



Australian Government
Australian Taxation Office

ATO-SwD Partnership Event - Strategic working group

Operational Framework for Developers and Service
Providers

Presented by George Afarian
3 March 2016

- Overview of the scope and background to date
http://softwaredevelopers.at0.gov.au/operational_framework
- Outline of the proposed Developer Registration
- Outline of the proposed Product Certification
- Outline of the draft “Best practice guidelines and minimum requirements”
- Software industry feedback on certification, guidelines, minimum requirements, verification
- Software industry feedback on next steps



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 third party data services.



Developer System / Product Vetting (Certification)

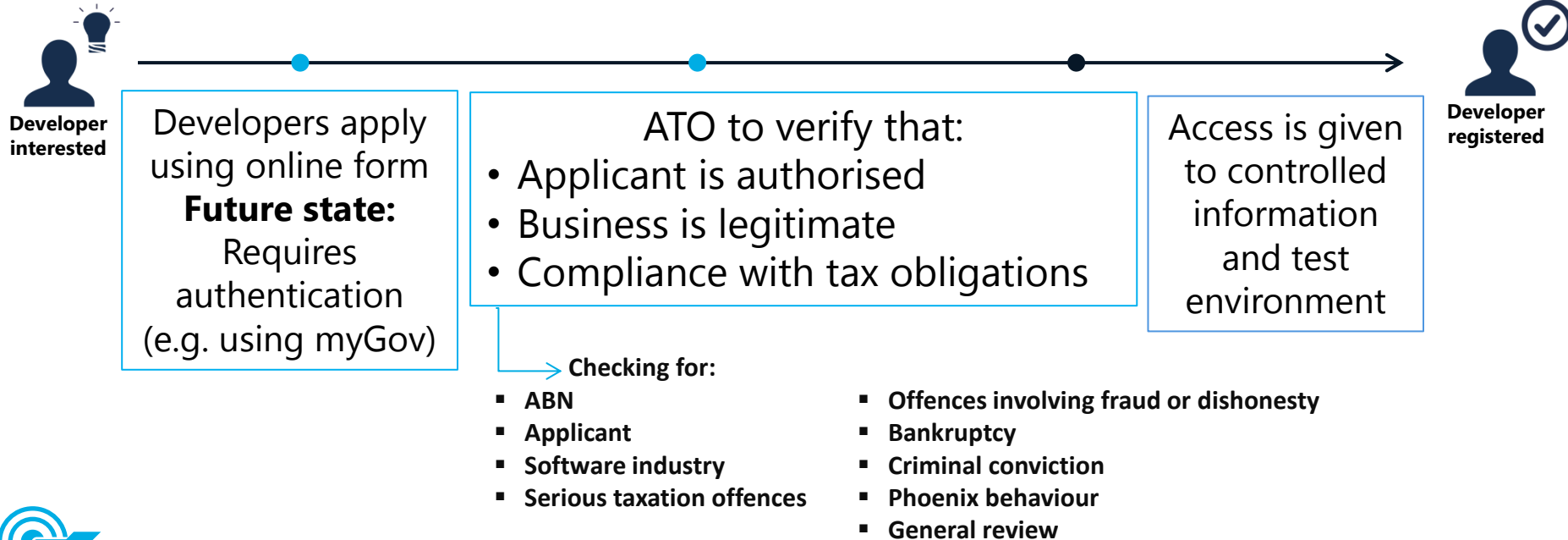
The introduction of a best practice guidelines and minimum requirements* that ensure 'whitelisted' products and their supporting systems have the appropriate security controls in place to protect business information.



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.

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



End state overview

- **Single registration** process for access to ATO information and test environment
- **Eligibility elements** to be assessed (including 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

