Australian Government

Industry Data Classification Framework

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Technology Security Policy Branch
Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

Acknowledgement

The Department of Home Affairs acknowledges CSIRO's Data61 for their expertise and collaborative work in the development of the IDCF.

Disclaimer

The Department of Home Affairs has developed the Industry Data Classification Framework (IDCF) as comprehensive industry guidance material for information purposes. However, the publication and distribution of the IDCF including on the Department's webpage does not constitute an endorsement or approval for specific circumstances. Users are required to make their own determination as to the appropriate use of the information provided in the IDCF.

The material in this IDCF is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. As for any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

To the full extent permitted by law, the Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in the IDCF.

Any third-party views or recommendations included in this guide do not necessarily reflect the views of the Commonwealth, its endorsement or indicate its commitment to a particular course of action.

Contents

1.
Overview of the Industry Data Classification Framework

The Industry Data Classification Framework (IDCF) provides a foundation for consistent data management and sharing across industry. It is designed to help organisations understand the value of their data and classify it using the Data Security Levels (DSL), ensuring the level of protection is communicated clearly and consistently.

The IDCF includes four modules:

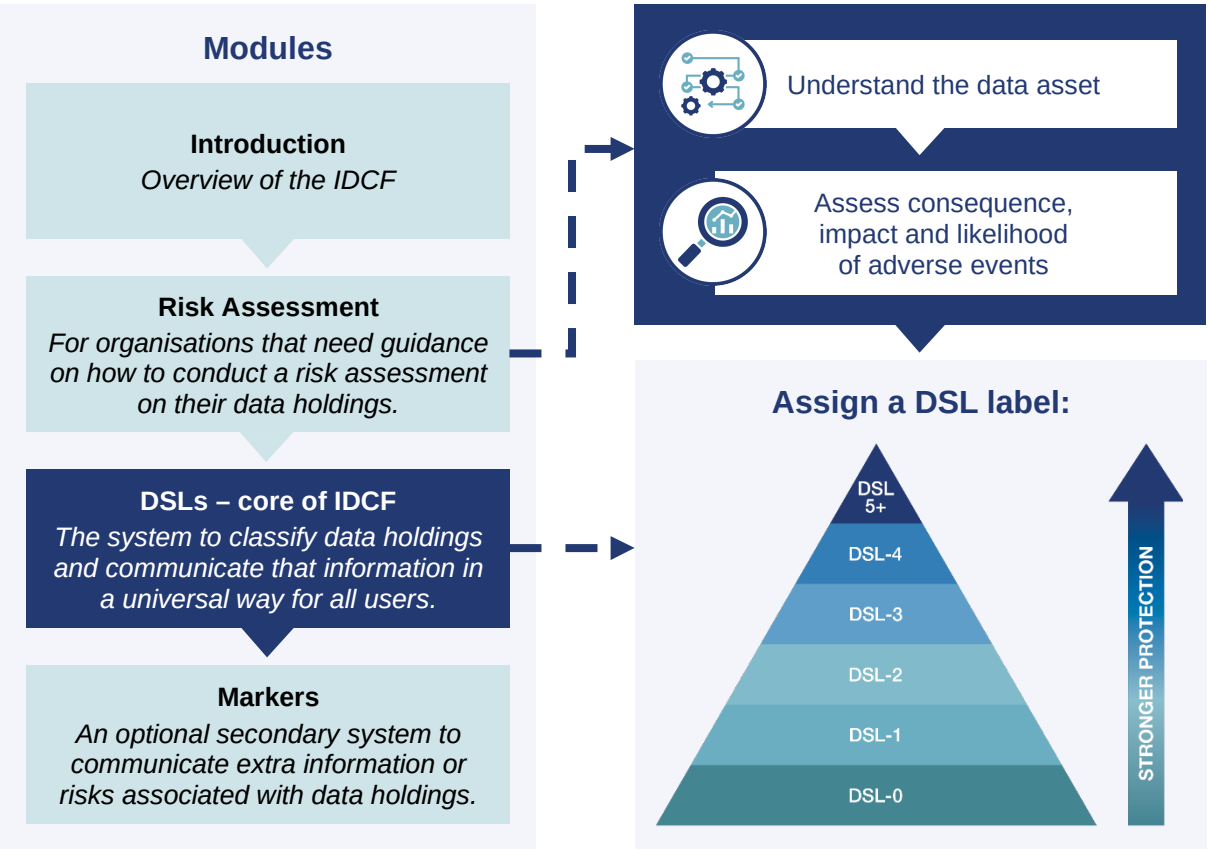

Figure 1: An overview of the IDCF

2. Introduction to the IDCF

This section introduces the Industry Data Classification Framework (IDCF) and provides an overview of the modules and key terms. It outlines expectations and obligations when using the IDCF, including a code of conduct.

2.1. Overview

The IDCF provides a foundation for consistent data management and sharing, both within organisations and between them. It is designed to help organisations understand the value of their data and communicate the level of protection it needs in a consistent and unified way. The IDCF uses six distinct labels, known as the Data Security Levels (DSLs), to communicate the required protection level and handling instructions for the data based on the data owner's risk appetite.

It is designed to be used in the context of data risk assessment and classification of electronic data, computer systems and devices that carry data electronically. While the IDCF focuses on electronic systems, it can be used on other objects that contain data such as printed copies.

The framework is modular, providing guidance on data risk assessment and data classification as described in the Introduction: Data risk management and the IDCF. This design allows organisations to adopt individual modules as needed, enabling flexible integration based on existing practices and maturity levels.

Adopting the entire IDCF (all four modules) is not necessary to gain its benefits. However, DSL classification is a prerequisite to be identified as using the IDCF.

For more information on DSLs, please see the DSL module.

2.1.1. Purpose of the IDCF

The IDCF has been developed as part of an Australian Government commitment in the *2023-2030 Australian Cyber Security Strategy*. The aim of the framework is to:

- provide guidance to industry on how to identify, assess, classify and communicate the value of their data holdings
- support industry to handle their data in a consistent way by providing a common classification language
- enable organisations to assess risk associated with their data and apply controls to reduce risk from adverse events
- enable organisations to consider and manage confidentiality, integrity and availability requirements of the data
- draw from existing classification systems, including the Protective Security Policy Framework (PSPF) which applies to Australian Government non-corporate Commonwealth entities, to promote common approaches to data risk management.

For more information about how to use the IDCF, please see the Introduction: Using the IDCF.

2.1.2. Data risk management and the IDCF

Data risk management is the process of identifying, assessing and mitigating threats to an organisation's data to protect it from adverse events.

A data risk assessment and classification process typically consists of an organisation:

- understanding the data it holds
- assessing the inherent risk of the data by considering potential consequences, impact and the likelihood of adverse events
- determining the protection needed to reduce the data risk, communicating that requirement using DSL labels, and ensuring the data is stored in systems appropriate to the protection required.

