Australian Government

Australia's Digital ID System

November 2024

Compliance Referral and Reporting Strategy – 2024-25

System Administrator
Australian Government Digital ID System (AGDIS)

digitalidsystem.gov.au

Contents

1. Document information 2
   1.1 Change history 2
   1.2 Endorsement 2
2. Document purpose and operating context 2
   2.1 Purpose of the strategy 2
   2.2 Operating context 2
3. Compliance model 3
   3.1 Promoting compliance 3
   3.2 Accreditation and annual reviews 3
   3.3 Operational Standards 3
   3.4 Reporting 4
4. Record keeping and referrals 4
   4.1 Recording potential non-compliance 4
   4.2 Written direction to a participating entity 4
   4.3 Referral to the Digital ID Regulator 4
   4.4 Prioritisation and assessment 5
   4.5 Triggering events for referral 5
   4.6 IT System Incident prioritisation matrix and resolution targets 8
5. Effectiveness of strategy 9
6. Relevant documents 9
7. Appendix – Referral matrix 9
   7.1 Fraud and cyber security incidents referral matrix 9
   7.2 Change Enablement regulator referral matrix 12

1. Document information

1.1 Change history

The System Administrator maintains this document in electronic form. It is the responsibility of the user to verify that this copy is the latest revision.

Version	Date Last Revised	Author	Change Description
1	14 November 2024	Jason Oversby	Preliminary Draft

1.2 Endorsement

Version	Endorsed by	Date
1	Jo Hadley – Director, Office of the System Administrator	18 November 2024

2. Document purpose and operating context

2.1 Purpose of the strategy

This document is the Compliance Referral and Reporting Strategy (the strategy) of the System Administrator for the Australian Government Digital ID System (AGDIS). The strategy describes the activities and processes, which collectively enable the System Administrator to promote compliance and refer potential non-compliance matters to the Digital ID Regulator as represented by the Australian Competition & Consumer Commission (ACCC).

The strategy covers accredited entities and participating relying parties (and their respective services) approved by the Digital ID Regulator to participate in the AGDIS. These entities are listed on the AGDIS Register established and maintained by the Digital ID Regulator.

The purpose of this strategy is to:

- ensure accountability, transparency, confidentiality, timeliness, proportionality and fairness in achieving compliance
- assist in the development of processes to facilitate accredited entity and participating relying party compliance with legislation
- support accredited entities and participating relying party compliance
- identify strategies and actions to promote and support compliance and identify opportunities for quality improvement to strengthen the operation of the AGDIS
- identify potential non-compliance, including factors that lead to repeat or systemic issues and refer these matters to the Digital ID Regulator
- identify accredited entities and participating relying party educational needs.

2.2 Operating context

In the context of this strategy, compliance refers to accredited entities and participating relying parties taking actions to meet their respective obligations contained within the *Digital ID Act 2024* (the Act), *Digital ID Rules 2024* (the Rules), *Digital Accreditation Rules 2024* (the Accreditation Rules), *Digital ID Accreditation Data Standards 2024* (the Accreditation Data Standards) Service Levels[1], and Operational Standards in the AGDIS System Administrator Operational Handbook (the Handbook).

[1] Service levels may be set in the future by the Digital ID Data Standards Chair (DSC), in accordance with section 80 of the Act.

The Act, Rules, Accreditation Rules, Accreditation Data Standards and Operational Standards set the requirements for accredited entities. The Digital ID Regulator ensures compliance and may conduct assessments to determine if an accredited entity follows these requirements.

The System Administrator may identify matters of potential non-compliance and exercise its power under section 96 of the Act to refer a participating entity to the Digital ID Regulator to assist them to exercise their powers or perform their functions.

The Digital ID Regulator may also request information from the System Administrator that we hold for the purposes of compliance and enforcement.

3. Compliance model

3.1 Promoting compliance

The System Administrator collaborates with entities participating in the AGDIS. The System Administrator uses a range of initiatives that directly support and encourage adherence to the Act, Rules, Accreditation Rules, Accreditation Data Standards and Operational Standards.

The System Administrator incorporates a range of initiatives which aim to support accredited entities and participating relying parties understand their obligations. The System Administrator undertakes these initiatives throughout the following phases.

