Australian Government
Australian Taxation Office

Operational Framework for Developers and Service Providers

Overview

Intent

Develop an **Operational *Framework for Developers and Service Providers*** that sets out how the ATO will provide access to and monitor the digital transfer of data through software/applications.

Background

Demand for digital services is increasing. The community expects to leverage their natural systems and interact with government through software solutions.

Government is investing in digital service offerings, through Standard Business Reporting (SBR) and by publishing ATO Application Programming Interfaces (API). This enables developers to offer services through business applications on various platforms, such as mobile applications. These offerings will increase two-way data flows, where information is pulled down from the ATO through software, as opposed to the more traditional 'inbound' data flows (e.g. lodging forms to the ATO).

Businesses are increasingly moving to cloud based software solutions, changing the risk environment for Government services. Developers are starting to transition to the Cloud Software Authentication & Authorisation (CAA) solution and the Practitioner Lodgment Service (PLS).

There is a need to provide guidance to our partners and address potential risks to the ATO arising from the introduction of ATO published APIs and the increased use of two-way data flows. The following areas require further development:

- Registration process for businesses looking to develop software or applications that connect to ATO held data
- Best practice guidelines and minimum requirements developers/service providers products and supporting environments must meet to be certified
- Capability to proactively detect potential fraud or threats to ATO systems (in real time or close to real time) and an incident management process to address known or potential impacts.

Software Industry Consultation

- We are working with a small group of developers to represent the broader industry. We will continue to consult with industry throughout the development and implementation of the framework as the need arises.
- Information on the development of the framework is available on http://softwaredevelopers.ato.gov.au/operational_framework

ATO Contact

Robyn Theacos
Email: Robyn.Theacos@ato.gov.au

Government Approach – A Global Snapshot

United Kingdom

- Software developers are required to register with Her Majesty's Revenue and Customs (HMRC) by completing an online form which captures basic information e.g. name, address, phone number
- Developers undertake self assessment against technical specifications provided
- Commercial software developers are listed on the HMRC website.

What they're saying:

The table below shows a list of commercial software suppliers that have successfully demonstrated the ability to submit [specific] requests online.

In each case, HMRC will accept these details for the products that are listed. HM Revenue and Customs (HMRC) can't recommend or endorse any one product or service over another and will not be responsible for any loss, damage, cost or expense in connection with using this software.

If you encounter any problems when using commercial software, please contact the software supplier. They will work with HMRC to resolve any issues. HMRC do not carry out any form of security testing of these products or the services provided, so customers are encouraged to ask their suppliers about this. Follow the link below to read about the security of the HMRC services that these products and services interface with.'

New Zealand

- Software developers interested in registering with the New Zealand Inland Revenue Department (NZIRD) are required to contact the software developers liaison unit with their contact details and an outline of the service they want to provide
- Technical specifications are published on their website including payroll and withholding tax documents
- The first API for submitting GST returns will be made available in March 2016 with additional APIs expected to be published later in the year
- The APIs can be used by software providers who are developing services for accounting, finance and tax processing
- Software providers will be required to meet a range of criteria relating to security, tax compliance and privacy. Developers will be required to consent to a criminal history check via the New Zealand Department of Justice

What they're saying:

'As a software developer it's your responsibility to:

- *meet your customers' needs with your software package*
- *comply with tax legislation*
- *cover any start-up costs or costs you may incur creating your software package*
- *ensure you exchange information securely.*

You need to tell us as soon as possible, if you:

- *change your name*
- *have any incidents with your products or services*
- *change your contact details, eg:*
  - *physical address*
  - *website/s*
  - *phone numbers, and*
  - *email addresses.'*

United States of America

- Developers are required to create an online account with the IRS including:
  - Provision of personal information i.e. name, Social Security Number, date of birth, phone number, address, income
  - Create a username, password and PIN
- Registration is confirmed via code sent in the mail
- Every principal and responsible official in the firm is also required to create an account
- They then apply to become an authorised provider. This is a 'comprehensive application… necessary to protect the integrity and security of the electronic filing system' that may take up to 45 days to approve. This process includes providing fingerprints to the IRS via a trained professional.
- IRS conducts a suitability check on the entity and each person listed in the application which may include tax compliance, credit and criminal background check.

What they're saying:

'Software Developers must pass either acceptance or assurance testing. If a Provider is a Software Developer that performs no other role in IRS e-file but that of software development, its Principals and Responsible Officials do not have to pass a suitability check during the application process.