The IDCF provides resources and guidance for organisations at various stages of the data risk management process. It provides further resources to assist organisations with limited experience or expertise in data risk management or for those who are renewing current practices.

Organisations can use their own existing data risk assessment processes when they adopt the IDCF. For these organisations, the IDCF provides a common language, the DSL labels, that can be used when engaging with other organisations.

The use of DSLs is the core feature of the IDCF as they provide the common language for communicating risk and protection requirements for data.

Figure 2 illustrates the risk assessment and data classification process used in the IDCF.

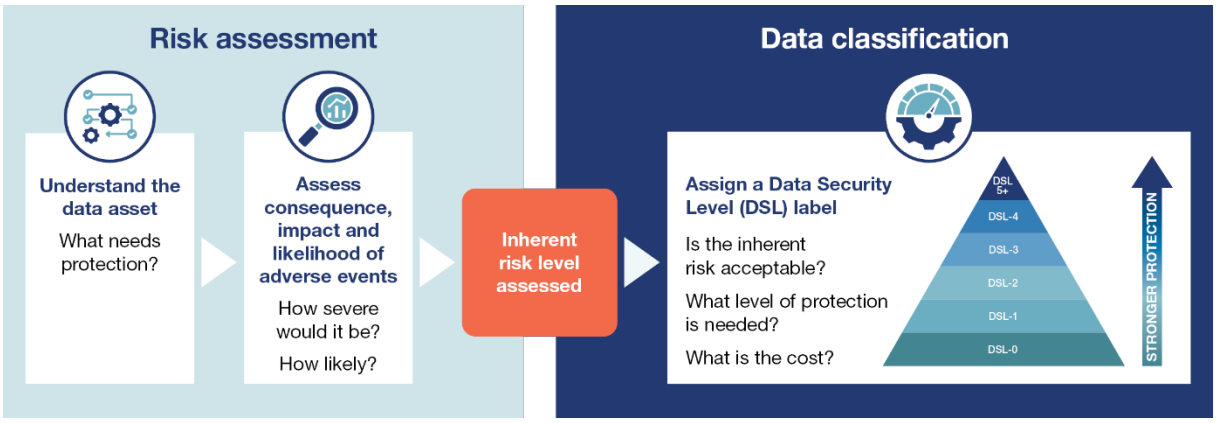

Figure 2: Data risk assessment and classification process in the IDCF

For more information on the risk assessment process, please see the Risk Assessment module.

2.1.3. Modules

The IDCF is organised into four modules, which focus on the process outlined in the previous subsection:

1. Introduction

Provides an overview *of the framework and modules, including the code of conduct.*

2. Risk Assessment

Provides guidance on how to conduct a risk assessment on data held by an organisation. This is aimed at users with limited experience or expertise in data risk assessment.

3. Data Security Levels (DSL)

Provides a system to classify data holdings and communicate that information in a universal way for all users. This is the core feature of the IDCF.

4. Markers

Provides an optional secondary *system to communicate extra information or risks associated with data holdings within an organisation.*

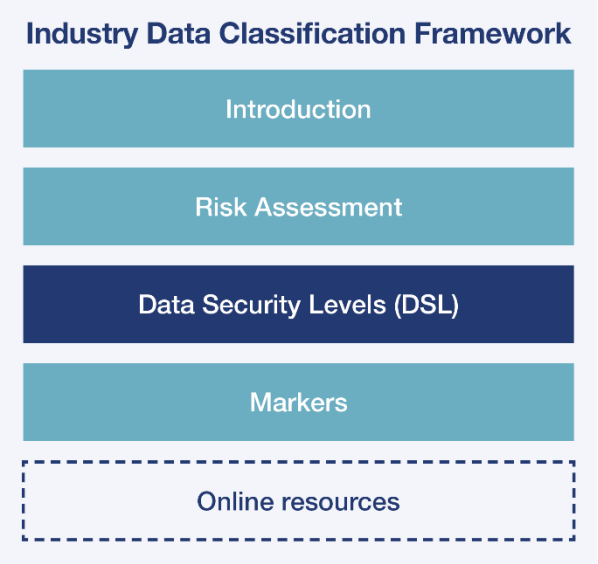

Figure 3: Provides an overview of the IDCF

For more IDCF resources, please see the IDCF website.

Risk assessment module

Data risk assessment involves identifying potential adverse events and the consequences of those events on organisations and individuals. In the IDCF, risk assessments can be used to determine the appropriate DSL to apply to a particular dataset. This module provides general guidance on how to conduct a risk assessment to determine the data's inherent risk. Once the potential impact is understood, the appropriate DSL can be determined and organisations can apply a DSL label to communicate the level of protection needed to relevant parties.

The module is an additional resource designed for users with limited experience or expertise in data risk assessment. Organisations with existing risk assessments and/or policy that determines the inherent risk in data might choose to continue using their own processes.

For more information on risk assessment, please see the Risk Assessment module.

DSL module

The DSLs communicate the level of protection and security needed for the data, as determined by the data owner. This determines which types of computer systems and devices are suitable for handling that data. Data is assigned one DSL label to indicate the level of protection the data needs.

There are six DSLs; DSL-0, DSL-1, DSL-2, DSL-3, DSL-4 and DSL-5+. Lower-level classifications, like DSL-0 and DSL-1, are for data that has low sensitivity or value and where an adverse event would have a low impact on individuals or the broader community. DSL-2 and DSL-3 will be used by most organisations for typical everyday data. DSL-3 may be preferred by organisations with a low tolerance for risk or when dealing with sensitive data where an adverse event would have moderate impact. DSL-4 and DSL-5+ are for data that needs significant security controls.

For more information on DSLs, please see the DSL module.

Markers module

Markers are an optional, secondary level of classification (additional to the DSL classification) that communicate specific areas of risk such as privacy or confidentiality. They can also describe dissemination restrictions and who is allowed to see the data, such as only the executive team within an organisation.

There are three categories of markers used in the IDCF: *integrated markers*, which are defined by the IDCF, *adopted markers,* which are defined and published by another organisation, and *user-defined markers* for internal use or with other organisations by agreement. Unlike DSL labels, multiple markers may be applied to data or a document.

For more information on markers, please see the Markers module.

Additional resources

Additional resources, including guides for small and medium-sized enterprises (SMEs), are available on the IDCF website.

For more IDCF resources, please see the IDCF website.

2.1.4. Key terms

The IDCF includes key terms, some of which are commonly used. A list of additional relevant key terms is also included in each module.