During the pre-participation phase, the System Administrator invites all new entities, including existing entities that are adding a new service, to attend a facilitated focus session. These sessions educate entities on the requirements in preparation for participating in the AGDIS once they become approved.

The System Administrator provides the Handbook and the Configuration form, which enables the System Administrator to confirm specific requirements can be met. This informs the application to the Digital ID Regulator for approval to participate in the AGDIS. This process also includes the collection of relevant contacts within the entity and the set-up of ICT accesses to facilitate online reporting and access to services.

3.2 Accreditation and annual reviews

The Act provides a legislative framework for the phased expansion of the AGDIS and establishes an accreditation scheme for Accredited Entities.

The *Digital ID Rules 2024* (the Rules), *Digital Accreditation Rules 2024* (the Accreditation Rules) and *Digital ID (AGDIS) Data Standards 2024* (the AGDIS Data Standards) set out the details of the Accreditation Scheme and the AGDIS. These standards apply consistently across all digital ID services to ensure a fast, safe, and seamless experience for users of digital ID.

To maintain accreditation, accredited entities are required to conduct an annual review and report on certain matters as specified in the Accreditation Rules. The System Administrator assists the Digital ID Regulator by providing data to support the assessment.

An accredited entity can be an attribute service provider, identity service provider, or identity exchange provider.

3.3 Operational Standards

The Handbook describes the Operational Standards necessary to ensure the effective operation of the AGDIS.

Operational performance outcomes for Change Enablement activities and IT System Incidents (ITSI) relating to the Identity Exchange, Identity Services Providers, Attribute Providers, Participating Relying Parties and Relying Parties, are updated and calculated in the AGDIS

Administrator Portal. Availability & Outages are reported to the System Administrator monthly by Accredited Entities.

Monthly and quarterly reports are created and distributed to stakeholders in accordance with Schedule B of the System Administrator's Data Sharing Principles.

3.4 Reporting

The System Administrator produces the following regular reports:

- Fraud and Cyber Security Insights Dashboard/Report
- Operational Standards Report (monthly and quarterly)
- Accredited Entities Compliance Report (quarterly)

These reports provide the System Administrator with an opportunity to monitor adherence to their respective requirements and performance against the Act and the Rules and provide the Digital ID Regulator with a snapshot of activity for compliance assessment.

4. Record keeping and referrals

4.1 Recording potential non-compliance

The System Administrator records all instances of identified potential non-compliance into the Non-Compliance Register. The Non-Compliance Register details information about the instance, including:

- name of the entity and service affected
- the date the matter was identified
- where identified by the System Administrator, the name of the System Administrator Officer and their Director
- where reported by another entity, their name and a contact name and telephone number
- a description of the matter
- a reference to the breached requirements, e.g., the Act, the Rules etc
- any action taken to address the matter.

4.2 Written direction to a participating entity

The System Administrator may issue a written direction to a participating entity under section 130 of the Act to protect the integrity and performance of the AGDIS. Should a participating entity fail to comply with a direction issued by the System Administrator, the matter may be referred to the Digital ID Regulator for assessment.

4.3 Referral to the Digital ID Regulator

Method of referrals

The System Administrator may refer potential non-compliance matters or respond to inquiries from the Digital ID Regulator via email, until the Application Program Interface (API) between both parties is implemented, allowing referrals to occur through the AGDIS Administrator Portal.

Not all matters of potential non-compliance will be referred (such as Medium or Low in section 4.4 of the strategy), as some may be resolved through the System Administrator's engagement with the participating entity and reported to the Digital ID Regulator through routine reporting that occurs on a monthly or quarterly basis.

The information provided to the Digital ID Regulator is specified under section 4 of the System Administrator's Data Sharing Principles.

Notifying a participating entity about a referral

Where a triggering event[2] has been assessed as requiring a referral to the Digital ID Regulator, a written notice may be provided to the entity to advise of the referral. The written notice may also include a written direction under section 130 of the Act to mitigate further harm to the AGDIS or end users. This will be by exception, as the standard process is to refer the matter to the Digital ID Regulator for their assessment.

4.4 Prioritisation and assessment

Referral rating, treatment and timing of referral

The System Administrator will evaluate potential non-compliance triggering events and the potential harm to the AGDIS or end users. The table below outlines the actions the System Administrator may take to address potential non-compliance against the legislative framework.

