Australian Government
Digital Transformation Agency

Risk Management Requirements

Trusted Digital Identity Framework
February 2018, version 1.0

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)

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, Trusted Digital Identity Framework at identity@dta.gov.au.

Document Management

This document has been reviewed and endorsed by the following groups.

Endorsement

Group	Endorsement date
Director, Trusted Digital Identity Framework	Jan 2018
Commonwealth GovPass Design Authority	Feb 2018

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

Conventions

The following conventions[1] are used in this document.

- **MUST** – means an absolute requirement of this document.
- **SHOULD** – means there may exist valid reasons to ignore a particular item in this document, but the full implications need to be understood before choosing a different course.
- **MAY** – means truly optional.

[1] These conventions are taken from Request for Comments 2119 (RFC2119) – Keywords for use in RFCs to indicate requirements levels

Contents

1 Introduction

The Digital Transformation Agency (DTA), in collaboration with other government agencies and key private sector bodies, is leading the development of a national federated identity 'eco-system' (the 'identity federation'). Implementation and operation of the identity federation is underpinned by the Trusted Digital Identity Framework (TDIF). This document should be read in conjunction with the *Trust Framework: Overview and Glossary*, which provides a high-level overview of the TDIF including its scope and objectives, the relationship between its various documents and the definition of key terms.

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.

This document includes two parts:

- Part one: defines the risk management responsibilities that Applicants are required to implement in order to mitigate credible, likely and realistic risks to their identity service.
- Part two: sets out an approach to risk management[2] that Applicants can use to meet the requirements specified in Part one.

The intended audience for this document includes:

- Accredited Providers.
- Applicants.
- Authorised Assessors.
- Relying Parties.
- Trust Framework Accreditation Authority.

[2] Provided they meet the requirements listed in part one of this document, Applicants can use alternative risk management approaches if they determine them more suitable for their needs.

2 Part one: Risk management responsibilities

The following risk management responsibilities apply to Applicants.

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.

> Applicants **MUST** 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 (e.g. AS/NZS ISO/IEC 31000:2009, AS/NZS ISO/IEC 27005:2012).
- 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.,
- 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

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.

> **Note:** Risks may affect one or more participants in the identity federation. Applicants **MUST** 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.

3 Part two: A guide to risk management

The risk management process outlined in Figure 1 below combines the systemic risk management approaches of *AS/NZS ISO 31000:2009* and *HB167:2006*. It is a tailored approach that Applicants **MAY** use to mitigate credible, likely and realistic protective security, identity-related, and service delivery risks. Provided they meet the requirements listed in part one of this document, Applicants can use alternative risk management approaches if they determine them more suitable for their needs.

3.1 Benefits of risk management

The benefits of risk management include the following.

- Improved ability to identify, evaluate and manage threats and opportunities.
- Improved accountability and better governance.
- Better management of complex and shared risks.
- Improved financial management.
- Improved organisational performance and resilience.
- Confidence in making difficult decisions.
- Decreased potential for unacceptable or undesirable behaviours such as fraud and harassment.

3.2 Principles of risk management

AS/NZS ISO 31000:2009 identifies the following risk management principles:

- Creates and protects value.
- Is an integral part of the organisation's processes.
- Is part of decision making processes.
- Explicitly addresses uncertainty.
- Is systematic, structured and timely.
- Is based on the best available information.
- Is tailored to the organisation.
- Takes human and cultural factors into account.
- Is transparent and inclusive.
- Is dynamic, iterative and responsive to change.

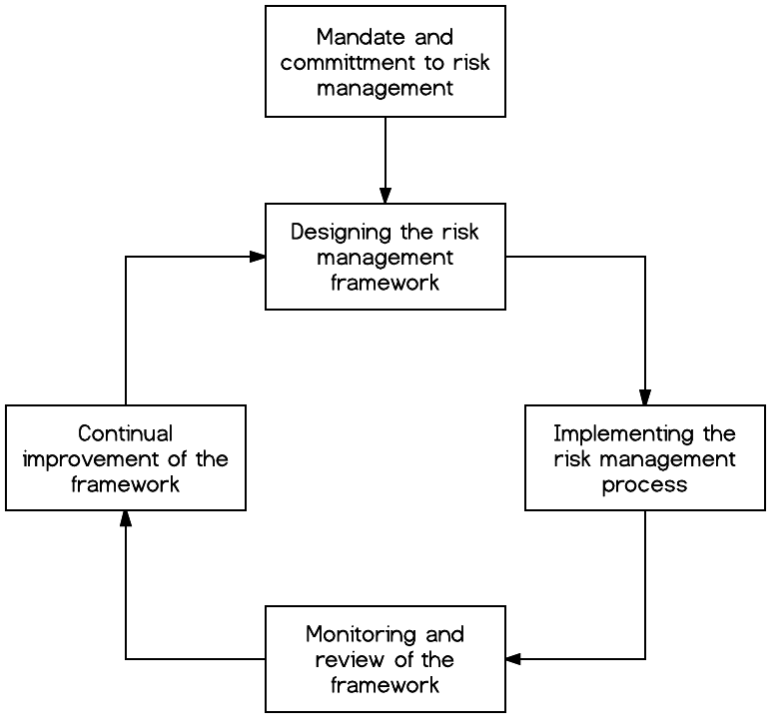
- Facilitates continual improvement of the organisation.

An organisation may choose to enhance their performance in managing risk by adopting the following approaches:

- Continual improvement in risk management and organisational performance.
- Full accountability for risks, controls and risk treatments.
- Application of risk management in all decision making, whatever the level of importance and significance.
- Continual communication and consultation with stakeholders.
- Full integration of risk management in the organisation's governance structure.

