Australian Government
Digital Transformation Agency

Risk Management Requirements

Trusted Digital Identity Framework
March 2019, version 1.3

dta

Digital Transformation Agency

Licence

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It's an Honour website (http://www.itsanhonour.gov.au)

Conventions

TDIF documents refenced by this document are denoted in italics. For example, *TDIF: Overview and Glossary* is a reference to the TDIF document titled Overview and Glossary.

The key words "**MUST**", "**MUST NOT**", "**SHOULD**", "**SHOULD NOT**", and "**MAY**" in this document are to be interpreted as described in the current version of the *TDIF: Overview and Glossary.*

Contact us

Digital Transformation Agency is committed to providing web accessible content wherever possible. If you are having difficulties with accessing this document, or have questions or comments regarding this document please email the Director, Digital Identity Policy at identity@dta.gov.au.

Document Management

The TDIF Accreditation Authority has reviewed and endorsed this document for release.

Change log

Version	Date	Author	Description of the changes
0.01	Jul 2016	EY	Initial version.
0.02	Aug 2016	SJP	Content review and update. Released as part of the Trust Framework Alpha suite.
0.03	Jun 2017	SJP	Content review and update. Alignment with AS/NZS ISO 31000:2009 and HB: 167:2006.
0.04	Jul 2017	SJP	Minor updates to align with other Trust Framework documents.
0.05	Sept 2017	SJP	Minor updates to support the public consultation draft.
0.06	Jan 2018	SJP	Incorporates feedback from stakeholders and public consultation and merged the *Core Risk Management Requirements* and *Risk Management Guide* into the one document.
1.0	Feb 2018		Endorsed by the Commonwealth GovPass Authority.
1.1	Oct 2018	SJP	Minor content updates.
1.2	Jan 2019	SJP	Incorporated feedback from stakeholders.
1.3	March 2019	SJP	Incorporated feedback from public consultation.

Contents

1 Introduction

Agencies and organisations that apply to be accredited under the TDIF undergo a series of rigorous evaluations across all aspects of their identity service operations. The *TDIF: Accreditation Process* requires Applicants to demonstrate their identity service is usable, privacy enhancing and is secure and resilient to cyber threats. The intent of these evaluations is to determine whether the Applicant's identity service meets the TDIF Guiding Principles[1] and whether it is suitable to join the identity federation.

This document defines the risk management responsibilities that Applicants are required to implement in order to mitigate credible, likely and realistic risks to their identity service.

The intended audience for this document includes:

- Applicants and Accredited Providers.
- Relying Parties.
- TDIF Accreditation Authority.

[1] See *TDIF: Overview and Glossary* for further information on the TDIF guiding principles.

2 Risk management responsibilities

Risk management is a structured process used to determine the nature of threats, identify vulnerabilities, understand potential consequences of future events and develop an approach to the conduct of activities across an organisation. Robust risk management enables informed, targeted and cost-effective allocation of resources and effort to protect an organisation's people, information assets and infrastructure to support its operations.

Applicants are unique and their approach to managing risk needs to be appropriate and tailored to their business requirements, size, complexity, operating environment and risk profile. Applicants are responsible for appropriately identifying, assessing and managing all likely risks and is therefore best placed to identify:

- Their level of risk tolerance.
- Specific risks to its people, information and assets.
- Appropriate protections to mitigate identified risks.

Objective: Applicants establish and maintain effective risk governance that includes an appropriate internal management structure and oversight arrangements for managing risk.

Applicants **MUST**:

- Implement a risk management framework and supporting processes consistent with an internationally recognised approach[2].
- Annually review their risk management framework and their risk profile to ensure it remains current and is enhanced as required.
- Evaluate the potential sources of risk at *Annex A: potential sources of risk* as part of their risk management process.
- Define their risk appetite and manage risks to an acceptable level. Document and communicate this information to relevant stakeholders, as appropriate.
    - Clearly identify and communicate to stakeholders who in their organisation is responsible for managing each risk.
- Contribute to the management of shared risks across the identity federation, as appropriate.

[2] For example, AS/NZS ISO/IEC 31000:2009, AS/NZS ISO/IEC 27005:2012, etc

- Ensure adequate resources and capabilities to ensure its risk management function operates effectively. This includes:
    - The necessary people, skills, experience and competence.
    - Adequate funding.
    - Processes, methods, and tools for managing risk.
    - Information and systems.
    - Staff training and education.
    - Risk tools and techniques.

2.1 Management requirements of shared risks

Risks may affect one or more participants in the identity federation. Applicants have responsibilities for managing risk beyond their organisational boundaries. Arrangements for addressing shared risks **MUST** be part of their risk management framework. Collaboration will be necessary for shared risks to be managed effectively.