The System Administrator may undertake educational measures and issue written notices to participating entities to mitigate potential harm to the AGDIS or end users.

Referral Rating	Treatment	Timing of referral
VERY HIGH	Referral to the Digital ID Regulator is certain. This is because an entity may not be or may not consistently be compliant with the Act, Rules, or Standards. Or, because a potential breach of the Act, Rules, or Standards has, or may result in, extreme harm to the AGDIS or individual(s) outlined in the **Critical** priority of the harm descriptor table.	**Immediate**
HIGH	Referral to the Digital ID Regulator is highly likely. This is because an entity may not be or may not frequently be compliant with the Act, Rules, or Standards. Or, because a potential breach of the Act, Rules, or Standards has, or may result in, major harm to the AGDIS or individual(s) outlined in the **Major** priority of the harm descriptor table.	**Within one business day of identification**
MEDIUM	Referral to the Digital ID Regulator will be considered. A review will be undertaken to understand if there is a pattern of continuous potential non-compliance. If a pattern is identified, a referral may be completed, or the System Administrator may issue a written direction to the participating entity. This is because an entity may sometimes be potentially non-compliant with the Act, Rules, or Standards. Or, because a potential breach of the Act, Rules, or Standards has, or may result in, moderate harm to the AGDIS or an individual outlined in **Moderate** priority of the harm descriptor table.	**Within five business days of identification (review completion)**
LOW	Referral to the Digital ID Regulator is unlikely because there may have been a minor breach of the Act, Rules, or Standards, resulting in no harm to the AGDIS or an individual outlined in the **Low** priority of the harm descriptor table. However, if a continuous pattern is identified, this may increase the referral rating.	**Monthly reporting**

4.5 Triggering events for referral

This section describes a non-exhaustive list based on triggering events to identify instances of potential non-compliance with the legislative framework, including those in the Handbook. To determine the likelihood of referral to the Digital ID Regulator, these events are either assessed using the System Administrator's Digital ID Regulator referral matrix and harm descriptor table (section 7 of the strategy) or are core triggers that the System Administrator will immediately refer to the Digital ID Regulator.

[2] A triggering event refers to a specific occurrence or action that initiates a particular response or set of actions by the System Administrator.

Core triggering events for referral

The table below outlines core triggering events that, once identified by the System Administrator, will result in an immediate referral to the Digital ID Regulator without the need for assessment using a referral matrix and harm descriptor table.

Triggers for non-compliance referral	Threshold	Referral Rating
Critical digital ID incidents • A total, or near total, unplanned IT System Outage including a major interruption, or degradation to the availability of the AGDIS (P1/P2 incident detailed in section 4.6). • An IT system incident that also involves any form of a data breach. • Cyber security incident causing immediate threat or substantial potentially disruption to the AGDIS. • A data breach relating to an accredited entity's services. • Digital ID fraud incident within the AGDIS potentially has been caused by a failing of an accredited entity, such as an unauthorised assumed identity at the IP3 or above level. • Onboarding a service without approval by the Digital ID Regulator.	≥ 1 event	VERY HIGH
Interoperability: a participating relying party has not provided individuals with a choice of accredited identity service providers and no exemption exists in accordance with s 79 of the *Digital ID Act 2024*. Note: Currently, there is only one Identity Service Provider (IdP) participating in the AGDIS. This scenario may be relevant when additional IdP join the AGDIS.	≥ 1 event	
Voluntariness: a participating relying party requires an individual to create a digital ID to access a service without providing an alternative in accordance with s 74 of the *Digital ID Act 2024*.	≥ 1 event	
A participating relying party is not collecting or storing a pairwise identifier issued to a relying party to enable the entity to comply with the reportable incident requirements in accordance with 4.2(3)(k) of the *Digital ID Rules 2024*.	≥ 1 event	
Trustmark misuse: An accredited entity is displaying the Australia Digital ID System Accreditation Mark; however, they have not used and displayed a hyperlink to the Digital ID Accredited Entities Register in accordance with rule 5.3(3)(a) of the *Digital ID Rules 2024*.	≥ 1 event	
Significant digital ID incidents • Digital ID fraud incidents involving unauthorised access to sensitive information and incident. • Cyber security incident that includes the use of the digital ID Accreditation Trustmark or 'holding out' conduct. • Cyber security incident where user data has been breached. • Significant material change or other matter notified to the System Administrator that may impact the operation of the AGDIS.	≥ 1 event	HIGH
Notable digital ID Incidents • Minor disruption, interruption, or degradation to the availability of the AGDIS (P3 and P4 incident).	Monthly reporting	LOW

Triggering events for potential referral

The table below details triggering events and scenarios relating to participating entity potential non-compliance. These scenarios have been assessed using a risk matrix and harm descriptor table (section 7 of the strategy) to determine the likelihood of referral to the Digital ID Regulator based on the associated risk to the AGDIS or end users.