A Software Developer has a variety of responsibilities that include, but are not limited to the following:

- *Promptly correcting any software error causing returns to reject and distributing the correction*
- *Ensuring its software creates accurate returns*
- *Adhering to specifications provided by the IRS in publications'*

Scope, Risks and Test Scenarios

In scope

The following areas are in scope and will be covered. The framework will:

- be specifically focused on ATO with consideration given to whole-of-government where appropriate
- cover digital services offered through SBR and future release of APIs
- address software/applications provided in-house and commercial solutions, cloud and non-cloud
- provide registration criteria for developers/service providers seeking access to ATO software services
- outline guidelines and requirements developers/service providers and their products must meet to become certified
- include the capability to monitor developer/service provider compliance against the criteria and requirements set, monitor the interactions through ATO systems to identify threats and fraudulent activity, and establish an incident notification process for developers/service providers
- incorporate an implementation and communication approach

Out of scope

- Certification of individual forms is out of scope. The overarching product will be reviewed for compliance.

Assumptions

Any channel used to connect with third party software to the ATO (SBR and any other channels that supersede it) will be secured in alignment with the highest classification of data that will be sent across the channel

Test scenarios

Outlined below are scenarios that have been used to test that the framework developed addresses the requirements.

Scenario 1: A fraudulent developer/service provider seeking access to ATO systems

Scenario 2: A legitimate but inexperienced or unsophisticated developer/service provider (e.g. has security flaws in their systems/products)

Scenario 3: A legitimate developer/service provider that continually releases new versions of their product and does not provide support to its users

Scenario 4: A legitimate developer/service provider that is not compliant in their own obligations as a business/company

Risks

The framework has been developed to address risks identified in the enhancement to SBR and release of ATO APIs:

- Current network of software developers/providers are well known to the ATO, there are established relationships and a level of assurance in the security of their systems through existing processes. It is expected the network of software and application developers will grow substantially and this level of assurance will decrease through the introduction of small, less experienced developers with unknown infrastructure.
- This creates potential for misuse of user credentials/accounts and unauthorised access to ATO data/information through security vulnerabilities in software products leading to identity theft.
- Currently interactions between the ATO and software are predominantly lodgment of forms (ie one-way). The enhancements to SBR and provision of APIs will increase two-way data flows where information is pulled down from the ATO through software as opposed to more traditional 'inbound' data flows. The ATO has no oversight or control over how information is handled or accessed outside of ATO systems. Information may also be stored outside of Australia and therefore subject to foreign laws. There is also potential for the release of restricted client data to unauthorised parties (e.g. Special interest Indicator clients, RACS, High Wealth, High profile).

Mitigation via Operational Framework

- The Operational Framework will provide best practice guidelines and minimum requirements to software developers on how to store, share, handle and access provided information once received by their system.
- The Operational Framework will develop a monitoring capability and incident management plan for software incidents that happen outside the ATO environment.

Framework Summary

Developer registration

The introduction of a single, more stringent registration process* for businesses looking to develop or provide software or applications that connect to ATO data services.

Includes the following:

- Single registration form ensuring the applicant is associated/authorised to represent the business
- Updated internal processes with checks to ensure the business is legitimate and tax obligations are up to date
- Updated declaration/terms and conditions

Developer System/Product Vetting (Certification)

The introduction of a best practice guidelines and minimum requirements* that ensure 'whitelisted' products and their supporting systems have the appropriate security controls in place to protect business information.

Includes the following:

- Development of best practice guidelines to assist software/app development
- Development of minimum requirements software/app and supporting systems must meet
- Development of self-certification process for software product and its environment
- Development of a risk based approach to verify that products and their supporting environment comply with ATO's best practice guidelines and minimum requirements
- Updated declaration/terms and conditions

Monitoring capability

The development of a capability to monitor and proactively detect potential fraud or threats to ATO systems (real time or close to real time)and an incident management process to address known or potential impacts to developers or their clients.

Includes the following:

- Develop and mature a monitoring capability that monitors the environment and developer and provider activity in ATO systems
- Identify opportunities to automate verification of developer and provider compliance against standards/minimum requirements
- Develop a breach/incident notification process

**Registration, guidelines and requirements will differentiate between developers and service providers where appropriate.*

Roles and Framework Application

Role definitions *(Entities may have multiple, concurrent roles)*

Role	Description
Developer (API, mobile app, software)	An entity that develops commercial software or applications designed to assist users in meeting tax and super/government reporting obligations. Responsible for: ▪ Development and support of software or applications in line with documented requirements (e.g. MIGs, BIGs etc.) ▪ Ongoing development to maintain software or application currency (e.g. support tax time releases, transition to cloud solution, PLS)
In-house developer	An entity that develops in-house software or applications designed to assist their own tax and super/government reporting obligations.
Service Provider (e.g. software provider, gateway providers, clearing house)	An entity that offers developed software or application as a service. Responsible for: ▪ Administration of supporting systems ▪ User support ▪ Storage of information and related controls (cloud)
Cloud Provider	An entity that offers cloud infrastructure that can be utilised by a developer, service provider or end user. Responsible for: ▪ Secure storage and transfer of information
Intermediary and Tax Professional (e.g. tax agents, BAS agents, bookkeeper, payroll provider)	Assists businesses and individuals to meet tax obligations. Users of tax practice/payroll software or applications.
Businesses and Individuals	Users of software or application(s)