3.3 Risk management framework

Figure 1: Risk management framework

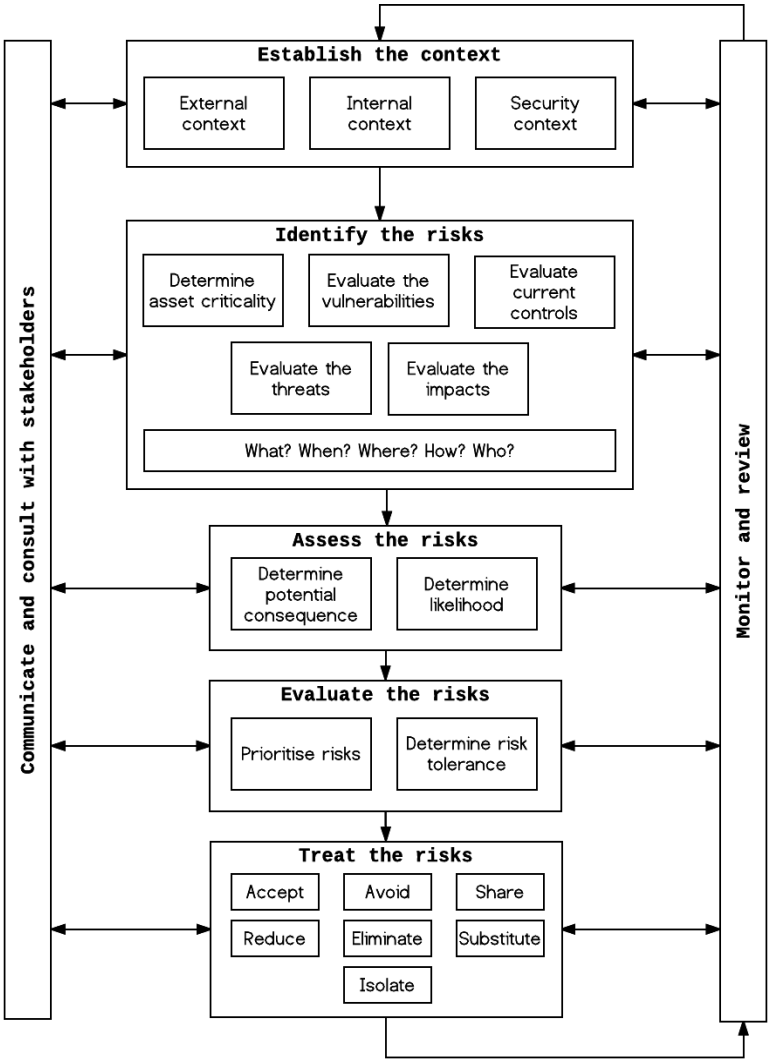


The key elements of the *AS/NZS ISO 31000:2009* risk management framework (Figure 1 above) are as follows:

- **Mandate and commitment** - Organisations require a strong and sustained commitment by management to ensure the ongoing effectiveness of risk management in their environment.
- **Design of framework for managing risk** - Organisations require a systematic approach in designing a risk management framework that is relevant, effective, efficient and adequate. The framework should include:
    - Appropriate risk management strategies, including identifying when to work with others to manage risk.
    - A risk management policy.
    - Effective governance.
    - Communication and reporting arrangements.
    - Resource requirements.
    - Risk management accountabilities.
- **Implementing risk management** - the risk management process is applied at all relevant levels and functions in the organisation as part of its practices and processes. Investment in resources and capabilities enables an organisation to effectively and efficiently apply its risk management activities.
- **Monitoring and review of the framework** - organisations continually ensure that risk management is effective and supports organisational performance. Risk management activities are reviewed annually and enhanced as required.
- **Continually improvement of the framework -** based on the results of monitoring, review and any independent assurance of risk management controls and practices, decisions can be made on how the risk management framework, policy and plan can be improved.

4 Risk management process

Figure 2: Risk management process



The key elements of the *AS/NZS ISO 31000:2009* risk management process (Figure 2 above) are as follows:

- **Establish the context** means understand the organisation's objectives, defining internal and external factors that could be a source of uncertainty, helping identify risk and setting the scope and risk criteria for the remaining risk management process.
- **Risk assessment** includes risk identification, risk analysis and risk evaluation.

- Risk identification determines what, where, when, why and how risks could arise, and the effect this would have on the organisation's ability to achieve its objectives. A range of government and industry resources may be employed to assist in the identification of risks.
- Risk analysis and evaluation determines the risk level against the risk criteria by understanding how quickly a risk can occur, the sources and cause of a risk, the consequences and likelihood of those consequences. Analysis takes into account the effectiveness of existing controls. Risk evaluation compares the level of risk against the risk criteria and considers the need for treatment. The approach to risk evaluation should follow a typical risk assessment process of applying consequence and likelihood matrix. Assessing the risks in relation to each other supports prioritisation and highlights differences. Mitigation strategies can be taken into account to derive the residual risk.

- **Risk treatment** involves assessing and selecting one or more options for modifying risks by changing the consequence or likelihood and implementing selected options through a treatment plan.
- **Communication and consultation** takes place throughout the risk management process with all identified stakeholders to ensure those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made.
- **Monitoring and review** confirms that risk and the effectiveness of control and risk treatments are monitored and reported to ensure that changing context and priorities are managed and emerging risks are identified.

The remainder of this section is dedicated to explaining the risk management process.

4.1 Establish the context

Establishing the context is the starting point to the development of the risk management process. It will identify what the organisation, its objectives, the internal and external environments in which it operates and the reasons why the risk assessment is being developed.