Information required for registration

ABN:	What information do you wish to access
Name of entity:	<input type="checkbox"/> Tax Preparation
Trading name:	<input type="checkbox"/> Tax file number
Main business location:	<input type="checkbox"/> Tax time
Applicant details	<input type="checkbox"/> eBMS3 –
Name:	<input type="checkbox"/> Software will be developed principally for use by tax practitioners
Position in entity:	
Contact number:	Which segment(s) are you developing for:
Email:	<input type="checkbox"/> Superannuation
	<input type="checkbox"/> Tax Preparation
Select the one that applies to you	<input type="checkbox"/> Payroll
<input type="checkbox"/> Software developer	<input type="checkbox"/> Business Accounting
<input type="checkbox"/> Mobile device/App developer	<input type="checkbox"/> Other - provide description
<input type="checkbox"/> Software service provider	
<input type="checkbox"/> In-house developer	
<input type="checkbox"/> Other - provide description	
Software development platform:	
Government agency interested in developing for:	Where an entity is requesting registration as an SBR developer, access to information is available on specific terms and conditions see SBR Conditions of Use and the associated supplements: Copyright , SBR End User Agreement , Disclaimer and Privacy conditions.
Are you planning/considering developing for SBR?	The ATO makes access to controlled information available on specific terms and conditions: Controlled information is information that is not yet available to the general public, but is made available to software developers for the sole purpose of assisting in the development of tax-related software. In some cases the information is in draft form or has been made available for the purposes of consultation, proof of concept work and or pilots. You should not on-forward controlled information to any person or entity outside the entity you are developing for.
<input type="checkbox"/> Yes <input type="checkbox"/> No	
Are you planning/considering developing cloud based software products?	
<input type="checkbox"/> Yes <input type="checkbox"/> No	

Declaration

I declare that:

- I am the applicant identified above
- I am authorised to make this application for and on behalf of the entity identified above
- this application is for access to restricted materials and information to assist in the development of tax-related software
- I and the entity identified above have complied with our obligations under Australian tax laws
- In the last 5 years, neither I nor the entity identified above have been convicted of an offence involving fraud or dishonesty, had the status of an undischarged bankrupt, and
- the information provided in this application is true and correct.

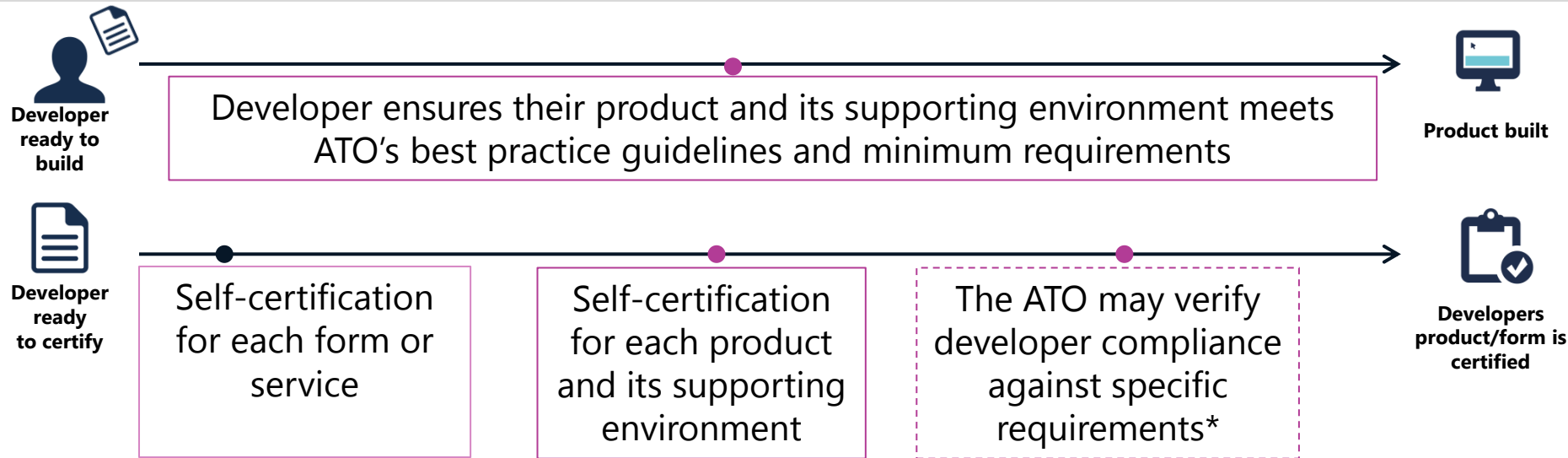
- ① It is an offence under Division 137 of the Criminal Code 1995 (Cth) to give false and misleading information to the Commonwealth.

„Press Submit to make this declaration.