How the Framework applies

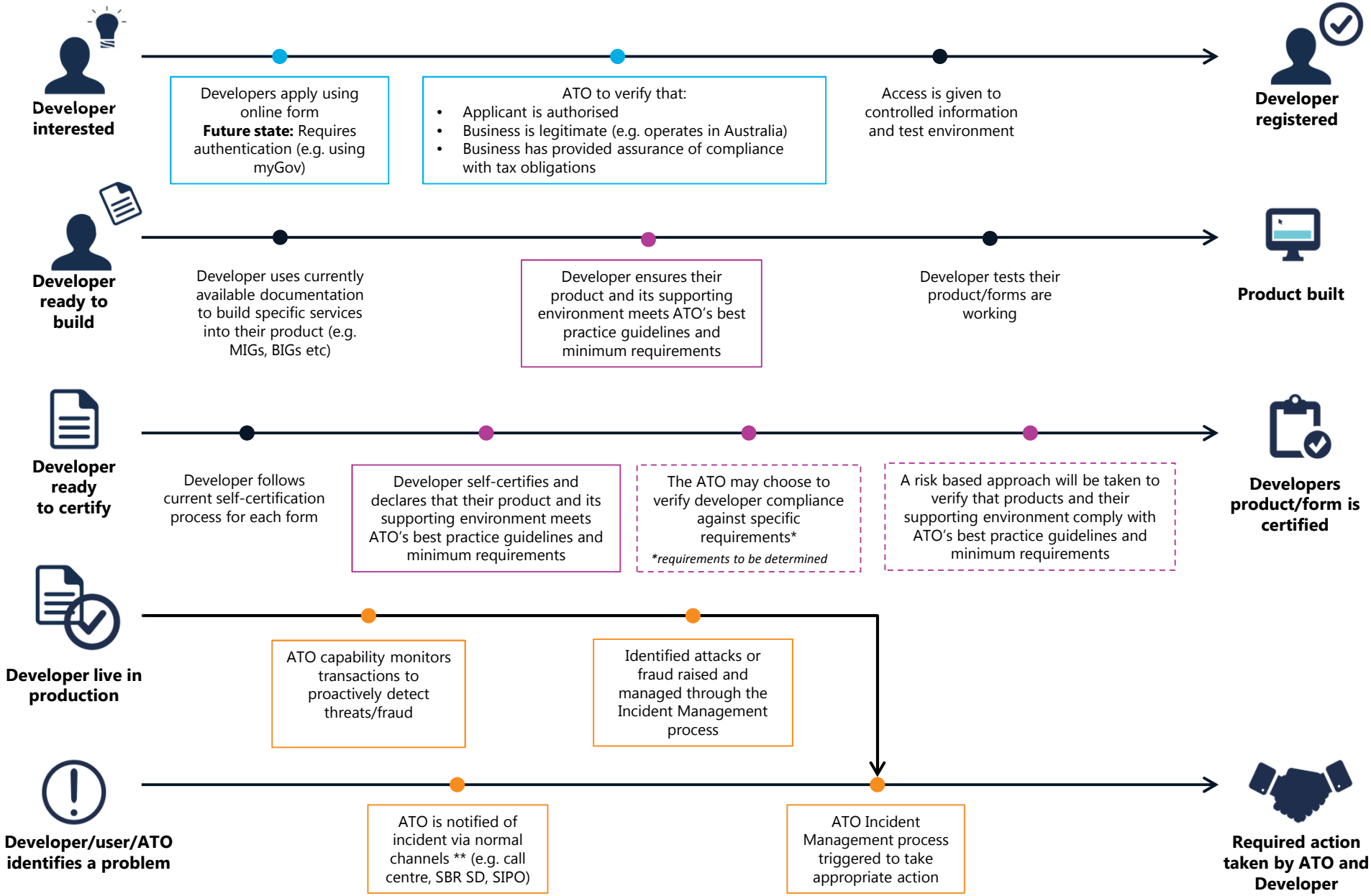
Entity is required to register

Entity is required to self-certify, meet guidelines and minimum requirements

Scenario	Developer (D)	Service Provider (SP)	Cloud Provider (CP)	In-house developer (IHD)
Desktop software developed, then installed and managed by business user (D→User)		N/A	N/A	N/A
Software or application developed and offered as a service by the same entity (D/SP→User)			N/A	N/A
Software or application developed by one entity and offered as a service by another (D→SP→User)			N/A	N/A
In house software or application developed to meet its own entity reporting obligations (IHD/User)	N/A	N/A	N/A	
Cloud based software or application offered using the service providers cloud infrastructure (D/SP/CP→User)				N/A
Cloud based software or application offered using third party cloud provider's cloud infrastructure (D/SP→CP→User)			**	N/A