Establishing the context is critical as it sets the basis on which all subsequent risk assessments are conducted. If this step is done poorly it will impact the value of the rest of the process and will lead to an unreliable assessment of risk, and possibly the selection of inappropriate controls.

HB 167:2006 outlines an approach for establishing the context of the risk assessment process and breaks it into three elements:

1. Establishing the external context within which the organisation operates.
2. Establishing the internal context of the organisation.
3. Establishing the security risk management context for the organisation.

4.1.1 External context

This part of the context refers to the external environment in which the organisation operates and may be operating in the near future. The purpose of the external context is to create an agreed understanding of the external factors that may influence the organisation's risk exposure for their identity service or the activities being undertaken to manage them.

The following questions **SHOULD** be considered when establishing the external context:

- How will other participants in the identity federation impact the organisation and its ability manage risks?
- How will the organisation impact other participants in the identity federation and their ability to manage risks?
- Are there any relevant governance or political concerns that could affect how the organisation operations?
    - Is there government instability that may affect the organisation's ability to function fully?
    - What groups may wish to disrupt any function that the organisation has (e.g. crime group or issue motivated group).
- Are there any legislative concerns that may arise due to the organisation's operations?

- What are the relevant legislation, regulations and government policies to be met by the Applicant?
- Has the government affected changes or is likely to implement changes that will in turn affect the Applicant? (e.g. data breach reporting, metadata retention).

- Who are key external stakeholders and what relationship does the organisation have with them?

4.1.2 Internal context

This part of the context refers to the organisation itself. The purpose of the internal context is to create an agreed understanding of the internal environment and issues that may influence the nature of risk exposure to their identity service or the activities being undertaken to manage them.

The following questions **SHOULD** be considered when establishing the internal context:

- What does the organisation use and need in order to maintain their identity service?
  - What resources are used such as people, information and places?
  - What are the governance, structure, roles and accountabilities of the organisation?
  - What are the organisation's decision-making processes?
  - How is the organisational culture? How is the security culture?
  - What standards, guidelines and policies are adopted by the organisation?
- Who are the internal stakeholders and what are their interests?
  - What is the scope and purpose of the risk assessment?
  - Who are the key participants in the risk management process?
  - What are the perceptions or judgements about risk being made by these stakeholders?
  - These perceptions and judgements can vary due to differences in values, needs, assumptions and concerns of the stakeholder.
- What affects the immediate working environment in which the identity service operates?

- What physical, logical and personnel assets used to maintain the identity service?
- What physical, logical and personnel controls are in place to protect the identity service?
- What systems and services are used to support the identity service?
- What information flows occur into, within and out of the identity service?

- What is the nature and extent of contractual relationships?
  - Is any part of the identity service operated by, or outsourced (including sub-contracting) to a third party (including to cloud service providers)

4.1.3 Security context

This part of the context refers to the organisation's security operations. The purpose of the security context is to create an agreed understanding of the organisation's security posture and issues that may influence the nature of risk exposure or the activities being undertaken to manage them.

The following questions **SHOULD** be considered when establishing the security context:

- How could the confidentiality, integrity or availability of the identity service (including identity information or authentication credentials) be affected?
- What would be the consequence to the Applicant if the integrity of identity information collected, stored or processed by the identity service was corrupted?
- How is information compiled. How are data aggregation risks managed[3]?
- What would an unintended disclosure look like?
- What would a data breach look like?
- How will consent be captured, stored and managed?
- How will an individual access services and what is the likely frequency of this occurring?
- What risks will result if the identity binding process fails, or a fraudulent digital identity is created?
- What are the ongoing requirements to collect, store or process identity information?

[3] See *References* for further information on the management of aggregated information

4.2 The risk assessment: risk identification

Security risk events are scenarios where **THREAT** exploits a **VULNERABILITY** to interact with an **ASSET** in a credible, likely and realistic way. This step is used to determine applicable sources of risk and potential events that could impact an organisation which requires them to:

- Evaluate assets and determine their criticality.
- Evaluate the vulnerabilities to their identity service, including the effectiveness of current controls.
- Evaluate threat actors and the consequence of their actions.
- Identify potential risks (as a result of evaluating assets, current controls, vulnerabilities, threat actors and the consequence of their actions).

4.2.1 Asset criticality

The Australian Signals Directorate Information Security Manual defines an asset as:

"Anything of value such as ICT equipment, software and information"

The following table provides a list of non-exhaustive assets to be protected.

Table 1: assets to be protected

Assets to be protected		
Hardware Security Module passphrases (if used).	Database passphrases.	Network infrastructure.
Communications systems.	Perimeter security devices.	Backup systems.
Power supplies.	ICT and information assets.	Identity information and authentication credentials of end users.
Transaction histories.	Backup and archived information.	Operational documents.
Backup and data transfer procedures.	Logical access controls.	TDIF accreditation policies & criteria.
Audit logs.	Internal system user logon credentials.	

The following table provides a list of definitions which could be used to determine the criticality rating of assets needed to support the operation of an identity service.