Objective

A registration process that:

- **‘Validates’ the applicant** – Are they who they say they are? Are they authorised to apply on behalf of the developer/provider entity?
- **‘Validates’ the developer/provider** – Are they a registered business? Are they legitimate / genuine?
- **Captures information useful in the monitoring / incident management capability** – post event analysis to determine / resolve weaknesses, proactive / predictive capability based on risk factors
- **Includes relevant / necessary legal requirements** within terms and conditions / user agreements
- **Incorporates suitable rejection, remediation and review processes**
- **Is streamlined / effective / sustainable / reasonable / future-proofed** and compatible with whole of government use



End state overview

- Developers/service providers will refer to best practice guidelines** developed to ensure their product/service meets expected standards (including 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. 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)

The guidelines and requirements are applicable to:

- Commercial third party developers who intend to create software or APIs that interact with ATO systems, including to consume ATO resources or provide submissions to ATO systems.
- Service Providers who provide software or APIs, as described above, to agents, business, individuals or other parties who have transactions with the ATO.

Guidelines

It is **highly recommended** that the following controls are implemented:

- Use the Australian Signals Directorate (ASD) Information Security Manual (ISM) when developing specific controls.
- Where not otherwise specified, use industry best practice with regards to specific technologies and configurations.

Minimum requirements**1. ISO / required standards**

- ISO 27017 and ISO 27018 controls implemented and Privacy Act requirements met.

2. Access Control

- Access control policy and associated procedures required to include user identification, authentication and authorisation.
- SBR Cloud Software Authentication and Authorisation requirements (<http://www.sbr.gov.au/forms/CAA>).

3. Audit Logging

- Keeping logs for staff and clients, reviewing as part of the auditing process and providing to ATO forensics staff if required.

4. Cyber Security Incident Handling

- Documented security incident response plan including informing the ATO **within 24 hours** of any incident which may have resulted in the compromise of data.

5. Data Transfer

- Accepted data format and assurance of delivery and receipt.

6. Encryption

- Use of ASD Approved Cryptographic Protocols and ASD Approved Cryptographic Algorithms (AACAs) .

7. Segmentation and Data Isolation

- Segregation of data within cloud environments from other tenants and clients.

8. Standard Operating Environments and System Maintenance

- Environments to be hardened and a standard operating environment (SOE) applied, which is defined, documented, reviewed, updated and patched regularly.

9. System Backups and Data Recovery

- Backup Policy and Disaster Recovery Plan to be developed to address all data obtained from the ATO including encryption of backup copies.

10. System Integrity Audit

- Security processes including user access rights and administrator accounts are reviewed at least annually, and updated as required

11. Security Awareness and Training

- All staff should be aware of the service provider's security policies and procedures and receive refresher training at least annually.

12. Data Security

- Requirements refer to storage, archiving, retention and destruction of ATO data.

13. Secure Development Practices

- Secure development processes, practices and policies must be followed when developing applications, APIs and other software that interacts with ATO systems in accordance with industry best practice.
- Penetration testing, static and dynamic secure code analysis should be undertaken on applications.

- Are the guidelines reasonable? Is anything missing?
- Are the minimum requirements what you would expect?
- How would you provide evidence of meeting the minimum requirements?
- What kind of verification activity would you expect the ATO to undertake?
- How often would you expect to review your certification?
- Is there anything in the minimum requirements that stands out?

- Industry consultation and feedback – ato.gov.au
- Finalise Framework
- Implement recommendations
- Ongoing communication

Appendix

Background

The Australian Government, and the ATO, 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 development and implementation of the Operational Framework for Developers and Service Providers will focus on the registration and certification processes, as well as incident management and monitoring capabilities.

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 system. 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)
















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: <ul style="list-style-type: none"> 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 a developed software or application as a service. Responsible for: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Secure storage and transfer of information
Intermediary and Tax Professional (e.g. tax agents, BAS agents, bookkeeper, payroll provider)	Assists businesses and individuals 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

 **What do we know now?**

- Developers apply online or via a web form to become registered to access ATO materials
- Two forms collect a range of information but not the same information
- 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
- 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 just 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 is required as part of the application
- Determine what needs to be included in terms and conditions/ user agreements
- Determine the updated registration process – high level
- Determine the trigger points for rejecting a registration

**What are the gaps / issues?**

- Single area to undertake registration and review processes – 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

✓ 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 and certification is against each form (e.g. BAS, CTR etc.), and 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 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 recommended 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?