***no requirement to self-certify, must meet guidelines and minimum requirements*

High Level Overview – Developer life-cycle



***note** incidents may also be raised through other channels*

1. Developer registration

Lead: Robyn (SIPO) | Key Contributors: Stephen (BRR) Anna (eCSD)

What do we know now?

- Developers apply online or via a web form to become registered to access ATO materials
- Currently two forms collect various information but not consistent
- SBR developers must read and accept the SBR Disclaimer and Conditions of use before submitting the form
- Forms actioned by SIPO and SBR Service Desk (including BRR involvement)
- Minimal (and different) checks completed for each form
- Developer notified by email that they have been successfully registered
- Developers given access to information/test environment depending on what they have registered for

Note: Whilst the current state is focused on SBR related processes, the scope of 'Developer registration' would be applied more broadly to cover API developers etc.

What needs to change?

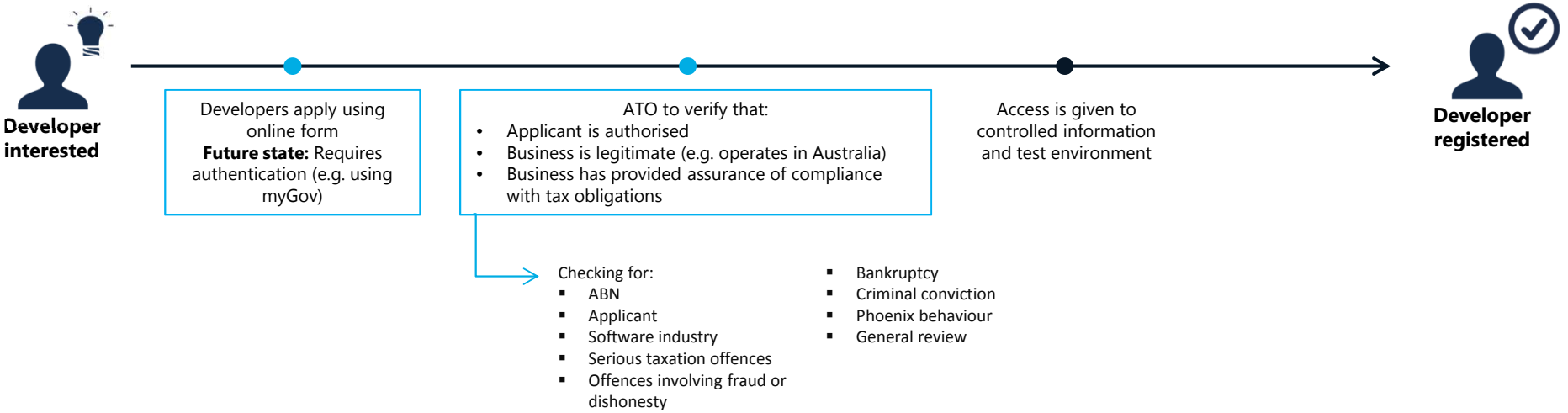
- Determine the criteria developers/service providers need to meet before being registered
- Determine what information we need to capture as part of the application
- Determine what needs to be included in terms and conditions/user agreements
- Determine what the updated registration process would be – high level
- Determine the trigger points for rejecting a registration

What are the gaps/issues?

- Single area to undertake registration process and review process – resource allocation?
- Smarter Data support to assess applications for specific criteria – resource allocation?
- Service standard – currently very quick but minimal checks are undertaken
- Current process does not include assurance that tax obligations are up to date

1. Developer registration | recommendations

Lead: Robyn (SIPO) | Key Contributors: Stephen (BRR) Anna (eCSD)



***Note** while the diagram reflects ATO process only, this is also applicable for whole-of-government developer registration processes*

End state overview

- Single registration process for access to ATO information and test environment.
- Eligibility elements to be assessed (including assurance of compliance behaviour, criminal history and bankruptcy etc).
- Information requested for a specific purpose eg identification/authentication, intent, purpose of access.
- Terms and conditions that support the process.
- Processing service standards for registration.
- Single register of developers/providers maintained in the ATO.
- Registrations to be reviewed annually for those that have not certified.