Triggers covered in the Digital ID Rules 2024	Threshold	Referral Rating
Trigger: Cyber security incidents and digital ID fraud incidents service level: A participating entity did not meet the notification requirement of *no later than 1 business day* after the entity becomes aware of the incident or a suspected incident in accordance with rule 4.2(4) of the *Digital ID Rules 2024.* **Scenario**: Entity A is approved to participate within the AGDIS. Entity A identifies a potentially fraudulent digital ID proofed to IP2 on 9 January 2025. The entity does not submit the incident to the System Administrator, via the Portal, until 14 January 2025. As Entity A did not meet the notification requirement of within 1 business day as per Rule 4.2(4), the non-compliance referral rating applied to this event is “Medium”. A review will be conducted to determine if there is a pattern of behaviour. If consistent behaviour is identified, this will be referred to the Digital ID Regulator for non-compliance assessment within five business days of identification.	≥ 1 business day	**MEDIUM**
Trigger: A participating entity did not meet the 5 business day change notification requirement for a change to the entity’s IT system that interacts with the AGDIS throughout one monthly reporting cycle. a. Digital ID Rules 2024, rule 4.3(3)–(5) for accredited entity b. Digital ID Rules 2024, rule 3.4, Item 2(a)–(b) for participating relying party. **Scenario**: On 7 October 2024, a Participating Relying Party (PRP), with a large number of users, became aware of a proposed change to their information technology (IT) system that could reasonably have a material effect on the operation of the AGDIS. The proposed change will result in a planned outage of the PRP’s IT system, and degraded performance of the AGDIS. The PRP scheduled the proposed change to take effect on 4 November 2024. On 31 October 2024, the System Administrator was notified by the PRP that their IT system will experience an outage due to their proposed system changes. The PRP was non-compliant as they did not meet the notification requirements of no later than 5 business days after becoming aware of the proposed change detailed in rule 3.4, Item 2(a)–(b) of the Digital ID Rules. The event has been rated as “Major” based on the change enablement harm descriptor table, and the non-compliance referral rating applied to the event is “High”, resulting in the System Administrator referring the PRP to the Digital ID Regulator for non-compliance assessment within one business day of identification.	≥ 5 business days	**HIGH**

4.6 IT System Incident prioritisation matrix and resolution targets

The priority of IT System Incidents (ITSI) and how they are treated depends on the incident priority. This is based on both urgency (how quickly the resolution is needed) and impact (to business, to digital ID users, the AGDIS's reputation, and ministerial and legislative expectations). Impact to the AGDIS is considered, as well as impact to an individual entity. Thus, the priority determined by the System Administrator may be different to the view taken by entities.

System availability will be largely determined using the Availability Monitoring Application. System availability will be verified with Accredited Entities wherever possible.

Circumstances which increase the impact severity may be considered and increase priority regardless of system availability. This could include sensitivities or considerations specific to a Participating Relying Party.

Availability for users	**≤ 100%**	**≤ 95%**	**≤ 75%**	**≤ 25%**
Participating entity service is degraded	4	3	2	1
Participating entity service is not working as intended	4	3	2	1
Participating entity service – critical non-production env is degraded	4	4	4	3
Other factors that may increase priority				
Increased vulnerability for intrusion, abuse or fraud	1			
Legislative commitment or obligation, or ministerial deadline cannot be met	1			
Serious reputational damage to the System	1			
System processing or data causing compromised user privacy or safety	1			
High likelihood of serious non-compliance with accreditation requirements	1			
Apparent non-compliance with accreditation requirements	2			
Risk of serious reputational damage to the System	2			
Participating Relying Parties unable to deliver critical functions	2			

Incident resolution targets and non-compliance referral ratings		
Priority	**Resolution performance target**	**Non-compliance referral rating**
P1 – Critical	Resolved within 4 hours	**1 – Very High**
P2 – High	Resolved within 24 hours	**2 – High**
P3 – Moderate	Resolved within 7 days	**3 – Medium**
P4 – Low	Resolved within 20 days	**4 – Low**

5. Effectiveness of strategy

The strategy will be reviewed annually by the System Administrator, or sooner if necessary to ensure its effectiveness and alignment with developing legislative and policy requirements.

