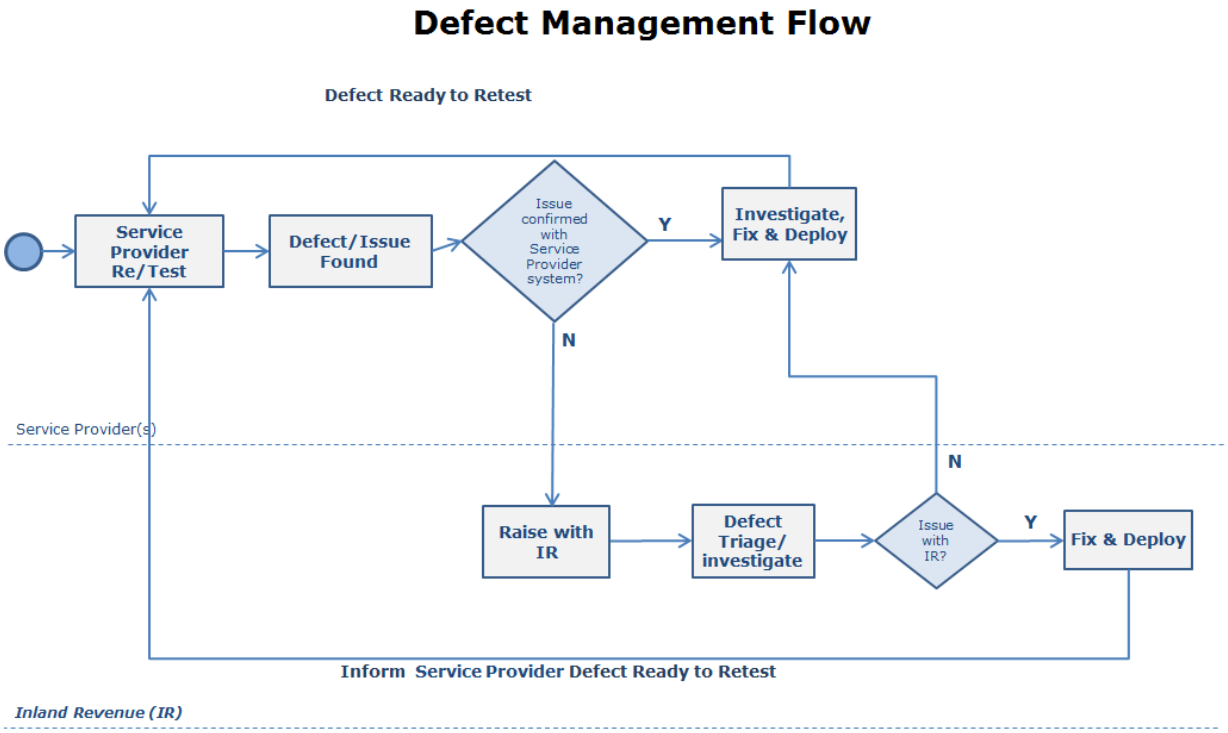


Figure 4: Defect management flow

4.4 Test exit report

Service Providers are required to provide Inland Revenue with evidence of the following:

- That all tests have been executed with associated evidence
- Details of any tests that have not been executed (including a reason)
- Details of all outstanding defects or issues found in test execution.

5 Production support

The following is information for support of the AIM Service.

5.1 Service hours

These are internet-facing services and are generally available 24 hours a day, seven days a week, other than approved scheduled changes, which can usually be accommodated without taking down the system.

In the unlikely event of a unscheduled outage, the IR Relationship Manager will deal with this on a case-by-case basis.

5.2 Service provider support

All support requests are to be directed to the following email address:

SoftwareDevelopersLiaisonUnit@ird.govt.nz

The requests will be picked up by the relationship manager to ensure that they have visibility of the support query and to ensure that the query is directed at the appropriate support team

The relationship manager will be in constant contact in regards of the status of the request.

If it is a major incident please call your Relationship Manager directly.

6 Appendix A—Build pack references

The following Gateway Services build packs complement this one.

6.1 Return service build pack

The Return service build pack describes the operations provided under the Return web service, which forms part of the Gateway Services suite. The operations offered to employers by this service include the ability to request the status or a copy of a previously-filed return, request a prepopulated return, file a new return and request the next filing obligation.

This AIM onboarding document was written using information from version 0.8 of the Return Service build pack.

6.2 Identity and Access services build pack

The Identity and Access (IAS) services build pack describes the operations provided under Identity and Access services, which is another part of the Gateway Services suite. These services are used to authenticate access.

This AIM onboarding document was written using information from version 1.5 of the Identity and Access Services build pack.

7 Appendix B—Glossary

Acronym/term	Definition
Activity statement	Formally known as the Statement of Activity—the name for the data that is filed for AIM.
AIM	Accounting Income Method—a method that businesses can use for reporting and paying provisional income tax. Participating business are required to file a Statement Of Activity.
Authentication	The process that verifies the identity of the party attempting to access IR.
Authorisation	The process of determining whether a party is entitled to perform the function or access a resource.
EA	Employment Activities—umbrella term for employment activities performed using the Return service (submission of Employment Information) and/or Employment service (submission of Employee Details) operations
ED	Employee Details—data submitted by an employer to IR relating to new, existing, or departing employees that is submitted via the Employment service.
EI	Employment Information— data submitted by an employer relating to deductions made for their employees for a paydate.
eServices	START's authenticated customer-facing portal.
Gateway	START's web services gateway.
GST	Goods and Services Tax.
GWS	GateWay Services—the brand name for the suite of web services that IR is providing. The Employment Service is a Gateway Service.
HTTP(S)	Hyper Text Transmission Protocol (Secure)—the protocol by which web browsers and servers interact with each other. When implemented over TLS1.2 HTTP becomes HTTPS.
IAMS	Identity and Access Management—a logical component that performs authentication and authorisation. Physically it is a set of discrete hardware and software products, plug-ins and protocols. Usually implemented as separate External IAMS (XIAMS) and Internal IAMS.
IP	Internet Protocol—the principal communication protocol in the Internet protocol suite for relaying datagrams across networks.
NZISM	NZ Information Security Manual—the security standards and best practices for Government agencies. Maintained by the NZ Government Communications Security Bureau (GCSB).
OAuth2	An HTTPS based protocol for authorising access to a resource, currently at version 2.
SOAP	Simple Object Access Protocol—a set of standards for specifying web services. Gateway Services uses SOAP version 1.2.
SSL	Secure Sockets Layer certificates—used to establish an encrypted connection between a browser or user's computer and a service or website.
START	Simplified Taxation and Revenue Technology—IR's new core tax

Acronym/term	Definition
	processing application. It is an implementation of the GenTax product from FAST Enterprises.
Statement of Activity	See Activity Statement
TLS1.2	Transport Layer Security version 1.2—the protocol that is observed between adjacent servers for encrypting the data that they exchange. Prior versions of TLS and all versions of SSL have been compromised and are superseded by TLS1.2.
URL	Universal Resource Locator—also known as a web address.
WSDL	Web Service Definition Language—an XML definition of a web service interface.
XIAMS	External IAMS—an instance of IAMS that authenticates and authorises access by external parties, i.e. customers, trading partners etc. as opposed to internal parties such as staff.
XML	Extensible Markup Language—a language used to define a set of rules used for encoding documents in a format that can be read by humans and machines.
XSD	XML Schema Definition—the current standard schema language for all XML data and documents.