Recommendations

Short term

1. Develop a single registration form.
2. Develop high level process (existing back end process to remain unchanged).
3. Review/update terms and conditions/user agreements to support the process.

Medium term

1. Implement process.
2. Determine data or tools that will assist in automating the registration process.

Long term

1. Consider digital authentication as a requirement for registration.
2. Explore use across whole-of-government.
3. Determine and implement appropriate management system.

2. Developer system/product vetting (certification)

Lead: Anna (eCSD) | Key Contributors: George (CS&S) Grant (GC) Belinda (ITSec) Rebecca (IS)

What do we know now?

Certification

- Once a developer has built their product and is satisfied with their testing results, certification is requested via email to the SBR Service Desk. This request includes a Portable Documentation Format (PDF).
- SBR is a self-certification process, certification is against each form (e.g. BAS, CTR etc.), all tests focus on business functions only.
- eCSD verifies self-certification results to ensure the messages are sent through correctly. If eCSD are not satisfied with the results they will request additional tests to be carried out.
- In some cases (e.g. for SBR2) developers are asked to perform Production Verification Test (PVT) – pilot in production to also perform end-to-end testing.
- Once eCSD are satisfied with the results and all errors are rectified, the software product and service/form is added to the product register (whitelisted) and developers are given access to call the certified services in production.

Cloud providers

- Cloud providers are asked to declare that their product meets the specified requirements (e.g. minimum authentication requirements) via an online form.
- The SBR Service Desk is notified and developers are given relevant access in Access Manager to set up their device AUSkey and manage cloud nominations.
- The product register is also updated to indicate that they are an approved cloud provider.

Developer system/product standards

- Currently no ATO guidelines or standards have been set that around how developers deal with cloud storage and data security. Industry guidelines for cloud are available, but they are not enforceable.
- ABSIA are currently developing guidelines for cloud developers in collaboration with Standards Australia.

Note: Whilst the current state is focused on SBR related processes, the scope of 'Developer system/product vetting' would be applied more broadly to cover API developers etc.

What needs to change?

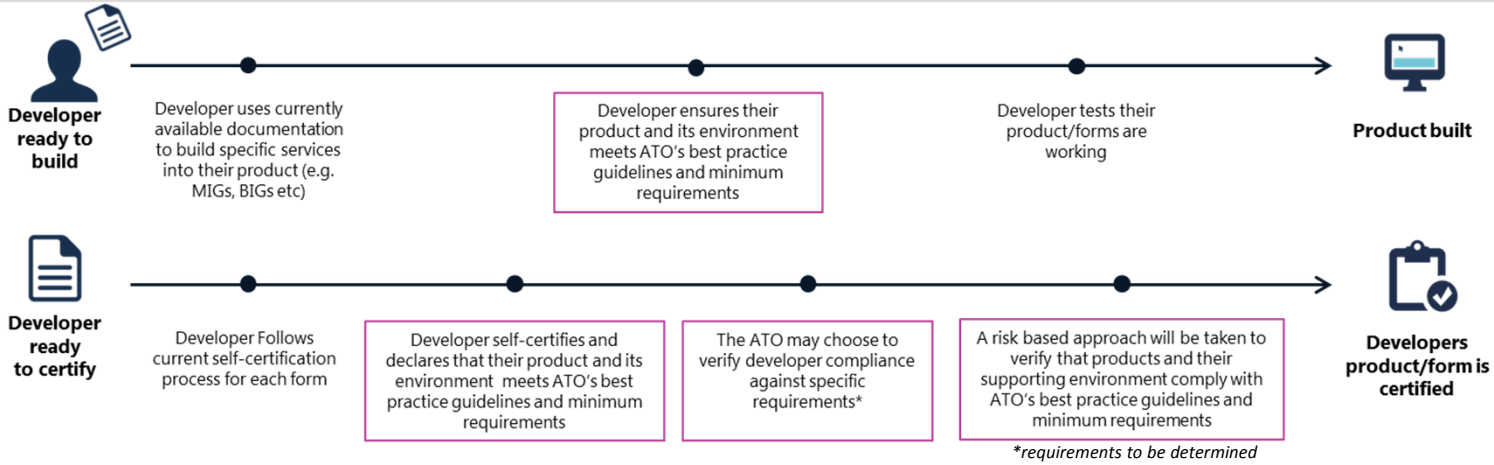
- Determine what the high-level guidelines are in relation to authentication, authorisation, storage and data security (cloud and non-cloud) including recommendation of ISO standards (e.g. 27001-5 and 27017).
- Determine what the required minimum requirements are in relation to authentication, storage and data security (cloud and non-cloud).
- Determine what needs to be included in terms and conditions/user agreements/legal declarations for either self-certification or ATO/ATO-sponsored certification process.
- Determine the high level vetting (certification) and whitelisting process.
- Determine the risk based approach to verify compliance against minimum requirements. For example
  - Test the product against required security controls
  - Evaluate the third party provided documentation for its environment and/or product , i.e. against required standards and best practice guidelines.
- Determine the trigger points for rejecting, suspending or cancelling a certification.
- Determine the validity timeframe for whitelisted products.