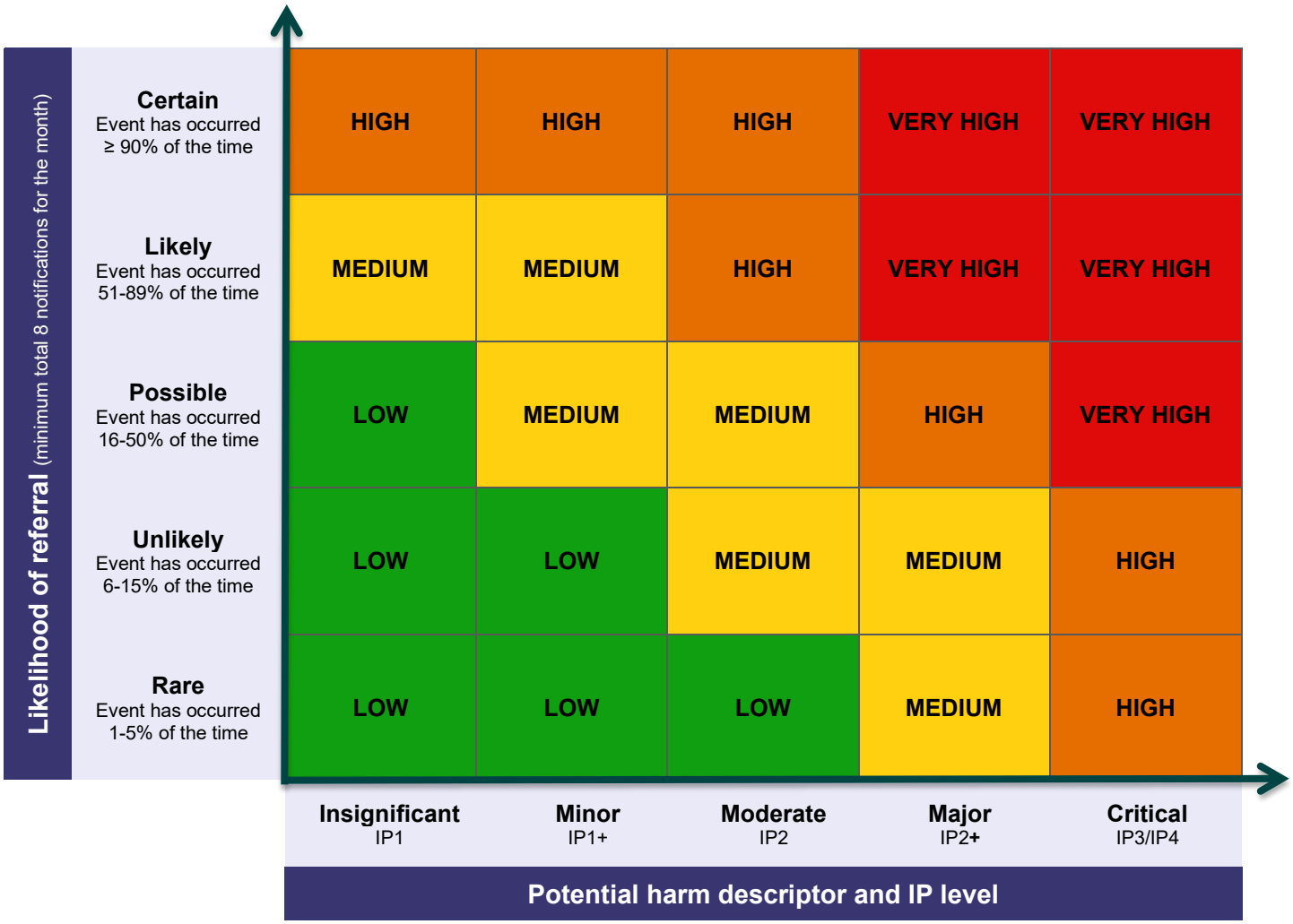
6. Relevant documents

- AGDIS System Administrator Operational Handbook
- Participating entity non-compliance process
- AGDIS System Administrator Data Sharing Principles.