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 third party 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



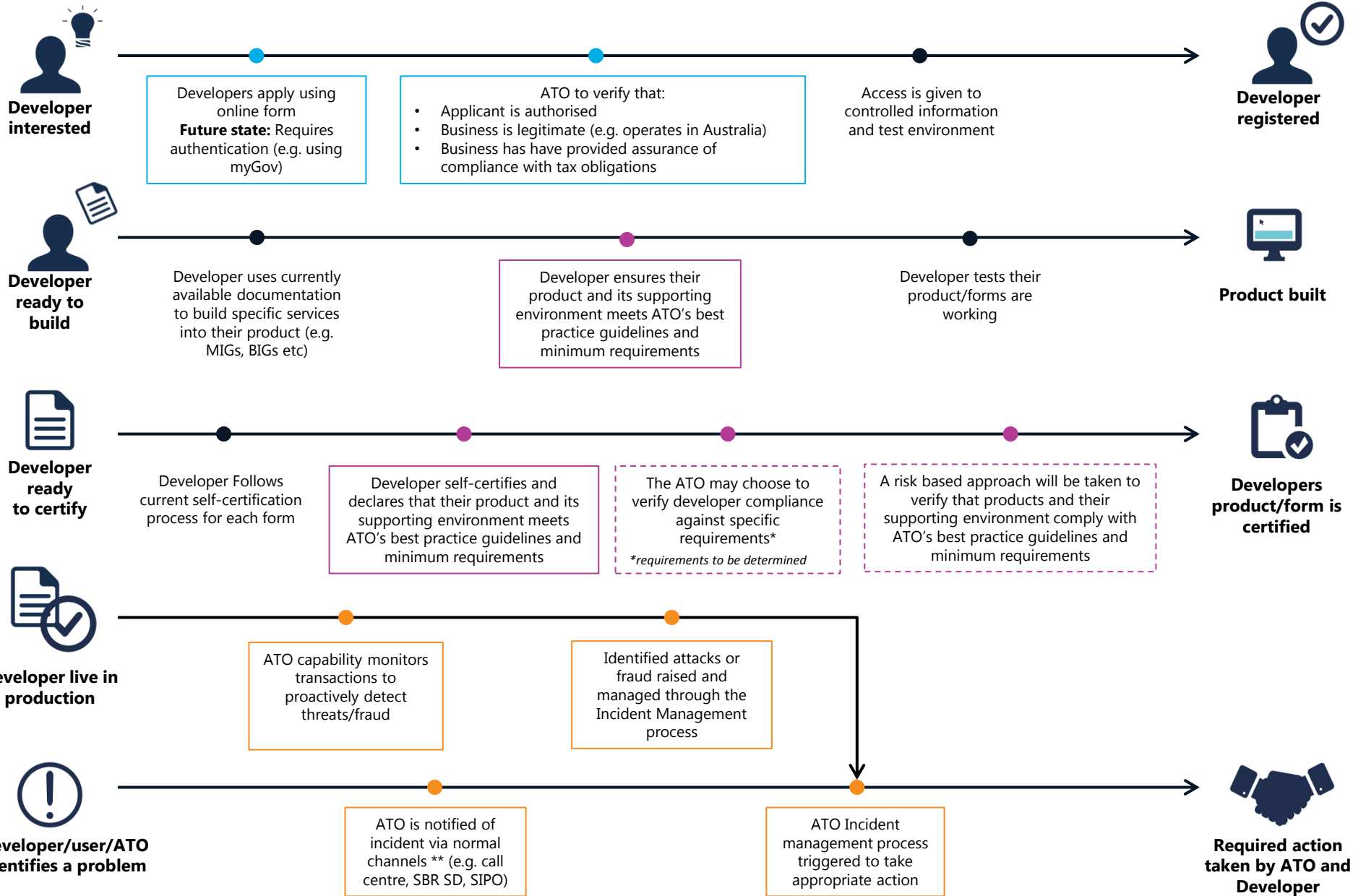
Monitoring capability

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.