Table 1: Defines key terms used throughout the IDCF

Key term	Definition
Adverse event	An accidental or malicious event with a negative consequence that compromises the confidentiality, integrity and availability of data. A data breach is one type of adverse event. This is based on the definition in NIST SP 800-61r3.
Availability	Timely and reliable access to data.
Classification	The process of placing data in a class. In the IDCF, this means applying a data security level (DSL) label and optionally applying markers based on a risk assessment.
Classified data	Data classified with a DSL. In the IDCF, this term does not mean data that has a government security classification.
Confidentiality	Preserving authorised restrictions on data access and disclosure, including means for protecting personal privacy and proprietary information. This is based on the NIST definition.
Consequence	The outcomes of an event. For example, identity theft might be a consequence of a loss of personal information.
Data breach	The unauthorised movement or disclosure of sensitive private or business information, including personal information under the *Privacy Act 1988* (Cth). For more information see ASD's glossary and information on data breaches.
Data owner	The individual or organisation that owns or originally collected, curated, generated or classified the data.
Data recipient	The individual or organisation that receives data from a data owner.

Key term	Definition
Event	An action, occurrence or change involving data that may cause an impact.
Event likelihood	The chance or probability, expressed qualitatively, of an event resulting in an adverse event.
Impact	The level of harm expected to result from the consequence(s).
Industry	A collective term for many organisations operating in a common area of the economy and for all organisations together. For example, the health industry or Australian industry.
Inherent risk	The risk of an event before security controls have been implemented.
Integrity	A property whereby data has not been modified in an unauthorised manner since it was created, transmitted or stored. This is based on the NIST definition.
Label	A visible indicator in physical or electronic form applied to data to communicate its DSL classification.
Marker	A visible indicator in physical or electronic form, applied to data to communicate a secondary classification, such as specific handling, sensitivity or dissemination requirements.
Metadata	The information that describes the characteristics of data, such as its structure, for example data format, syntax, semantics, or its content, for example type of data, date or location of collection. This is based on the NIST definition.
Organisation	An entity. This includes a business, company, association, sole trader, partnership or government, for example Corporate Commonwealth Entities and State and Territory to the extent they can use the IDCF.
Security	When unqualified (no description of the type of security, for example 'national' security), it is an abbreviation for protective security as defined above.

For a full list of terminology and definitions, please see Appendix A: Glossary.

2.2. Using the IDCF

The IDCF is modular, providing guidance on data risk assessment and data classification as described in subsection 1.1.2. This design allows organisations to adopt individual modules as needed, enabling flexible integration based on existing practices and maturity levels.

Of the IDCF's four modules, the DSL module provides the core features. This module links system protection to the level of security the data requires. Once DSL labels have been applied, the organisation is deemed to be using the IDCF and adhering to the code of conduct (refer to the Introduction: Code of conduct). Not all DSLs and markers are relevant to all organisations, allowing organisations to decide which DSLs and markers should be used in their operations or data sharing agreements.

Some organisations with limited experience or expertise in data risk management may adopt all IDCF modules. Other organisations with existing risk assessment processes may choose to continue using these and only adopt the DSLs (DSL module). Organisations who do not formally classify their data or are looking to update current systems, may use the DSLs (DSL module) and markers for internal classification (Markers module). For those with current classification systems, the common language of the IDCF DSLs can be useful when sharing data with other organisations.

Organisations should focus on the parts of the IDCF most valuable to them and use them to suit their needs, expanding their use as appropriate. Organisations can ask the following questions to identify how to use the IDCF:

- Do we have current practices that are compatible with the IDCF? Will we retain them?
- Which parts of the IDCF would provide benefit for our organisation?
- Which DSLs will our organisation use and what systems and controls do we need to meet our security requirements?
- Will we be using the IDCF for data sharing with other organisations?

A key decision for an organisation is to determine where the IDCF will be used, whether internally and/or at the boundary for sharing data with other organisations. The classification, labelling and marking of data and documents when using the IDCF is decided by the organisation.

For more information on classifying and marking data, please see the Introduction: Labelling and marking.

2.2.1. Expectations of using the IDCF

Organisations may voluntarily agree to use the IDCF as part of data-sharing agreements with other parties. For example, an organisation that stores their customers' personal information may choose to include its use of the IDCF in its privacy policy/agreement. Where an agreement is in place, the IDCF comes with obligations. It is important that all parties agree on the approach to using the IDCF before sharing data, acknowledging that organisations' risk appetites may vary. Due diligence is recommended to ensure the parties' use of the IDCF meets organisations' expectations.

The IDCF provides a code of conduct (refer to the Introduction: Code of conduct) with default rules and obligations to guide its responsible use. These terms may be modified by agreement, however they should remain aligned with the intent and purpose of the IDCF.

Although the IDCF is designed to provide a common language when sharing data, organisations may choose not to use the IDCF in data sharing agreements. This means organisations will not be able to use the common language of the IDCF to communicate protection requirements. This may result in inconsistent data handling practises and inadequate system controls to protect the data. In these cases, an organisation can still use the IDCF internally without external obligations.

For more information on the code of conduct, please see the Introduction: Code of conduct.

2.3. Labelling and marking

DSL labels and markers are the primary means of communicating information about data under the IDCF. The IDCF requires DSL labels and markers to be clearly placed and formatted. Guidance on visual marking for electronic documents and emails is provided in the relevant module (refer below). Organisations may decide to use other data labelling and marking methods, for example, on physical information.

2.3.1. Visual labelling and marking

In the IDCF, labelling is the process of applying a DSL classification to data. Marking is the optional process of applying markers to data. Visual labelling and markers are the primary method of communicating the DSL classification and markers applied to data. Methods for labelling and marking images or other multimedia data, databases or other data formats is at the discretion of the organisation.

For more information on classifying and marking, please see the DSL module: DSL overview and the Markers module: Details about markers.

2.3.2. Metadata for labelling and marking

The IDCF does not determine a preferred way to capture DSL labels and markers in metadata.

2.4. Code of conduct

The IDCF is voluntary, however it comes with a set of expectations and responsibilities. While these may be explicitly captured in legal agreements between parties, there are also broad community expectations when an organisation claims to use the IDCF.

Any organisation claiming to use, have systems consistent with, or engage with the IDCF, is expected to uphold these expectations and obligations.

The code of conduct outlines broad expected behaviours and requirements that an organisation should adhere to when they claim to be using or be compliant with the IDCF.

Any organisation that uses the IDCF to classify data or agrees to receive data that has been classified under the IDCF should agree to adhere to the code of conduct. This means data has been risk assessed, a DSL label has been applied and the related systems are secured to meet the DSL's required level of protection.

The code of conduct applies only to organisations that have indicated to another party (publicly or privately) they will act in a way that is consistent with the IDCF. It also applies only to the data associated with that commitment.