Table 2: asset criticality rating matrix

	Impact on organisation	**Impact on groups (e.g. stakeholders/community)**	**Impact on individuals (e.g. employees, system users)**
	Loss of asset results in:		
Extreme	Complete cessation of all functions. No short-term recovery capability. Serious prolonged reputation loss (extending for many months). Financial loss > 30% operating budget.	• Severe prolonged loss of amenity (extending several months). • Severe community outrage at loss of service. • Extreme financial distress (e.g. loss of 30% revenue potential of business).	• Catastrophic safety incidents (multiple serious casualties, fatalities). • Long term major financial loss (e.g. loss of employment).
High	Complete cessation of one or more key functions. No short-term recovery capability. Serious prolonged reputation loss (extending for weeks to months). Financial loss > 10% operating budget.	• Severe prolonged loss of amenity (extending weeks). • Community outrage at loss of service. • >10% of revenue potential of business.	• Multiple serious safety incidents (serious casualties, or a fatality). • Mid to long term financial loss (e.g. prolonged stand down of employment over several months).
Significant	Cessation of one or more key functions. Limited short-term recovery capability. Reputational loss on specific operations (extending for weeks to months). Financial loss > 5% operating budget.	• Loss of amenity (extending to days to weeks). • Community upset at loss of service. • >5% of revenue potential of business.	• Major safety incident (multiple injuries requiring medical attention). • Financial losses extending over several weeks (e.g. contracts put on hold).

	Impact on organisation	Impact on groups (e.g. stakeholders/community)	Impact on individuals (e.g. employees, system users)
Moderate	Reduced effectiveness of one or more key functions. Short term recovery capability is possible. Financial loss > 2% of operating budget.	• Partial or temporary loss of amenity (days). • Community disquiet at loss of service. • >2% revenue potential of business.	• Safety incidents requiring first aid treatment. • Long term major financial loss (e.g. loss of employment).
Low	Little impact on functions. Recovery is possible immediately. Little measurable reputational loss. Financial loss <2% of operating budget.	• Little loss of amenity. • Little negative reaction arising from loss of service. • <2% revenue potential of business.	• Insignificant safety implications. • No appreciable financial loss.

4.2.2 Evaluate the vulnerabilities

Vulnerabilities need to be continually assessed to ensure they are being appropriately managed. The following provides a non-exhaustive list of the types of vulnerabilities that could be considered.

- **Physical** - physical storage of and handling of identity information is vulnerable to a multitude of attacks including loss and theft.
- **People** - individuals that manage the identity service are vulnerable to social engineering attacks (e.g. phishing) and also through a lack of security training and awareness.
- **Technical** - organisations are vulnerable to technical attacks on the systems used to provision the identity service. Vulnerabilities exist in technical systems due to poor development, design and implementation of systems and software and through failures to keep systems and applications patched and up to date. Systems should be tested for vulnerabilities on a regular basis to ensure that security measures continue to appropriately treat existing and emerging vulnerabilities.

- **Documentation** - poor documentation or procedures for the use and provision of an identity service will leave an organisation vulnerable to attacks on the identity information it collects, stores, processes or manages.

4.2.3 Effectiveness of current controls

AS/NZS ISO 31000:2009 describes a control as:

"A measure that is modifying risk - controls include any process, policy, device, practice or other actions which modify risk. Controls may not always exert the intended or assumed modifying effect"

Vulnerabilities exist where controls are easily defeated, for example because they have not been tested prior to implementation, are implemented poorly, or have not been tested after their operating environment has materially changed.

The effectiveness of the current controls **SHOULD** be assessed. The following table provides a non-exhaustive list of controls to be considered when defining a list of current controls.

Table 3: common controls

Common controls		
Legislation	Network and logical access controls	Policies, operating procedures, guidelines and standards
System logging	Encryption	Checklists and templates
Awareness training	Audits, reviews, investigations	Physical access controls
Organisational culture	Values and behaviours, code of conduct	Personnel access controls
Employee screening	Security roles and responsibilities	Intrusion detection and prevention controls
Denial of service controls	Intruder alarm systems	ASD's Essential Eight[4]

[4] See *References* for further information on the ASD's Essential Eight.

Controls influence how a risk is rated. A risk may be rated too high or too low based on how a control is viewed, its effectiveness or its absence. Understanding the control environment is an important part of the risk management process.

Common issues with controls are:

- Defects.
- They deteriorate over time.
- There is uncertainty regarding the assumptions made when the control was designed.
- Changes in the environment in which the control operates.

Other considerations may include:

- Currency of the control.
- Test schedule of the control.
- Last time the control was tested.
- Has the control been modified from its intended purpose.

The effectiveness of current controls **SHOULD** include information on:

- The control's ability to deter an attack.
- The control's ability to detect an attack.
- The control's ability to delay an attack.
- The control's ability to respond to an attack.
- The degree to which the control can recover from attack.

4.2.4 Vulnerability matrix

The following table provides a list of definitions that **SHOULD** be used to determine the vulnerability level of current controls.

Table 4: vulnerability level of current controls

Vulnerability level	Assessment criteria
Very high or extreme	Controls are non-existent, critical and urgent improvements have been identified. It is almost certain that controls will be compromised or fail. There is recent evidence of widespread control failures. There are no contingencies in place, severe disruptions to business are likely.
High	Controls are largely ineffective, significant areas for improvement are identified. There is an increasingly likely probability of the controls being compromised. There is recent evidence of a significant number of controls being compromised. Few contingencies are in place and significant disruptions to the business are expected.
Moderate	The majority of controls are functioning, but a number of areas for improvement are identified. There is a moderate probability of the controls being compromised. There is recent evidence of a small number of controls being compromised. Contingencies are in place for only a few key areas of the business to manage potential disruptions.
Low	Controls are effective, but small improvements could be made. There is a low probability of the controls being compromised in the future. There are no recent examples of controls being compromised. Adequacy of controls is assessed on a regular basis (i.e. annually). Contingencies are in place for key areas of the business to manage potential disruptions to the business.
Very Low	Controls are optimum and are sustainable. There is an extremely low probability of the controls being compromised in the future. There are no previous incidents of the controls being compromised. Adequacy of the controls is assessed on a regular and frequent basis. Comprehensive contingencies are in place to manage most potential disruptions to the business.