What are the gaps/issues?

- Do we need to be more stringent in accepting API developers than others?
- How do we apply the certification process to existing third parties already interacting with the ATO?

2. Developer system/product vetting (certification) | recommendations

Lead: Anna (eCSD) | Key Contributors: George (CS&S) Grant (GC) Belinda (ITSec) Rebecca (IS)



End state overview

- Developers/service providers will refer to best practice guidelines developed to ensure their product/service meets expected standards (inc. authentication, data security and storage). Guidelines will be based on ISO 27001-27005 (information security) and ISO 27017 (cloud specific security).
- Developers/service providers will self-certify that their product and/or system meets minimum requirements specified by the ATO.
- A risk based approach will be taken to verify that products and their supporting environments comply with ATO's best practice guidelines and minimum requirements (e.g. can be randomly targeted or based on a risk profile etc).
- The ATO may choose to verify developer compliance against specific requirements (this is dependent on the determined set of requirements).

Recommendations

Short term

1. To support the release of DES, engage an external consultant to perform an independent assessment (focused on the developer). Outcomes to inform the Framework.
2. Develop and publish best practice guidelines and minimum requirements in consultation with industry representatives (e.g. ABSIA and SWD working group) including reference to data held in transit.
3. Develop high level processes for certification/vetting.
4. Develop interim process for on-boarding new cloud developers seeking approval to consume the CAA solution – until Framework in place.

Medium term

1. Determine a risk based approach to verify developer/service provider compliance against minimum requirements.
2. Implement self-certification/vetting process.
3. Update terms and conditions/user agreements to support the process.

Long term

1. Develop functionality and risk based approach to obtain and test products end-to-end.
2. Determine data or tools that will assist in automating the vetting process.
3. Develop existing capability to ensure currency of standards and requirements, detect potential fraud behaviour within certification process.

3. Monitoring capability

Lead: Veli (SDP) Rebecca (IS) | Key Contributors: Stephen (BRR) Anna (eCSD) George (CS&S) Ian (Super) Belinda (ITSec) Hilary (CAS)

What do we know now?

- Manual processes monitor developer interactions for specific services only (e.g. SuperTICK).
- Audit logs are captured, however these are only used to investigate specific fraud cases. It is unclear whether current audit logs capture the right information to monitor developer activity effectively.

Incident Management

- Different third party groups may wish to develop ATO services (e.g. known SBR, new emerging SBR, API, mobile app) and require access to ATO information. Incidents could occur across any of these different environments.
- Software developers operate outside the ATO environment. Relationships between developers and their business client may not be known by the ATO.
- ATO does not have an integrated organisational process for managing and responding to software developer incidents.
- There is no formal process for software developer groups to notify the ATO of incidents (multiple contact channels are currently used, e.g. SBR service desk phone and email, SWD Technical help desk phone and email, AUSkey phone line, SIPO helpdesk phone and email, ATO Business phone line, general direct email or phone contact).
- Current SBR terms and conditions, software registration and certification processes do not include ATO expectations for incident notification or sharing of information.

What needs to change?

- Develop capability to monitor developer/provider interactions and proactively detect and respond to threats/fraudulent activity
- **Lead:** Veli (SDP) **Key Contributors:** Ian (Super) Anna (eCSD) Belinda (ITSec)
- Establish an incident management process for developer/provider interactions including:
  - Notification of an issue (including legal and expectation based responsibilities)
  - Response strategy within the Community Information Incident Framework for protection of clients affected, guidance assistance to the developer/provider to recover, and support for tax agents who might also be affected
- **Lead:** Rebecca (IS) **Key Contributors:** Anna (eCSD) Belinda (ITSec) Hillary (CAS)

What are the gaps/issues?