2.4.1. General conduct

The terms ‘respect’ and ‘respecting’ refer to upholding the intent behind the IDCF components. Those adopting the framework are expected to act in good faith. This includes:

- Respecting DSL labels as applied to data and ensuring data is kept in systems with adequate protection measures appropriate to the data’s DSL classification.
- Prior to any data sharing, the data owner should negotiate with a data recipient on the use of the IDCF. This includes negotiating which DSLs will be handled by a data recipient and any expectation on the data recipient to respect additional IDCF markers applied to the shared data. The onus is on the data owner to ensure a data recipient can properly handle data classified under the IDCF.
- Ensuring systems are fairly assessed when determining their appropriateness for data of a specific DSL.
- Unless otherwise agreed with the original data owner, data received under an arrangement in which the IDCF is used (implied or explicit) will be handled and treated according to the DSL rules.
- Respecting and retaining markers that have been negotiated or agreed. All other markers may be removed by a data recipient.

For more information on DSL rules, please see the DSL module.

3.
Risk assessment module

This module provides introductory content for organisations with limited experience or technical expertise in risk assessment. More guidance may be needed from a security professional to effectively assess data risk in large organisations and complex contexts.

Organisations with existing data risk management processes may decide to continue using their own processes.

3.1. Introduction

Understanding and managing risk is central to protecting an organisation's data and classifying data under the Industry Data Classification Framework (IDCF). All data, whether financial records, client details, operational data or intellectual property, carries a level of risk if exposed, misused, modified, unavailable or lost.

A data risk assessment is a process that involves:

- identifying your organisation's data assets
- identifying potential events that could affect the data assets
- evaluating the consequences and impacts of those events.

3.1.1. Key terms

The following key words and phrases are used in this module and are defined in Appendix A: Glossary.

Table 2: Risk assessment key terms

Key term	Definition
Adversary	A person, group, organisation or government that conducts an adverse event. This is based on the NIST definition. Note that some frameworks refer to an adversary as a malicious actor.
Adverse event	An accidental or malicious event with a negative consequence that compromises the confidentiality, integrity and availability of data. A data breach is one type of adverse event. This is based on the definition in NIST SP 800-61r3.
Availability	Timely and reliable access to data.
Confidentiality	Preserving authorised restrictions on data access and disclosure, including means for protecting personal privacy and proprietary information. This is based on the NIST definition.
Consequence	The outcomes of an event. For example, identity theft might be a consequence of a loss of personal information.
Data breach	The unauthorised movement or disclosure of sensitive private or business information, including personal information under the *Privacy Act 1988*. For more information see ASD's glossary and information on data breaches.
Data protection	The process of safeguarding data from negative consequences that compromise its confidentiality, integrity and availability.
Event likelihood	The chance or probability, expressed qualitatively, of an event resulting in an adverse event.
Impact	The level of harm expected to result from the consequence(s).
Inherent risk	The risk of an event before security controls have been implemented.
Integrity	A property whereby data has not been modified in an unauthorised manner since it was created, transmitted or stored. This is based on the NIST definition.

3.1.2. Module overview

This section provides introductory guidance on conducting a risk assessment and provides links to supplementary resources. By identifying data risks and understanding the consequences and impact posed by adverse events, organisations can use the appropriate IDCF Data Security Level (DSL) to communicate the level of protection required for their data.

The process considers what could happen to data assets if there was an adverse event. It considers different aspects of data protection, including:

- **Confidentiality**: preventing unauthorised disclosure or exposure of data
- **Integrity**: maintaining accuracy and preventing unauthorised modification or corruption
- **Availability**: ensuring that authorised users can access data and systems when needed.

By assessing potential events along these three aspects of data protection, organisations can better understand their vulnerabilities and what proportionate controls are required.

This risk assessment module comprises five sections, About risk assessment, Understanding your data, Consequences of an adverse event, Impact assessment and Understanding adverse events.

For more information on DSLs, please see the DSL module.

Understanding your data

This section is for users with limited experience or technical expertise in risk assessment. It outlines the concepts of data types, scale and currency and explains how they influence the consequences and impact of an adverse event. These insights underpin effective data risk assessments and help guide the classification and protection requirements of data.

For more information on understanding data, please see the Risk Assessment module: Understanding your data.

Consequences of an adverse event

Consequence refers to the potential direct outcome of an event. When an adverse event occurs, various types of consequences can arise, affecting not only the individuals but also the organisation's assets or operations. This section provides an overview of different consequence types and helps organisations understand and identify the unique repercussions of each.

For more information on consequences, please see the Risk Assessment module: Consequences of an adverse event.

Impact assessment

This section outlines the potential impact of consequences on individuals or organisations when an adverse event occurs. It considers the severity or impact the adverse event (for example, data breach, data loss or system failure) could have on individuals or organisations. The impact could be financial, reputational, operational, legal or involve loss of data access or integrity.

While consequences and impact are often used interchangeably, in the IDCF the term **consequence** refers to the direct result of an **adverse event** and **impact** is the severity or level of harm of those consequences.

For more information on conducting an impact assessment, please see the Risk Assessment module: Impact assessment.

Understanding adverse events

The section explores different adverse event types that impact data. These events can be categorised into physical, cyber and authorised person events.

For more information on adverse events, please see the Risk Assessment module: Understanding adverse events.

3.2. About risk assessment

This section introduces and provides guidance on how to conduct a simple risk assessment on data assets. It also provides additional resources to support the risk assessment process.

3.2.1. What is data risk assessment?

A data risk assessment is a critical step in safeguarding your organisation against different threats. It is the process of identifying potential threats to your organisation's data and systems, evaluating the likelihood and impact of these threats, and determining appropriate controls to mitigate them.

A data risk assessment is a process that should be adapted to the organisation. It requires a thorough understanding of the data held and its value. Once the value is understood, an organisation can determine the appropriate environment to store the data. This is done by considering possible adverse events that could compromise the confidentiality, integrity and availability of the organisation’s data assets.

All data held by an organisation has an inherent risk level. This is the level of risk that exists before any protective controls are applied. Inherent risk reflects the potential impact if the data were exposed, modified, misused, unavailable or lost, regardless of current safeguards. Highly sensitive, business-critical or regulated data will naturally have higher inherent risk than routine or low-value data. This section outlines a simple risk assessment process to help organisations identify inherent risk in their data and determine the protection requirements needed to reduce the risk to an acceptable level.

Organisations can select and assign an appropriate IDCF DSL classification to ensure proper management and control of access to the data. Applying a DSL and storing the data in a secure system that is appropriate for its classification helps lower the risk to that data.

While data can be modified or destroyed to reduce risk, it is assumed in the IDCF’s risk assessment process that a decision to retain the unmodified data has already been made. Risk mitigation is therefore restricted to the implementation of security controls (physical, cyber and users) ensuring that the data is stored, processed and shared within environments that align with its IDCF DSL.