7. Appendix – Referral matrix

7.1 Fraud and cyber security incidents referral matrix

This matrix demonstrates the likelihood of referring a participating entity to the Digital ID Regulator. The matrix relates to fraud and cyber security incidents, that can consider the number of occurrences and the associated harm descriptor rating, including Identity Proofing Levels (IP Levels). It should be read along with the fraud and cyber harm descriptor table that details the potential harm caused to users and/or the AGDIS.



Fraud and cyber harm descriptor table

This table describes the potential harm caused to users and/or the AGDIS resulting from fraud and cyber security incidents associated with an Identity Proofing Level (IP Level).

Identity Proofing (IP) refers to the process of collecting, verifying, and validating sufficient attributes (and supporting evidence) about a specific individual to confirm their identity. IP Level describes the level of assurance or confidence in the Identity Proofing process.

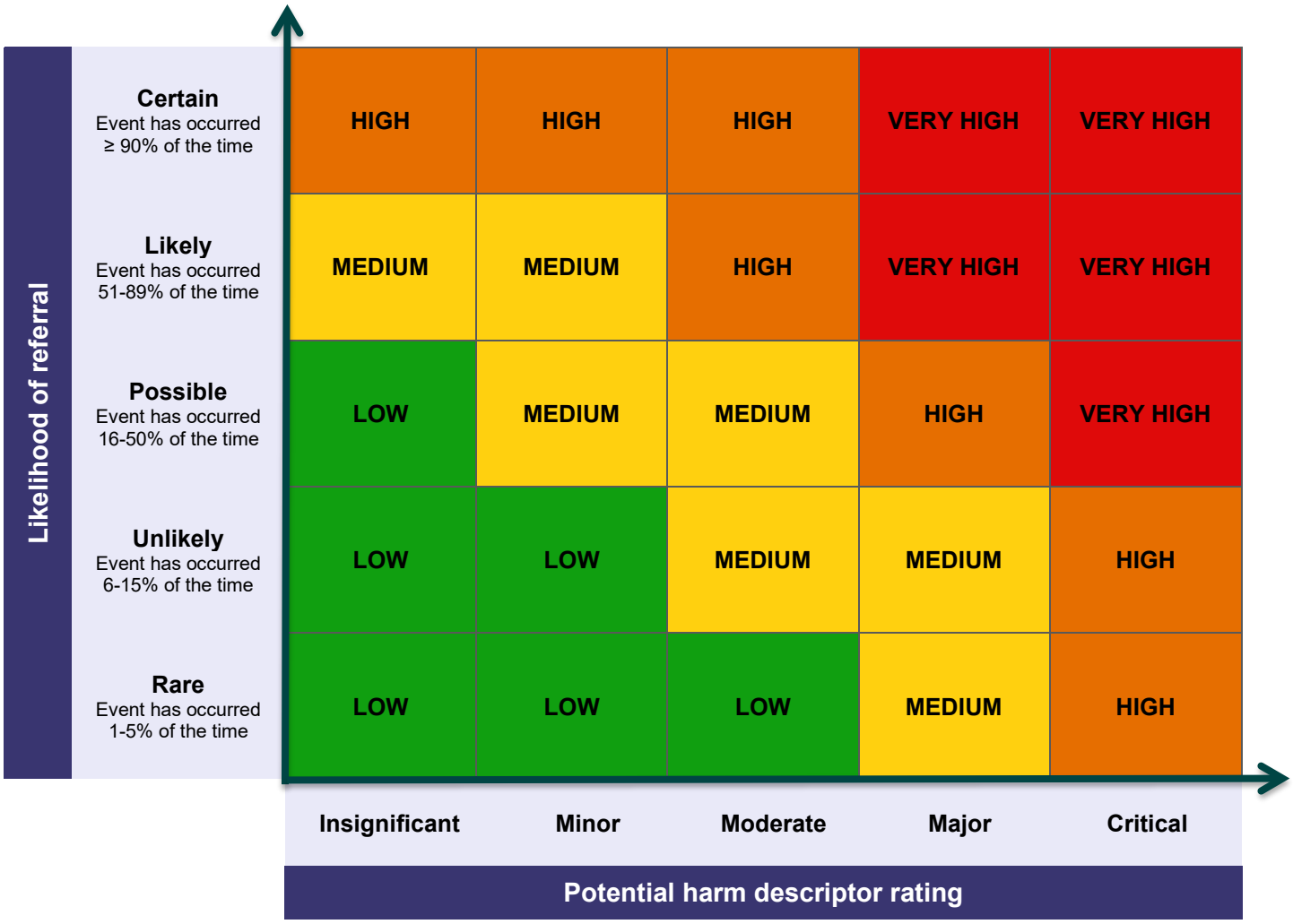
IP Level and Descriptions[3]	Potential Harm Description	Rating
IP4 IP4 is used when a very high level of confidence in the claimed identity is needed. This requires four or more identity documents to verify someone's claim to an existing Identity and the individual claiming an identity must attend an in-person interview as well as meet the requirements of IP3. The intended use of IP4 is for services where the risks of getting Identity verification wrong will have a very high consequences to the individual or the service. For example, the issuance of government-issued documents such as an Australian passport. **IP3** IP3 is used when a high level of confidence in the claimed identity is needed. This requires two or more identity documents to verify someone's claim to an existing Identity and requires biometric verification. The intended use of IP3 is for services where the risks of getting Identity verification wrong will have high consequences to the individual or the service. For example, access to welfare and related government services.	A digital ID proofed to IP3 requires a unique username, email address, phone number, two acceptable ID documents such as Australian driver license, Medicare card, Australian birth certificate or Australian passport. This level includes biometric binding to the Digital ID. A digital ID proofed to IP4 requires the same plus an additional Use in the Community document (total two Use in the Community documents). It also requires biometric binding to the Digital ID. Potential harm caused for IP3 and IP4 could include: • Existing security controls are ineffective, there is an extreme vulnerability for intrusion, abuse, or fraud • Catastrophic reputational impact to the Agency, or one of its customers, service providers or to other Australian Commonwealth and other Australian government entities • Catastrophic increase in media reporting about customer experience issues, complaints or outcomes – leading to significant adverse public perception • Unfavourable publicity continuing for greater than a year • Significant levels of customer and ministerial complaints • Incorrect information or advice or service is being provided to the user or the business through / by the participant service • Incorrect issuance of government-issed documents • Data and system processing and data integrity being compromised.	**Critical**