The following table is an example of how the effectiveness of current control information could be displayed.

Table 5: effectiveness of current controls example

Control Number: 1 | Control: encryption					
Ability to:	Deter	Detect	Delay	Respond	Recover
	X		X		
Last evaluation: 1/1/2018 - testing successful Next evaluation: 1/1/2019					
Modified since implemented: No					
Vulnerability rating: Low					
Required action: Nil					

4.2.5 Evaluate the threats

Understanding the nature of the likely threat and consequence is an essential component of the risk management process.

The threat concept:

Threat = Intent (Desire + Expectation of Success) + Capability (Resources + Knowledge), where:

- **Intent**: is the degree to which the threat source has demonstrated its role, aims, or purpose to cause harm
  - Desire is an agenda, active history, current activities or interest to cause harm.
  - Expectation of Success is the threat actor's perception of its own ability to overcome existing security controls.
- **Capability**: is defined as a combination of resources and knowledge. It encompasses the adequacy of the structure, size, organisation, modus operandi, disposition and finances of the threat source as well as the opportunities available to it.
  - Resources that are available to the threat actor (including time or opportunity).

Knowledge of the threat actor.

When considering the threats to an identity service, Applicant **SHOULD** be aware that individuals or organisations that have the intent and capability to attack the service may choose to do so. Threat actors will seek to make use of lost, stolen, intercepted or hijacked identity information or authentication credentials to gain unauthorised access to systems, identity information or relying party services. Likely threat sources **SHOULD** be considered. The following provides a non-exhaustive list of the types of threat sources to be taken into account.

- Trusted insiders.
- Members of the public.
- Maverick individuals.
- Organised crime syndicates.
- Issues motivated groups.
- State sponsored actors.
- Acts of terrorism (lone wolves and terrorist groups).

4.2.6 Evaluate the impacts

The compromise of an identity service could potentially impact one or more of the following:

- Attribute Providers.
- Credential Service Providers.
- Identity Exchanges.
- Identity Service Providers.
- Individuals.
- Relying Parties.
- The broader identity federation.

The impact of a compromise needs to be clearly understood by all those affected. The following provides a non-exhaustive list of the types of consequence that **SHOULD** be considered if an identity service is compromised:

- **Loss of service availability:** a compromise of the identity service could lead to a loss of access to services for an individual or many users of the system.
- **Loss of information integrity:** an attacker may seek to maliciously change information that is collected, stored or processed by the identity service.

- **Individual loss of identity information:** a compromise of the identity service could lead to a loss, unintended disclosure or compromise of an individual's identity information.
- **Significant loss of identity information:** This can occur if a successful attack at compromising identity information of an individual can be repeated many times.
- **Individual financial loss**: a compromise of the identity service could lead to a compromise of an individual's financial information or their financial wellbeing if, for example, the individual uses the identity service to authenticate to government taxation services.
- **Significant financial loss:** This can occur if a successful attack against one financial transaction can be automated or repeated many times.
- **Reputation damage:** Any successful attack even if relatively insignificant in itself can result in a loss of confidence in the Applicant and the broader identity federation.

4.2.7 Potential sources of risk

A list of potential sources of risk to be evaluated by the Applicant is located in *Annex A: potential sources of risk*. The following **SHOULD** be considered for each 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?

To fully understand the potential of the risks identified, a clear understanding of the vulnerabilities that are apparent from each risk event **SHOULD** be developed. This is to gauge the consequence and likelihood of these risk events and to inform the risk assessment. This process will also help in the prioritisation of the identified risks, and guide the allocation of resources in mitigating their impacts.

4.3 The risk assessment: risk analysis

The level of risk is determined once the range of relevant risks has been identified. To achieve this, the potential consequences of the risk event, the likelihood of occurring, and the acceptable levels of tolerance are evaluated.

The sources of risk events, and the effectiveness of existing controls are considered in assessing the likelihood and consequence levels. This includes the level of oversight and control the Applicant has on the management of shared risks.

See *HB167:2006* for further information on assessing risk.

4.3.1 Determine potential consequences

Consequence considers what **the most likely outcome** of a risk event might be. This is **not the best or worst-case scenario**. The following table lists the potential consequences.

Table 6: potential consequences

	Minimal	Minor	Moderate	Major	Severe	Catastrophic
People	Injuries requiring first aid treatment with little or no impact on organisational performance.	Moderate injuries with limited impact on organisational performance.	Serious injuries resulting in the reduction of business performance and ability to achieve outcomes.	Extensive injuries, possibility of deaths, resulting in reduction of organisational performance and ability to achieve business outcomes.	Multiple deaths and injuries impacting on organisational performance and ability to achieve business outcomes.	Mass fatalities or casualties sufficient to stop the organisation from achieving its business outcomes.
Assets	Damage to assets resulting in inconvenience but no impact on achievement of organisational objectives.	Damage to assets resulting in manageable delays in achieving organisational objectives.	Damage to assets impacting on delivery of organisational outcomes.	Destruction or damage of physical assets or infrastructure causing significant impact on the delivery or organisational outcomes.	Destruction or damage to physical assets or infrastructure sufficient to prevent delivery of organisational outcomes for a protracted period.	Destruction or damage to physical assets or infrastructure which prevent the organisation's continued operation.