3.2.2. What are the elements of risk?

The elements of risk are the key components that together determine the level of risk in any scenario. Understanding these elements is essential for effective risk assessment and management. The core elements of risk are **assets**, **vulnerability, threat, likelihood, adverse event, consequence** and **impact.** Figure 4 below illustrates these core elements and their relationships.

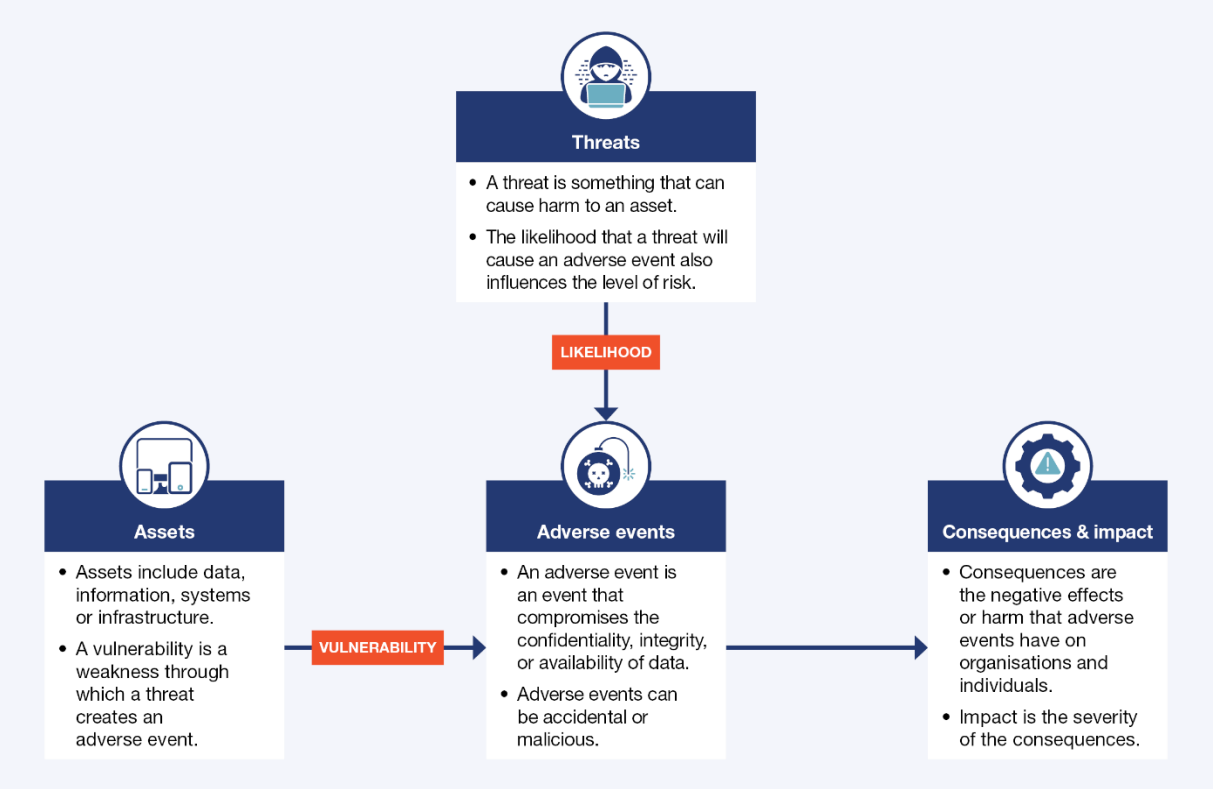

Figure 4: The elements of a simple risk assessment process

For more information about the elements of risk, please see the UK National Cyber Security Centre (NCSC) risk management guidance document.

Assets

An asset is an item that is protected due to its perceived or actual value. Assets include data, information, systems or infrastructure that have value to an organisation. For example, personal information of customers, intellectual property and critical IT systems. In the context of the IDCF, an asset is the data (or the information represented in data) and the systems or devices on which that data resides.

Consequence

Consequence refers to the negative effect or harm on individuals or organisations if an adverse event occurs. Consequences can be financial, reputational, operational, legal or a combination. For example, regulatory penalties and losing customers after a privacy breach.

For more information on consequences, please see the Risk Assessment module: Consequences of an adverse event.

Impact

Impact refers to the severity or level of harm of the negative consequences from an adverse event. Impact is measured as very low, low, moderate, high and very high.

For more information on impact, please see the Risk Assessment module: Impact assessment.

Threat

A threat is something that could cause harm to an asset. Threats can be intentional, for example, an adversary sending a phishing email to steal login credentials. They can also be unintentional, for example, an employee emailing the wrong file or damage to physical devices due to a natural disaster such as flood.

Vulnerability

A vulnerability is a weakness that makes an asset susceptible to a threat. Vulnerabilities could be technical, organisational or procedural. For example, a technical vulnerability could be outdated software, organisational vulnerabilities could include weak password policies or a lack of staff training, and procedural vulnerabilities could include a lack of established process or poor incident response plan.

Adverse event

An adverse event is an accidental or malicious event with negative consequences which compromises the confidentiality, integrity and availability of data. An adverse event can trigger a cascade of other events, affecting an organisation across multiple levels. These events may arise at various stages of the data lifecycle, from collection to disposal. Understanding the value and risk of the data organisations hold helps them to apply appropriate security controls to prevent adverse events.

For more information on adverse events, please see the Risk Assessment module: Understanding adverse events.

Likelihood

Likelihood refers to the probability of something occurring. The IDCF uses likelihood in the context of an adverse event. Likelihood is often expressed qualitatively as very low, low, medium, high or very high, and is based on past/historic data or expert judgement. For example, without email filtering there is a high likelihood of ransomware affecting a network.

3.2.3. Risk assessment process

Below is an outline of the process to perform a simple risk assessment. Please see Figure 5 for a visual representation of the risk assessment process.

1. Understand your data or information assets
    - A key component of assessing risk is to understand what needs protecting. Determine what data and information are held or might be held by your business operations. For example, customer data, financial records, employee information, intellectual property, operational software and hardware.
2. Identify potential consequences and impacts
    - Identify all potential consequences if an adverse event were to occur. To assess impact, organisations should determine which areas or activities of the organisation or individuals would be affected by the identified consequences. Then, organisations should rate the severity of those potential consequences on individuals or their organisation.
3. Identify potential events and assess their likelihoods
    - Identify potential adverse events that could lead to the previously identified consequences and impacts. Common events include cyberattacks (phishing and ransomware), physical thefts, system failures or human errors. Ensure both external and internal threats are considered when assessing events, as well as the compromise of the confidentiality, integrity and availability of your assets.
    - Assess vulnerabilities in your organisation to evaluate how susceptible your assets are to the identified adverse events and evaluate the likelihood of such events without any controls in place.