[3] Source: Digital ID (Accreditation) Rules 2024

IP2+ IP2+ is used when a medium level of confidence in the claimed identity is needed. This requires two or more identity documents to verify someone's claim to an existing identity. The intended use of IP2+ is for services where the risks of getting identity verification wrong will have moderate-high consequences to the individual or the service. For example, undertaking large financial transactions.	A digital ID proofed to IP2+ requires a unique username, email address, phone number, two acceptable ID documents such as Australian driver license, Medicare card, Australian birth certificate or Australian passport. Potential harm caused for IP2+ could include: • Existing security controls are partly effective, there is a major vulnerability for intrusion, abuse, or fraud • Major reputational impact to the Agency, or one of its customers, service providers or to other Australian Commonwealth and other Australian government entities • Significant increase in media reporting about customer experience issues, complaints or outcomes - leading to adverse public perception • Unfavourable publicity continuing for up to a year • High levels of customer and ministerial complaints • Delivery of information, advice or core services to the customer • Existing controls being compromised, with an increased risk of intrusion, abuse or fraud.	**Major**
IP2 IP2 is used when a low-medium level of confidence in the claimed identity is needed. This requires two or more identity documents to verify someone's claim to an existing identity. The intended use of IP2 is for services where the risks of getting identity verification wrong will have moderate consequences to the individual or the service. For example, the provision of utility services. An IP2 is sometimes referred to as a "100-point ID check".	A digital ID proofed to IP2 requires a unique username, email address, phone number; two acceptable ID document, which includes individual given name, middle name (if any), surname, and date of birth as they appear on a document. Potential harm caused for IP2 could include: • Moderate vulnerability for intrusion, abuse, or fraud • Moderate reputational impact to the Agency, or one of its customers, service providers or to other Australian Commonwealth and other Australian government entities • Increase in media reporting about customer experience issues, complaints or outcomes • Unfavourable publicity for up to six months • Increase in complaints and ministerial complaints.	**Moderate**
IP1+ IP1+ is used when a low level of confidence in the claimed identity is needed. This requires one identity document to verify someone's claim to an existing identity. The intended use of IP1+ is for services where the risks of getting identity verification wrong will have minor consequences to the individual or the service.	A digital ID proofed to IP1+ requires a unique username, email address, phone number; an acceptable ID document, which includes individual given name, middle name (if any), surname, and date of birth as they appear on a document. Potential harm caused for IP1+ could include: • Low reputational impact to the Agency, or one of its customers, service providers or to other Australian Commonwealth and other Australian government entities • Low levels of media reporting	**Low**
IP1 IP1 is used when no identity verification is needed or when a very low level of confidence in the claimed identity is needed. This level supports self-asserted identity (I am who I say I am) or pseudonymous identity. The intended use of IP1 is for services where the risks of not undertaking identity verification will have a negligible consequence to the individual or the service. For example, to pay a parking infringement or obtain a fishing licence.	A digital ID proofed to IP1 requires no identity verification, only need one email address or phone number. This level supports self-asserted identity (I am who I say I am).	**Insignifi-cant**