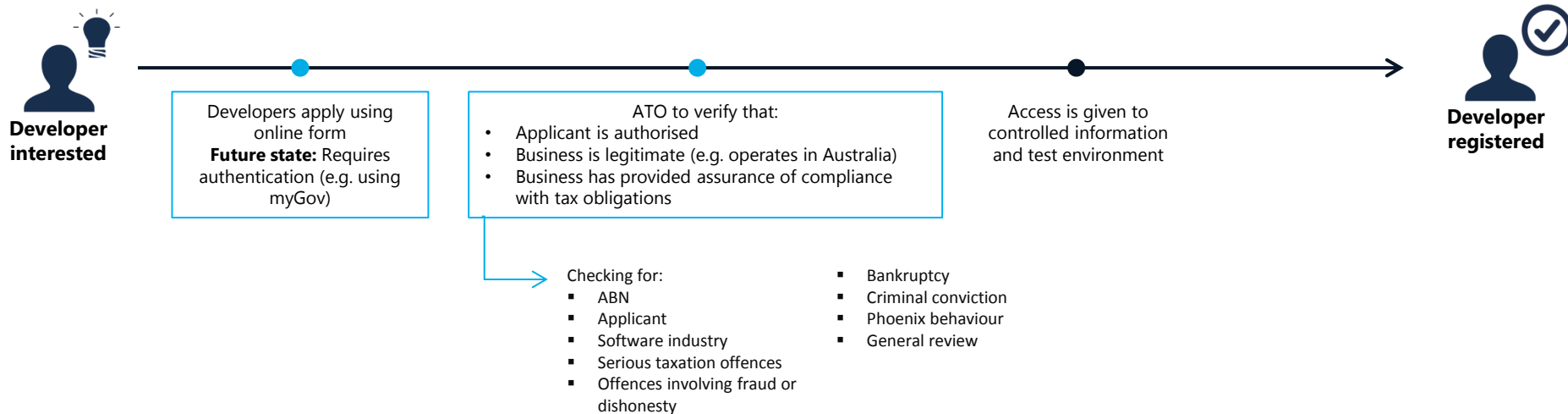
Includes the following:

- ↳ 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.



note incidents may also be raised through other channels



***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 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

Information required for registration

ABN:	What information do you wish to access
Name of entity:	<input type="checkbox"/> Tax Preparation
Trading name:	<input type="checkbox"/> Tax file number
Main business location:	<input type="checkbox"/> Tax time
Applicant details	<input type="checkbox"/> eBMS3 –
Name:	<input type="checkbox"/> Software will be developed principally for use by tax practitioners
Position in entity:	Which segment(s) are you developing for:
Contact number:	<input type="checkbox"/> Superannuation
Email:	<input type="checkbox"/> Tax Preparation
Select the one that applies to you	<input type="checkbox"/> Payroll
<input type="checkbox"/> Software developer	<input type="checkbox"/> Business Accounting
<input type="checkbox"/> Mobile device/App developer	<input type="checkbox"/> Other - provide description
<input type="checkbox"/> Software service provider	
<input type="checkbox"/> In-house developer	
<input type="checkbox"/> Other - provide description	
Software development platform:	Where an entity is requesting registration as an SBR developer, access to information is available on specific terms and conditions see SBR Conditions of Use and the associated supplements: Copyright , SBR End User Agreement , Disclaimer and Privacy conditions.
Government agency interested in developing for:	The ATO makes access to controlled information available on specific terms and conditions: Controlled information is information that is not yet available to the general public, but is made available to software developers for the sole purpose of assisting in the development of tax-related software. In some cases the information is in draft form or has been made available for the purposes of consultation, proof of concept work and or pilots. You should not on-forward controlled information to any person or entity outside the entity you are developing for.
Are you planning/considering developing for SBR?	
<input type="checkbox"/> Yes <input type="checkbox"/> No	
Are you planning/considering developing cloud based software products?	
<input type="checkbox"/> Yes <input type="checkbox"/> No	

Declaration

I declare that:

- I am the applicant identified above
- I am authorised to make this application for and on behalf of the entity identified above
- this application is for access to restricted materials and information to assist in the development of tax-related software
- I and the entity identified above have complied with our obligations under Australian tax laws
- In the last 5 years, neither I nor the entity identified above have been convicted of an offence involving fraud or dishonesty, had the status of an undischarged bankrupt, and
- the information provided in this application is true and correct.

- ① It is an offence under Division 137 of the Criminal Code 1995 (Cth) to give false and misleading information to the Commonwealth.

„Press Submit to make this declaration.