4. Evaluate the inherent risk level

    - To assess the inherent risk level, combine the information assessed about impact, events and their likelihoods. The organisation should then consider this knowledge within its business context to select an appropriate level of protection for the data or information.

For more information on classifying data under the IDCF, please see the DSL module.

5. Review and monitor

    - Risk assessment is not an activity that should be completed only once. Continuous monitoring and regular review ensure that data risk management remains effective over time. It is important to regularly:
        - review data assets, vulnerabilities and threats
        - revisit potential adverse events, their consequences and impacts
        - update the risk assessment as the organisation evolves.

Different organisations and industries apply risk assessment practices to systematically identify, evaluate and manage risks to data. These processes may have different steps. International standards, such as NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments have a four-step risk assessment process while UK NCSC's risk management guidance provides an introductory 11-step process. The IDCF adopts a simplified approach based on UK NCSC guidance.

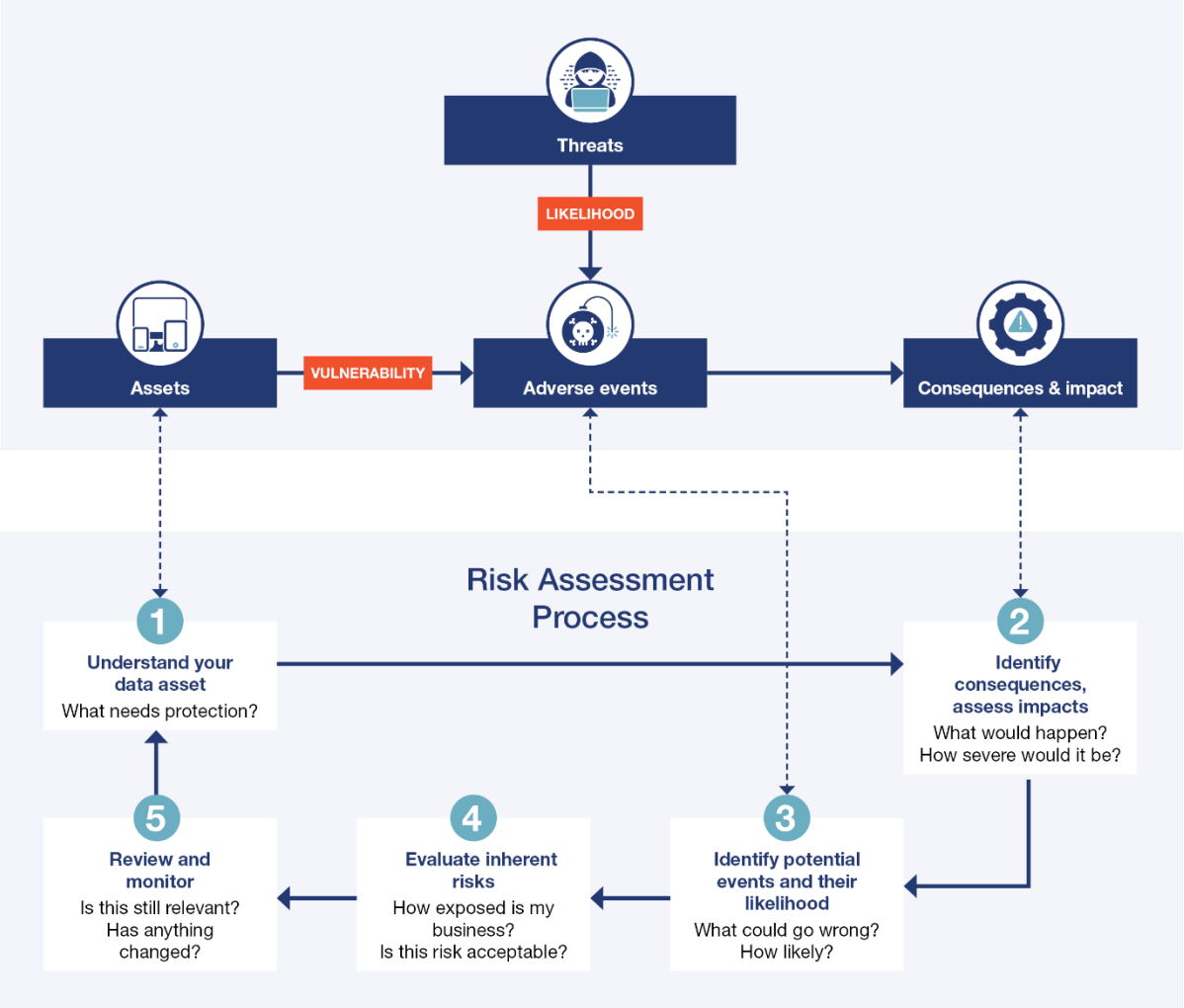

Figure 5: The elements (top half) and the steps (bottom half) of a simple risk assessment process

3.2.4. Practical tips

Conducting a data risk assessment does not need extensive technical knowledge and may not need an exhaustive assessment of all possible threats. Awareness of how the organisation operates and how data is used within the organisation will help streamline your data risk assessment. These tips can help simplify the process:

6. Start simple
    - Begin with your most critical assets, for example, customer data, payment details or your website. Identify what could go wrong and the consequences. You do not need to assess every possible risk at once.
7. Use available tools
    - Make use of risk assessment templates or checklists from trusted sources like the Australian Signals Directorate (ASD), NCSC or small business associations. These tools can guide your thinking and help you record your findings.

For a non-exhaustive list of available resources, please see the Risk Assessment module: Further reading.

8. Consider confidentiality, integrity and availability
    - It is important to go beyond simply protecting data. Certain adverse events will impact the integrity of your data, resulting in unauthorised modifications. Impact on availability may result in the organisation being unable to access its data.
9. Customers and stakeholders first
    - Focus on what matters to your organisation, your customers and stakeholders. For example, if losing access to a system would disrupt your work, it may be worth prioritising the management of this risk.
10. Triaging
    - Triaging is a quick and effective way to consider the risks of simple data assets. This process involves triaging simple data assets with a conservative approach of risk when classifying them under the IDCF. Although this may result in data being overclassified, if your systems are appropriate for the applied IDCF classification, the data will be appropriately protected.
    - If there is a need or want in the future to store data in a system with lower security, conduct a formal review or risk assessment first. This will help you decide if the change is suitable and if the new security measures remain adequate.
11. Create a risk aware culture
    - Risk assessment is everyone's responsibility in an organisation. Engaging with employees to consider risks and how they align to organisational objectives is essential to the process.
12. Seek external help when needed
    - When you find it difficult to understand the risk or follow existing risk assessment guides or tools, consider seeking expert advice from a data risk specialist.

3.3. Understanding your data

This section explains how different characteristics of data can influence the impact of an adverse event. It is intended to help individuals or organisations with limited experience in risk assessment to understand the value of their data and the potential impact of an adverse event as part of the risk assessment process.