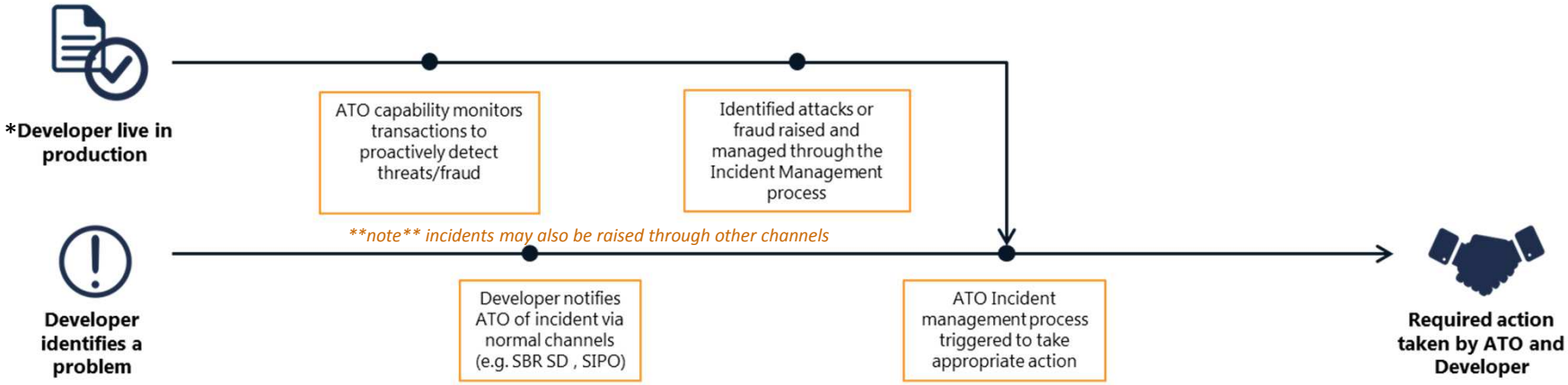
- Capability to monitor developer/provider interactions may take time to establish. What can be done in the interim?
- Current audit logs may not capture the required information to monitor developer/provider activity effectively.
- Resource allocation – who will do the work?
- Development and deployment of visualisation/Cognos, SASVA reports.
- Development and implementation of treatment plans.
- Treatment plan effectiveness measures.
- Gap analysis to assess existing capability (tools, team, data capture, logs)
- Proactive monitoring and predictive analytics for threats and cyber (IT) security perspectives do not currently exist. Investment is needed to build this capability.

Incident Management

- If a developer/third party does not notify of an incident, what recourse does the ATO have?
- Information sharing - software developers and some third parties (e.g. intermediaries) do not have a right to business user information. What information can the ATO share, when, and to whom?
- Managing incident notification from small/new developers/providers whose market segment is not big enough for them to worry about reputational issues/delisting.
- Transparency for intermediaries and the end to end incident where different developers/providers and environments are involved to enable containment of any breach and effective communication? (Complex environments are emerging)
- Access to third party logs may not be available or effective for managing and mitigating issues post event.
- Software developers by default set their products to not log transactions, so a user is required to manually change the default.
- For cloud-based transactions, who would the ATO have an agreement with?
- Incident types and levels requiring notification are not currently defined for third party software.

3. Monitoring capability | recommendations

Lead: Veli (SDP) | Key Contributors: Stephen (BRR) Anna (eCSD) Ian (Super) Belinda (ITSec)



*Process applies to developers and providers

End state overview:

- A capability established to monitor interactions that come through the SBR channel, using information collected by the ATO (e.g. CAL logs).
- Use 'real-time' analytic (digital suppression) and data visualisation tools developed to proactively detect fraudulent activity and threats to the ATO.
- Dedicated resources assigned to detect and treat fraud.
- Identified fraud or threats are fed through the Incident Management process to trigger action/resolution.
- Leverage off the current Online Analytics capability to automatically trigger actions that protect against fraud and threats to the ATO.
- Use the insights gained from analytics capability to continually develop and mature the developed tools and business rules.

Recommendations

Short term

1. Explore the use of current audit logs to develop interim monitoring capability.
2. Review info captured in audit logs and identify gaps.
3. Explore behavioural indicators and capability to develop analytical models.
4. Partner with areas with existing capability.

Medium term

1. Establish project team to mature monitoring capability.
2. Develop business case to leverage on-line analytics and EST program of work.
3. Identify and connect additional data (data virtualisation).
4. Build on behavioural indicators to be more sophisticated and near real time.