Objective: Applicants consider and implement appropriate risk management strategies, including working with other participants in the identity federation to effectively manage risk. A systematic approach to risk management is critical to successful operation of the identity federation.

Unlike risks that impact a single participant in the identity federation, shared risks cannot be addressed in isolation. Applicants **SHOULD** have an appreciation of the wider risk environment and where risks extend beyond its direct control. They should cooperate to identify and prioritise risks, develop clear accountabilities for their management and commit to collective solutions and outcomes.
For shared risks, the approach taken by Applicants **SHOULD** include:

- Identifying current and emerging risks and other identity federation participants likely to be affected by those risks.
- Analysing and evaluating identified risks in consultation with other affected identity federation participants.
- Implementing appropriate measures to manage the risks.
- Appropriate monitoring and reporting.

Annex A: potential sources of risk

The following table lists potential sources of risk that **MUST** be considered by Applicants as part of their risk management process.

The following questions should be considered for each relevant risk:

- What is the likely outcome of the risk eventuating?
- When and how frequently can the risk happen?
- Where is the risk likely to impact?
- Who could be impacted by the occurrence of the risk event?
- Who are the stakeholders of the risk event? What is the impact on them?
- What catalysts could lead to the risk event?
- How can eventuality of the risk be mitigated?
- How can the consequences of the risk event be mitigated?
- How reliable is the information that this risk assessment is being based on?

Table 11: potential sources of risk

Risk type	Potential sources of risk
Organisational risks.	Supply chain (including using third party or cloud environments). Shared tenancy requirements. Lack of regular security reviews. Inadequate security risk assessment undertaken. Effectiveness of current controls. Failure to comply with the TDIF accreditation requirements. Reputation damage resulting from system or compromise of identity information. Identity fraud. Known or previous cyber security incidents.
Protective security risks.	Physical Security. Building location, type and construction. Inadequate treatment of physical security requirements. Local crime activity. Building setbacks relative to street frontage. Pedestrian traffic. Vehicular traffic. Logical security. Inappropriate storage of ICT and information assets. Use of non-evaluated ICT assets. Use of poor cryptographic key management practices.

Risk type	Potential sources of risk
	ICT asset failures. Relying party ICT asset failures. Malicious code or ransomware infection. Exploitation through security vulnerabilities. Denials of service. Unauthorised access to systems. Data spills. Potential for error (e.g. system error, processing error, internal user error, etc). Source of data and nature of data entry. Extent and nature of system or application change. Network environment and structure. System integration failures. Fire or flood. Location and security of environments used to support the Participant's operations. Poor disaster recovery and business continuity planning. Availability and redundancy of entry points for communications services and essential services. Internet connectivity outages. Long term electricity outages. Personnel security. Personal harm to individuals that use the identity service. Inadequate personnel security checks undertaken. Inadequate security awareness training provided. Abuse of privileges by internal staff or administrators.
Identity risks.	Fraudulent creation of a legitimate identity. Falsified or fraudulent identity documents used during identity verification. Creation of an identity using stolen documents. Falsified or fraudulent use of another's identity. An individual denies verification, claiming it wasn't them. Duplicate identities created for same person by Identity Service Provider. Social engineering on an individual for their identity information. Identity Service Provider unable to verify identity information at source. Unintended disclosure of identity information to third party. Compromise of identity information by Identity Service Provider (trusted insider) or attacker (malicious outsider).
Authentication credential risks.	OAuth 2.0 security considerations (see RFC 6749 for further details). SAML 2.0 security and privacy considerations (see OASIS for further details). Unintended disclosure of authentication credential to third party. Unauthorised duplication or reproduction of authentication credential. Authentication credential compromised through modification or tampering.

Risk type	Potential sources of risk
	Authentication credentials insecure against brute force attacks. Authentication credentials insecure against offline attacks. Cryptographic-based authentication credentials use unsupported algorithms. Inability of Credential Service Provider to suspend or revoke authentication credentials. Incorrect authentication credential suspended or revoked. Inability of Credential Service Provider to recover lost authentication credentials. Inability of Credential Service Provider to renew or issue a replacement authentication credential. Incorrect authentication credential renewed, recovered or replaced. Unauthorised issuance of authentication credentials to third party. Social engineering of individual for their authentication credential. Authentication credentials not unique or not uniquely identifiable.
Authenticated session risks.	Insecure transfer of identity attributes, assertions and credentials between identity federation participants. Inability to measure normal and legitimate authentication behaviours. Inability to detect or report abnormal authentication behaviours. Suspended or revoked authentication credentials are accepted by identity federation participants. Unsupported or insecure cryptographic algorithms or protocols are used to secure information transfers between identity federation participants. Insecure against replay attacks. Insecure against Man-in-the-Middle or man-in-the-Browser attacks.
Downstream.	Individuals obtaining government services or payments that they are not entitled to. Refusal of government services for legitimate claimants.