3.3.1. What's the nature of your data and its potential impact?

Data is a strategic asset in today's digital landscape that carries inherent risks. While data enables insights, innovation and improved decision-making, it can also contain sensitive, personal or confidential information. If data is mishandled, it can lead to privacy breaches, reputational or financial damage, regulatory penalties, harm to individuals or even pose risks to national security.

Assessing data risk in terms of the impact on the data owner is an important part of accurate data classification and protection. The following is a summary of the content covered in this section.

What is the impact of your data?

- **Public data:** Carries low or insignificant impact, as the data is intended for sharing.
- **Synthetic/anonymised data:** Low impact, when the data is artificially generated. Anonymised data may hold greater risks depending on the quality of anonymisation.
- **Personal/sensitive data:** Medium to high impact in the event of a breach.
- **Nationally important data:** Potentially high impact depending on the value of the data.
- **Audit logs, metadata, AI models:** Risk level varies based on the content and context.

Risk depends on context

The impact of an adverse event depends on the:

- **Type of data**: Some data types may carry a higher impact than others if an adverse event occurs. For example, financial or health data may contain sensitive information about individuals compared to aggregated road traffic data.
- **Scale**: The number of records being held by an organisation is an important factor. For example, a data breach involving 100 records may be critical for a small business while it may be considered minor for a large corporation.
- **Timeliness**: Recent data may pose a greater impact to an organisation than older historical data. For example, an organisation's recent financial figures may affect business operations and be more valuable to an adversary than financial data from 10 years ago.

The bottom line

Not all data carries equivalent inherent risk and needs the same level of protection. The context in which data is used (such as the scale, sensitivity and timeliness of the data) greatly affects the potential impact to an organisation if compromised. This section encourages organisations to consider how valuable, current and identifiable the data is when determining risk levels.

3.3.2. Data types

Different types of data carry varying degrees of sensitivity and therefore have different levels of impact. Recognising these data types is essential when applying an appropriate IDCF DSL and security controls.

Below is a non-exhaustive outline of data types to help guide the risk assessment and data classification processes.

Publicly available information

Publicly available information refers to data that is intentionally accessible to the public without significant restrictions. Examples include company contact details published on a website, media releases, published reports, service brochures or statistical material that is intended for public distribution.

This information is typically published for the purpose of transparency, awareness or public benefit. While an adverse event regarding this type of data is considered to have very low or no impact, the data should still be reviewed to ensure:

- no sensitive details are inadvertently disclosed
- the data is unlikely to be linked with other data (public or private sources) in a way that creates risk
- impacts on data integrity and availability are low.

If any of these points are of concern, the data may need higher levels of protection. Where publicly available information is also personal information, the *Privacy Act 1988* may still apply.

Personal information

Personal information is any information that can identify an individual, either directly or indirectly. This includes obvious identifiers such as names, addresses or identification numbers, and less direct data like IP addresses, location data or characteristics that, when combined, could reveal someone's identity.

As this data relates to people, it carries a high level of impact if lost, exposed or misused. Unauthorised access to personal data can lead to privacy violations, identity theft, reputational harm or legal consequences. Handling personal data needs strong security controls, clear access permissions and compliance with data protection laws such as the *Privacy Act 1988*.

For more information on personal information, please see the Office of the Australian Information Commissioner (OAIC) guidance on What is personal information.

Sensitive information (*Privacy Act 1988*)

Under the *Privacy Act 1988*, sensitive information is a subcategory of personal information. This includes information such as health records, financial details, racial or ethnic origin, political opinions, religious beliefs, sexual orientation, or biometric and genetic data. Sensitive information may need extra protection due to the potential harm it could cause if disclosed or misused.

Exposure of sensitive information can lead to serious consequences such as discrimination, emotional distress, financial loss or targeted attacks. Under the *Privacy Act 1988*, organisations handling personal information, which includes sensitive information, must take reasonable steps to protect the information. For example, encryption, access restrictions, regular audits and compliance with privacy regulations. Consent is generally required to collect sensitive information.

Sensitive data (General)

Sensitive data may also refer to commercially sensitive information that an organisation has cause to keep private. Examples include amounts paid under a contract or the size of the company's inventory.

Synthetic data

Synthetic data is artificially generated data that mimics the structure and some characteristics of real data without revealing any attributable personal, sensitive or confidential information from actual individuals or organisations. It is typically used for system testing, AI model training and demonstrations, or situations where using real data would carry unacceptable risk or would otherwise be inappropriate. Additionally, synthetic data may act as a decoy dataset to lure, detect and analyse unauthorised access attempts, providing early warning of malicious activity without exposing real data.

When properly generated, synthetic data has minimal risk to individuals and organisations and carries a low level of impact. Synthetic data may pose risks where it is generated in a manner that does not fully guarantee the anonymisation of individuals, thereby not adequately mitigating the risk to those individuals. For example, scrambling existing real data to create synthetic data may leave unique patterns intact, allowing individuals to be re-identified if those patterns align too closely with real-world records. The risk of being able to re-identify will only increase as technology advances.

If the process of creating synthetic data does not sufficiently consider risks, it may give a false sense of security. This may result in reputational harm or regulatory consequences if assumed risks were not actually mitigated. For example, if a business's confidential strategies or operational models were inadvertently mirrored in the synthetic dataset, they may become exposed. Clear communication about the scope, limitations and intended use of synthetic data is essential to avoid misuse and ensure informed handling.

A risk that is often overlooked with synthetic data is the possibility that it could be mistaken for real data. If mistaken for real data, it may cause an adverse event for the organisation when no actual adverse event has occurred. Failure to communicate the limitations of synthetic data and to prepare for false claims about the data can result in financial and reputational harm to an organisation.

Aggregated data

Aggregated data is information or data compiled from multiple sources and summarised to provide general insights or trends. It is commonly used for reporting, analysis and decision-making. When the original data includes personal information, the aggregation process typically involves removing or anonymising personal identifiers to reduce privacy risks.

For sensitive business information, aggregated data may inadvertently contain specific patterns about business processes or operational strategies. For example, instead of reporting individual store sales, a retail chain may aggregate sales data across all stores in a region. This allows for meaningful trend analysis while protecting the performance details of any single store, thereby safeguarding commercially sensitive information.

Aggregated data that does not contain personal information can be lower risk than data containing individuals' or organisations' records. However, it can still pose a medium impact if sensitive or confidential information can be retrieved or reconstructed, especially when combined with other datasets.

For example, if quarterly revenue figures are published in aggregate for an industry with only a few major players, it may be possible to deduce an individual company's approximate financial performance. This may occur through subtracting known figures from other businesses, potentially exposing confidential business strategies or growth trends.