Validation/checking process

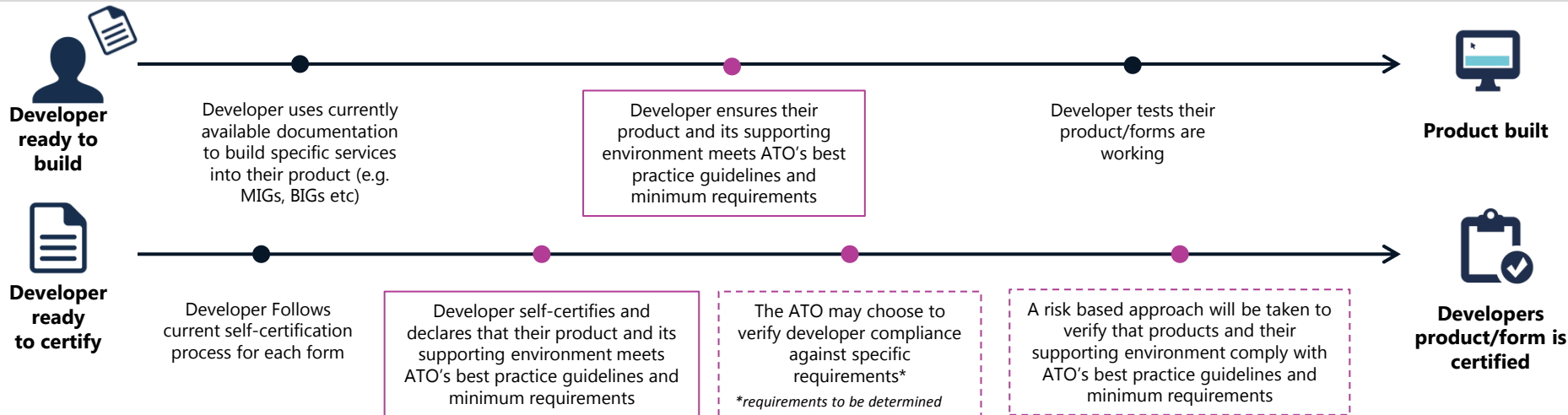
What	Checking for	Outcome
ABN	ABN active	Inactive ABN – refuse registration
Entity head	Check against ABR for Director/partners/Trustee	Incorrect match – refuse registration
Applicant	Check authorised person in ABR	Incorrect match – refuse registration
Software industry	Check ABR ANZSIC code Confirm organisation/entity in software industry or developer working as in-house developer	Risk based as to next step

- Change to existing process – email approving registration to be sent to the applicant with a copy to entity controlling head
- Additional guidelines for validation/will be developed as the process matures

Objective

A registration process that:

- ‘Validates’ the applicant – Are they who they say they are? Are they authorised to apply on behalf of the developer/provider entity?
- ‘Validates’ the developer/provider – Are they a registered business? Are they legitimate / genuine?
- Captures information useful in the monitoring / incident management capability – post event analysis to determine / resolve weaknesses, proactive / predictive capability based on risk factors
- Includes relevant / necessary legal requirements within terms and conditions / user agreements
- Incorporates suitable rejection, remediation and review processes
- Is streamlined / effective / sustainable / reasonable / future-proofed and compatible with whole of government use



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. Perform a risk assessment to determine risks and mitigation strategies to inform the framework and the development of standards/minimum reqs.
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

Medium term

1. Determine a risk based approach to verify developer/SP 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

The guidelines and requirements are applicable to:

- Commercial third party developers who intend to create software or APIs that interact with ATO systems, including to consume ATO resources or provide submissions to ATO systems.
- Service Providers who provide software of APIs, as described above, to agents, business, individuals or other parties who have transactions with the ATO.

Guidelines

It is highly recommended that the following controls are implemented:

- Use the Australian Signals Directorate (ASD) Information Security Manual (ISM) when developing specific controls.
- Where not otherwise specified, use industry best practice with regards to specific technologies and configurations.

Minimum requirements

1. ISO / required standards

- ISO 27017 and ISO 27018 controls implemented and Privacy Act requirements met.

2. Access Control

- Access control policy and associated procedures required to include user identification, authentication and authorisation.
- SBR Cloud Software Authentication and Authorisation requirements (<http://www.sbr.gov.au/forms/CAA>).

3. Audit Logging

- Keeping logs for staff and clients, reviewing as part of the auditing process and providing to ATO forensics staff if required.

4. Cyber Security Incident Handling

- Documented security incident response plan including informing the ATO **within 24 hours** of any incident which may have resulted in the compromise of data.

5. Data Transfer

- Accepted data format and assurance of delivery and receipt.

6. Encryption

- Use of ASD Approved Cryptographic Protocols and ASD Approved Cryptographic Algorithms (AACAs) .

7. Segmentation and Data Isolation

- Segregation of data within cloud environments from other tenants and clients.