7.2 Change Enablement referral matrix

This matrix demonstrates the likelihood of referring a participating entity to the Digital ID Regulator for non-compliance with the Act, Rules, and Standards. The matrix relates to change enablement activities, that can consider the number of non-compliance occurrences and the associated potential harm descriptor rating. It should be read along with the change enablement harm descriptor table that details the potential harm caused to users and/or the AGDIS.



Change enablement harm descriptor table

This table describes the potential harm caused to users and/or the AGDIS resulting from poor or ineffective management of change enablement activities affecting the AGDIS.

Types of Changes	Potential Harm Description	Rating
• Back-end changes • Change to consume more system features • Change to fix an issue within the system	Potential harm that may be experienced if a change is not managed by adequately notifying the System Administrator could include: • Impacting all other entities and end users of the AGDIS • Exposing a cyber risk to the AGDIS and end users • Exposing end user information • System degradation across the AGDIS due to higher than expected traffic • The wellbeing of external User/s or staff being put at risk • Data and system processing and data integrity being compromised • Core business services not being delivered • Relying Party customer services including benefits, payments, and rebates not occurring, or • Incorrect information or advice or service is being provided to the User or the business through / by the Participant service • A legislative commitment or obligation, or ministerial deadline cannot be met • Existing security controls are ineffective, there is an extreme vulnerability for intrusion, abuse, or fraud • Catastrophic reputational impact to the Agency, or one of its customers, service providers or to other Australian Commonwealth and other Australian government entities • The incident is resulting in an unmanageable volume of calls to the Participant's phone channel support • Material changes to the AGDIS resulting from Change Enablement activities by a participating entity results in services becoming unavailable or significantly and severely degraded.	**Critical**
• Adding a service • Onboarding a participant • Change to display or appearance to improve user experience • Change to introduce the ability to do something new within the system	Potential harm that may be experienced if a change is not managed by adequately notifying the System Administrator could include: • Delivery of Relying Party customer benefits, payments, and rebates • Delivery of information, advice or core services to the customer • Delays or impacts to legislative commitment or obligation, or ministerial deadline • Existing controls being compromised, with an increased risk of intrusion, abuse or fraud • Incident is affecting a large number of users • Significant reputational and financial loss likely • The incident is resulting in a high volume of calls to the Participant's phone channel support • The impacted user is displaying significant unreasonable conduct and aggression • Material changes to the AGDIS resulting from Change Enablement activities by a participating entity results in intermittent system and/or network degradation of service.	**Major**
• Enhancement to existing feature of the system • Offboarding a participant	Potential harm that may be experienced if a change is not managed by adequately notifying the System Administrator could include: • Incident is affecting a small number of users or staff • Moderate reputational impact • The incident is resulting in a low volume of calls to the Participant's phone channel support.	**Moderate**

• System maintenance	Potential harm that may be experienced if a change is not managed by adequately notifying the System Administrator could include: • Incident is affecting a very small number of users or staff • Minor reputational impact • Impacted staff cannot perform a component of their role • Minor fault or component failure which does not impact application or system availability and where a workaround is in place to enable Business as Usual (BAU) activities to continue.	**Low**