	Minimal	Minor	Moderate	Major	Severe	Catastrophic
Information (organisation or identity)	Negligible loss or compromise of organisational information. No impact on routine business. (e.g. no instances of identity compromised)	Limited loss or compromise of organisational information. Limited impact on routine business. e.g. no instances of identity compromised	Loss or compromise of organisational or identity information that reduces the organisations ability to achieve it outcomes. e.g. single instance of identity compromised	Loss or compromise of organisational or identity information that significantly impacts an individual or on the organisation achieving its business outcomes. e.g. few instances of identity compromised	Loss or compromise of significant amounts of organisational or identity information resulting in the inability for impacted persons operating in the community, or the organisation from achieving its business outcomes for a protracted period. e.g. majority of identities compromised	Loss or compromise of significant amounts of organisational or identity information resulting in the permanent loss of impacted persons operating in the community or the organisation from achieving its business outcomes. e.g. all identities compromised
Capability	No effect on capability. Impacts handled within local resources.	Limited effect on capability to carry out an organisational function.	Damage reducing but not denying availability of an organisational function.	Partial loss of or damage to, a capability for which alternative solutions are readily available.	Substantial loss or damage to a key capability which cannot be replaced for a protracted period.	Loss of key operational capability sufficient to disrupt the organisation's ability to deliver outcomes for a protracted period.
Reputation	Limited impact involving minor local issues. Freedom to operate unimpaired. Handled with local resources.	Local impact only. Freedom to operate unimpaired. Handled with local resources.	Internal inquiry required. Short term adverse media attention handled by existing business practice.	Persistent national concern requiring external independent scrutiny or protracted internal inquiry. Special arrangement required to manage impacts.	Loss of confidence in the organisation or identity federation affecting access to organisational or personal information or assets of business partners. Special arrangements required to manage impacts.	Significant damage to the organisation, and/or identity federation with international confidence in the Government diminished. Special arrangements required to manage impacts.

4.3.2 Determine likelihood

Likelihood is the chance or probability of an event or incident occurring which results in the unintended disclosure or compromise of either identity information or authentication credentials. Consideration is given to the timeframe in which the risk could potentially occur. The following table lists the likelihood ratings and descriptions.

Table 7: likelihood ratings

Likelihood rating	Description
Extreme	Credible specific information indicates a current intention, capability and planning to conduct action against an Applicant. Action is almost certain. Could happen within days to weeks.
High	Credible information indicates a current intention and capability to conduct action against an Applicant. Action is assessed as likely. Could happen within weeks to months.
Medium	Credible information indicates an Applicant is a potential target of threat vectors with an intention and capability to undertake action. Action is assessed as feasible and could well occur. Could occur within about a year.
Low	Credible information indicates an Applicant is a possible target of treat vectors who have either limited intent or limited capability or both. Action is assessed as possible, but is not expected. Could happen within the next several years.
Negligible	There is no indication of any threat to an Applicant. Action is assessed as very unlikely. Almost impossible even in the long term.

4.3.3 Security risk event 5x6 event matrix

Determining the risk rating (or level or risk) is the sum of combining the defined likelihood and consequence estimations. The risk rating is between the level of ‘Low’ through to ‘Extreme’. It is appropriate, when rating risk to use the most credible scenario to determine the overall level. The following table shows the risk rating matrix.

Table 8: security risk event matrix

Threat Likelihood	Consequence					
	Minimal	Minor	Moderate	Major	Severe	Catastrophic
Extreme	Moderate	Moderate	Moderate	High	Extreme	Extreme
High	Low	Moderate	Moderate	High	High	Extreme
Medium	Low	Moderate	Moderate	High	High	Extreme
Low	Low	Low	Moderate	Moderate	Moderate	High
Negligible	Low	Low	Low	Moderate	Moderate	Moderate

4.3.4 The risk assessment: risk evaluation

Evaluating risks involves considering risks in the context of the organisation's risk tolerance and potential treatment options.

Risk evaluation involves two stages:

1. Utilising the tolerance level of risks to accept risks that are below that agreed threshold.
2. Prioritising remaining/unacceptable risks into an agreed priority list for treatment.

4.3.5 Risk tolerance

Determining the risk tolerance will be highly dependent on the organisation's external, internal and security contexts. The organisation's risk tolerance is based on the principle of managing risk to a level that is as low as reasonably practicable, while still allowing scope for flexible and innovative business practices.

The organisation's tolerance can be affected by certain changing evaluation criteria and therefore their risk appetite can vary depending on:

- Strategic or business priorities.
- Prevailing political and community sensitivities and expectations.
- Existing or emerging security incident trends (e.g. cyber-attacks, trusted insider).
- Assets and their criticality.

- Vulnerabilities.
- The effectiveness of current controls.
- Resources available for treatment.
- The ability of the organisation to absorb losses or face reputation loss.

4.3.6 Prioritise risks

Prioritisation is achieved through the establishment of risk tolerance and the use of risk rating descriptors (i.e. 'Low' through to 'Extreme'). To aid in the prioritisation process, a risk rating matrix is added which is shown in the table below. As an example, a risk with a medium likelihood and minor consequence is rated as MODERATE (18). Likewise, a risk with a low likelihood and major consequence is also rated as MODERATE (90). Given this second risk has a higher rating, it will likely require prioritisation over the first risk. Using metrics can aid in prioritisation.