Long term

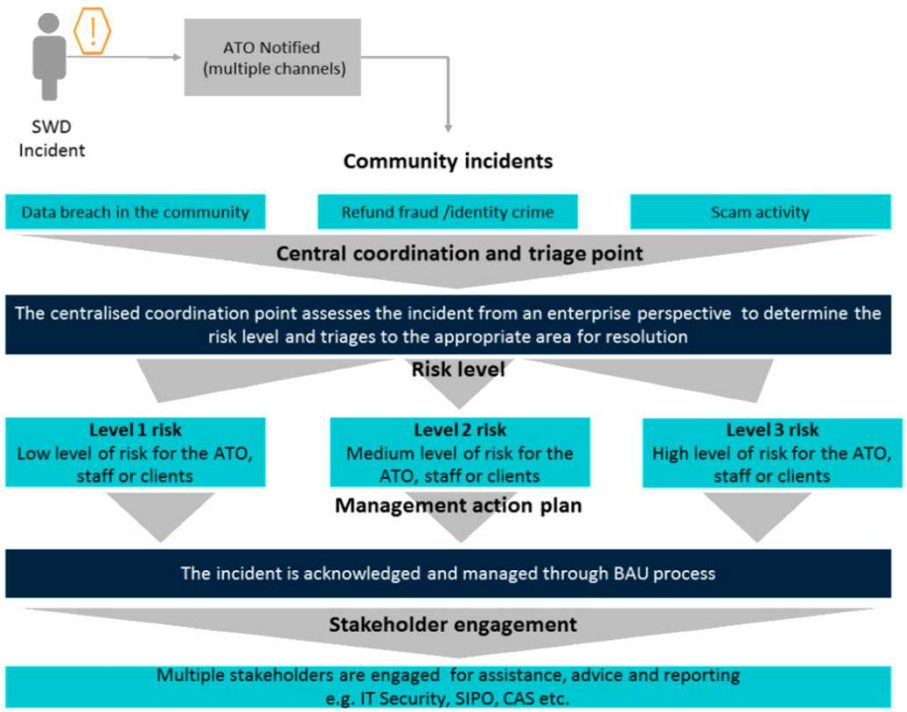
1. Capture and store logs real time in EDH/EDW.
2. Mature analytical models.
3. Develop and implement digital event processing.
4. Develop visualisation dashboard.
5. Develop and deploy treatment plans.
6. Develop effectiveness measures.

3. Monitoring capability - Incident management | recommendations

Lead: Rebecca (IS) | Key Contributors: Anna (eCSD) Belinda (ITSec) Hilary (CAS)

End state overview:

- Upon certification, any third party developing/providing services requiring access to ATO information:
  - Must notify the ATO and their business user as soon as possible after an incident occurs, or within 24 hours of the event
  - Accepts the ATO will take all reasonable steps required to contain any data breach including contacting business users
- Irrespective of which channel a notifier uses to contact the ATO, a central co-ordination point will triage and route the incident appropriately for action (i.e. no wrong door approach).
- Notification of a community incident in relation to software developers, will feed into ATO's Community Incident Management process.



Recommendations

Short term

1. Develop and communicate ATO expectations for developer/third party interactions.
2. Update certification process to include requirement for notification and agreement for information share.
3. Leverage the Community Incident Management process, strengthening communication between ATO and developer groups.

Medium term

1. Develop a central co-ordination point for all incident notifications.
2. Review the Community Incident Management process and determine software developer incidents that would fall into low, medium and high risk level ratings.
3. Incorporate and test a software developer scenario as part of the Business Continuity Incident Framework.

Long term

1. Consider opportunity to provide a single or known entry point for incident notification (maintaining a no wrong door approach).
2. Work with industry to provide feedback and communicate incident resolution examples to share intelligence and shape product improvements.

Glossary

ABSIA	Australian Business Software Industry Association
API	Application Programming Interface
BIG	Business Implementation Guide
BRR	ATO Business Reporting and Registration
CAA	Cloud Software Authentication & Authorisation
CAS	ATO Client Account Services
CS&S	ATO Customer Service and Solutions
eCSD	ATO eCommerce Service Delivery
GC	ATO General Counsel
IS	ATO Information Security
ISO	International Standards Organisation
ITSec	ATO Information Technology Security
MIG	Message Implementation Guide
PLS	Practitioner Lodgment Service – outcome of the Electronic Lodgment Service to Standard Business Reporting (ELS2SBR) project
PVT	Production Verification Testing
RRG	Rapid Response Group
SBR	Standard Business Reporting
SBR SD	Standard Business Reporting Service Desk
SDP	ATO Smarter Data Program
SIPO	ATO Software Industry Partnership Office
WIG	Web Service Implementation Guide

HMRC Agent authorisation: commercial software suppliers
https://www.gov.uk/government/publications/agent-authorisation-commercial-software-suppliers/agent-authorisation-commercial-software-suppliers

IRS
https://www.irs.gov/uac/Software-Developer
https://www.irs.gov/Tax-Professionals/e-File-Providers-&-Partners/Become-an-Authorized-e-file-Provider

NZIRD
http://www.ird.govt.nz/software-developers/about/
http://www.ird.govt.nz/software-developers/technical/
http://www.ird.govt.nz/software-developers/technical/api/