Table 9: risk prioritisation example

Threat Likelihood	Consequence					
	Minimal (1)	Minor (3)	Moderate (10)	Major (30)	Severe (50)	Catastrophic (100)
Extreme (10)	Moderate (10)	Moderate (30)	Moderate (100)	High (300)	Extreme (500)	Extreme (1000)
High (8)	Low (8)	Moderate (24)	Moderate (80)	High (240)	High (400)	Extreme (800)
Medium (6)	Low (6)	Moderate (18)	Moderate (60)	High (180)	High (300)	Extreme (600)
Low (3)	Low (3)	Low (9)	Moderate (30)	Moderate (90)	Moderate (150)	High (300)
Negligible (1)	Low (1)	Low (3)	Low (10)	Moderate (30)	Moderate (50)	Moderate (100)

There may be circumstances where the factors for consideration and judgements required are so complex that evaluating the risk is incalculable. If the risk is determined as incalculable, it will not be possible to manage it.

For further information on evaluating risk, see *HB167:2006*.

4.3.7 Risk register

The outcomes of the risk assessment process **SHOULD** be documented in the form of a risk register or risk narrative. At a minimum the following information should be documented:

- A description of the risk event,
- Asset(s) at risk.
- Asset criticality.
- Threat source.
- Risk likelihood.
- Risk consequence.
- Risk rating.

Examples of risk registers and a risk narrative are documented in Annex B: example risk register and risk narrative.

4.4 Risk treatment

Security is not absolute. Efforts to treat risks will not remove them completely but should aim to make the risk levels more tolerable. When selecting risk treatments, the allocation of resources **SHOULD** be proportional to the determined risk rating level.

HB167:2006 outlines a process for treating risk. This includes:

1. Prioritise unacceptable risks.
2. Establish treatment objectives.
3. Identify and develop treatment options.
4. Evaluate treatment options.
5. Detailed design of treatment options.
6. Review of treatment's design.
7. Communicate and implement treatment options.

4.4.1 Prioritise unacceptable risks

Risks assessed as unacceptable are treated to ensure that appropriate controls are applied to reduce either the likelihood of risk being realised or the consequence of it should it happen.

4.4.2 Establish treatment objectives

The objectives of the risk treatments focus on the purpose of the treatment, rather than the treatments themselves. An example of a treatment objective could be where possible, to shift intolerable risks into a tolerable zone through the application of treatments.

> **Note:** Risk treatment options may affect more than one risk.

4.4.3 Identify and develop treatment options

Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived. A number of treatment options can be considered and applied either individually or in combination. It will likely be of benefit to adopt a combination of treatment options.

Broadly speaking, options for the treatment of risk will involve one or a combination of the following treatment strategies. The following table is derived from *HB167:2006*

Table 10: risk treatment options

Treatment Option	Risk Treatment Description
Accept the risk	Although the risk is unacceptable, resourcing and capability is not available to treat the risk. The only option may be to retain the risk and to continue monitoring it until change allows action to be taken.
Avoid the risk	Where practicable, avoid specific activities. (e.g. transferring identity information in an insecure manner should be avoided).

Treatment Option	Risk Treatment Description
Share the risk	Use a third-party stakeholder to provide resources and capability where applicable to reduce likelihood or consequence of a risk (some degree of responsibility and all accountability will remain with the Risk Owner).
Reduce the risk	Implement new controls to remove vulnerabilities. This could include asset hardening or improving the response and recovery efforts (e.g. requiring all internal system users to login with multi-factor authentication).
Eliminate the risk	Where possible remove the source of the threat.
Substitute the risk	Employ a different process (e.g. allow people to use over-the-counter and telephone services to complete identity verification if they struggle to complete checks digitally).
Isolate the risk	Disperse the assets or place the asset within controls where it cannot be compromised.
Engineering controls	Introduce physical or technical protection systems or improve the level of preventative or reactive maintenance to current systems.
Administrative controls	Implement instructions, policy, procedures, training and data collection systems. (e.g. undertake regular risk assessments).

4.4.4 Treatment options

Evaluate treatment options for each identified risk. Risks assessed as acceptable may still require some level of treatment and the treatments themselves are required to meet minimum security standards.

4.4.5 Detailed design of treatment options

Once an appropriate treatment has been selected, a detailed design of that treatment is necessary before implementation to ensure that the treatment is well planned, tested and rolled out. The best way to achieve this goal is to involve the key stakeholders that will be involved in the implementation or end use.

4.4.6 Review of the treatment's design

Prior to beginning the treatment, the detailed design is required to meet the treatment objectives. The process of this evaluation may be a simple checking procedure or a more complex and formal one involving key stakeholders. At a minimum the review **SHOULD** include the following:

- Meet the requirements outlined in the Trust Framework: Protective Security Requirements,
- Be able to be practically implemented in the current environment with available resources and/or anticipated operating environments.
- Provide for sustainability or maintenance for the required lifespan of the treatment.
- Allow required monitoring to be practically undertaken.
- Not introduce new residual risk.

4.4.7 Communicate and implement treatment options

When selecting risk treatment options, the values, perceptions of stakeholders and the most appropriate ways to communicate with them **SHOULD** be considered. When risk treatment options can impact on risk elsewhere in the organisation or identity federation, stakeholders should be involved in any decision-making process. Though equally effective, some risk treatment options can be more acceptable to some stakeholders than others.

Decision makers and other stakeholders **SHOULD** be aware of the nature and extent of the residual risk after risk treatment. The residual risk **SHOULD** be documented and subject to monitoring, annual review and, where appropriate, further treatment.

4.4.8 Information and resources

This is the stage of the risk management process where risk events have been identified and mitigations have been considered that lower the rating to an acceptable level. Mitigations need to be employed and monitored to ensure they are treating the risk event as intended.

A risk treatment plan and risk action plan detail the treatments used for managing risk events. Examples of a risk treatment plan and risk action plan are documented in *Annex B: example risk register and risk narrative*.

> **Note:**
> The information contained in the risk treatment plan and risk action plan may already be incorporated as part of the Risk Narrative or Risk Register. It does not matter where the following details are captured, as long as stakeholders are aware of the risks and how they've been assessed, endorsed and monitored.

4.5 Communication and consultation

Effective communication and consultation through the risk management process will ensure that those responsible for implementing risk management and those with a stake in the process understand the basis on which risk management decisions are made.

A communication plan **SHOULD** be established at an early stage of the risk assessment to determine how the process will be communicated to key stakeholders (internal and external). At a minimum, the plan **SHOULD** answer the following questions at a minimum:

- What the objectives of the Risk Assessment?
- Who requires certain pieces of information in order to contribute effectively?
- Who are the key stakeholders?
- How and when should the stakeholders communicate and be communicated with?
- What are the timeframes for the plan?
- What resources are available to the stakeholders?

It is the responsibility of the organisation conducting the risk assessment to communicate any identified risk that could potentially impact on the operation or business of other participants in the identity federation.

Where the information has multiple stakeholders, the relevant risks and associated treatments are to be communicated to inform those stakeholders of the likely impacts.

Stakeholders perceptions of risk will vary in accordance with their different assumptions and needs. It is important that these different perceptions are appropriately factored into the risk assessment process.

4.6 Monitoring and review

For risk management processes and practices to remain relevant and effective they need to be adaptable to, and evolve with, changes in their internal and external environments, and stakeholder's perceptions and actions.

The following questions **SHOULD** be asked when monitoring and reviewing risks:

- Are the controls and their implementation effective in minimising risks?
- How might improvements be made and measured?
- Are the controls efficient and comparatively cost effective?
- Are the assumptions made about the internal and external environment, technology and resources still valid? Are better solutions available, now or in the near future?
- Do the controls still comply with the TDIF protective security requirements?

4.6.1 Documenting the risk assessment and risk treatment

Applicant **SHOULD** document that they have considered, calculated and accepted (or otherwise manage) the relevant risks to their identity service.

5 References

The following information sources have been used in developing this document.

1. Anderson, M. Fergus, N. Gibson, C. Kilgour, G. Love, D. Parsons, & Tarrant, M,2006,'Security risk management handbook, (HB 167:2006)', Standards Australia & New Zealand, Sydney & Wellington
2. Attorney General's Department, 2016, 'Management of aggregated information (policy advice), Australian Government, Canberra. https://www.protectivesecurity.gov.au/informationsecurity/Documents/Policy-Advice-Management-of-aggregated-information.pdf
3. Australian Signals Directorate, 2017, '2017 Australian Government Information Security Manual: Controls (ISM)', Australian Government, Canberra. https://www.asd.gov.au/infosec/ism/
4. Australian Signals Directorate, 2017, 'Essential Eight Explained', Australian Government, Canberra. https://asd.gov.au/publications/protect/essential-eight-explained.htm
5. Bradner, S. 1997, 'Key words for use in RFCs to Indicate Requirements Level' (Requests for Comment 2119), Internet Engineering Task Force, Switzerland. https://tools.ietf.org/html/rfc2119
6. Committee IT-012 Information Technology Security Techniques, 2012, 'information technology - security techniques - information security risk management (AS/NZS ISO/IEC 27005:2012)', Standards Australia & New Zealand, Sydney & Wellington
7. Department of Finance, 2016, 'Implementing the Commonwealth RIsk Management Policy - Guidance. Resource Management Guide 211', Australian Government, Canberra. https://www.finance.gov.au/comcover/risk-management/the-commonwealth-risk-management-policy/
8. Joint Technical Committee, 2009, 'Risk management - principles and guidelines (AS/NZS ISO/IEC 31000:2009)', Standards Australia & New Zealand, Sydney & Wellington

Annex A: potential sources of risk

5.1 Organisational and protective security sources of risks

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

The following **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. 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.

Risk type	Potential sources of risk
	Logical Security Inappropriate storage of ICT and information assets. Use of non-evaluated ICT assets. 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	Falsified identity documents used during identity verification. 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	Unintended disclosure of authentication credential to third party. Unauthorised duplication or reproduction of authentication credential. Authentication credential compromised through modification or tampering. Authentication credentials insecure against brute force attacks.

Risk type	Potential sources of risk
	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.

6 Annex B: example risk register and risk narrative

The following table is an example of a risk register with seven fields that captures all the key information gathered during the risk identification stage.

Table 12: risk register example

Risk event	Asset at risk	Assets criticality	Threat source	Threat likelihood	Threat Consequence	Risk rating

The following table is an example of a risk register with ten fields that captures all the key information gathered during the risk management process.

Table 13: risk register example

Risk event	Asset at risk[5]	Asset criticality	Risk source[6]	Risk likelihood	Risk consequence	Risk event rating	Treatment	Risk event rating after treatment	Prioritisation

The following table is an example of a risk event narrative with a number of fields that captures all the key information gathered during the risk management process. It combines and expands on the information gathered in the above risk registers.

[5] Expressed as either Information, People, Asset, Capability or Reputation

6 Expressed as either Trusted Insider, Criminal Elements, Protest and Issue Motivated Groups, Maverick Individual, State Sponsored Actor or Terrorism

Table 14: risk event narrative example

Risk Event No:	**Threat Source**:	**Asset Category**:
Description of risk (risk event)		
Security risk assessment		
	With current controls	**Post treatment**
Risk event likelihood		
Risk event consequence		
Risk event rating		
Vulnerability Assessment		
Identified vulnerabilities		
Current Control	**Control**	**Assessment of Control Effectiveness**
Additional comments or observations		