Pseudonymised data

Pseudonymised data has been processed to replace identifiable information (like names or ID numbers) with pseudonyms or codes. It aims to reduce the risk to individuals but may not address other risks such as commercial sensitivity. While this may prevent the direct identification of individuals, individuals would still be identifiable if the pseudonyms can be linked back to the original identities using additional information. This data is only de-identified while both the pseudonymised dataset and the re-identification keys remain securely protected and separated. If the re-identification keys are easily regenerated, they do not provide protection. An adverse event is likely to compromise this protection by exposing or altering the re-identification keys or making them unavailable.

Pseudonymised data carries a medium to high impact, depending on the protection of the re-identification keys. For example, if the keys are stored with strong encryption and appropriately separated from the pseudonymised dataset, the risk is reduced. If they are poorly secured or stored alongside the dataset, the risk is similar to that of fully identifiable data. To manage the risk effectively, organisations should store re-identification keys separately, limit access to authorised personnel and apply robust security controls. This approach is commonly used in research, analytics and system development where some connection to an individual must be maintained without revealing their identity.

Anonymised data

Anonymised data has been processed to remove all personally identifiable elements. The objective is to make it impossible to identify an individual from the data, either from the data alone or when combined with other information. This differs from pseudonymised data, where re-identification remains possible under certain conditions. Anonymised data only reduces the risk associated with individuals and may not address other risks such as commercial sensitivity. Data.gov.au Risk Key Concepts refers to anonymised data as *confidentialised data* that has been de-identified and has had other information removed or modified to reduce the risk of the person or organisation being identified.

An adverse event involving anonymised data is generally considered to have low impact as it no longer relates to identifiable individuals. However, there may be residual risks if the anonymisation process is flawed or if the data can be matched with other datasets to reverse the anonymisation. To maintain low levels of risk, organisations should apply strong anonymisation techniques and conduct regular reviews, especially when sharing data externally.

Nationally important data

Nationally important data refers to data that could cause significant harm to the nation if an adverse event were to occur. Protection of this type of data may involve ensuring that it is subject to the laws and governance of a specific country and must be processed, stored and/or handled in that country. This is done with the intention to minimise the data's exposure to other countries or jurisdictions.

Examples of this type of data include data collected, stored or processed by government entities that, due to its nature or source, must remain within a country's borders to comply with laws and regulations. It may also include data that is significant to critical infrastructure, such as electricity infrastructure design data, or the provision of services to significant populations, such as critical logistics details in a national supermarket organisation.

Nationally important data typically carries a potential high impact to a nation if compromised, especially when it involves sensitive national, legal or strategic information. This type of data does not need to be formally defined by laws or classified under national classification schemes. If the potential impact is of nation-wide significance, the data should usually be treated as nationally important. Unauthorised access, modification, transfer or processing of this data outside the permitted

jurisdiction can result in legal breaches, national security risks or loss of public trust. Organisations handling this type of data must ensure strict compliance with any applicable data residency laws.

Audit data

Audit data refers to records generated by systems and processes that log user activities, asset accesses, system changes and other operational events. This data is essential for monitoring, accountability, incident investigation and regulatory compliance.

Audit data is typically considered medium impact, depending on its contents. However, it can reveal significant information regarding the activities of the organisation. While it often excludes personal or sensitive information, it may contain usernames, IP addresses, access timestamps or actions that, when correlated, may reveal patterns about individuals or system vulnerabilities. Logs may also capture passwords where a user accidently enters it into the user field. To manage the risk, organisations should store audit data securely, ensuring it is available when needed, protect it against tampering and retain it according to regulatory or policy requirements. Access should be limited to authorised personnel and its use should align with privacy and security policies.

Metadata

Metadata refers to 'data about data'. It provides context or additional information about data assets. It may be personal information under the *Privacy Act 1988* and require specific protections. This can include details such as the creation date, author, file type, data source, access history, location and usage patterns. Metadata helps with organising, discovering and managing data or information efficiently.

Metadata is generally considered low to medium impact, depending on its content and how it is used. On its own, metadata may seem harmless, but it can reveal sensitive insights, such as who accessed a document, when and from where. Location data embedded in photos can place people in locations at specific times. Metadata may include usernames or device information, which could be exploited in social engineering or cyberattacks. To manage these risks, organisations should review metadata before sharing files externally and use tools to clean or control metadata exposure where necessary.

Metadata considered under the *Telecommunications (Interception and Access) Act 1979* have data retention obligations.

For more information, please see the Department of Home Affairs data retention obligations for service providers.

AI models

As data assets, AI models refer to the trained machine learning models or the resultant program that encapsulates patterns, relationships or insights learned from the datasets they were built on. These models can range from simple classifier models to complex large language models (LLMs) and often represent significant intellectual property and operational value.

AI models are typically considered medium to high impact depending on what data was used to train them, their intended use and how they are deployed. If models are trained on sensitive or personal data without proper safeguards, there is a risk of unintended leakage, where outputs or behaviours could reveal sensitive information. Additionally, AI models may be vulnerable to adversarial attacks where adversaries attempt to infer training data or manipulate outputs. To manage the risk, organisations should protect the confidentiality of their AI model, maintain its integrity and guarantee its availability. This can be achieved through measures such as access controls, resilient infrastructure and backup strategies.

For more information, please see ASD's Deploying AI systems securely.

AI-generated or AI-modified data

AI-generated or AI-modified data may introduce risks. This type of data may contain inaccuracies, bias or unintended disclosures, which may be derived from the original data used to train the AI or previous data given to it as prompts. This data should be validated before operational use, clearly

identified as AI-generated, and go through a data risk assessment under the same confidentiality, integrity and availability principles as other data assets. Organisations should ensure human oversight and appropriate governance to manage these risks.

3.3.3. Data scale

Data scale refers to the volume and breadth of data records, such as the number of individuals represented, or the geographical or organisational spread of the data. For example, a dataset containing health records for every hospital in a particular state or territory represents a significantly broader scale when compared to a dataset containing records from a single doctor's clinic. The scale of data plays a pivotal role in assessing the impact of an adverse event.

Generally, the larger the scale, the greater the potential impact of an adverse event, such as a data breach. High-scale datasets often carry amplified consequences. The compromise of high-scale data may affect a broader population, leading to widespread harm and reputational damage. It is important to recognise that even small-scale data can have a high impact if it represents all the data the organisation holds, is about a significant individual, or about a minority group with certain characteristics.

For example, consider the difference between:

- 100 customer records in a small or medium-sized enterprise
- 100 customer records from a database of 1 million in a large corporation.

Both datasets contain the same number of records, but the context, consequences and ability to react vary considerably as shown in Table 3.

Table 3: Difference of potential impact of a data breach between organisations according to the data scale

	Impact to SME (100 out of 100 records)	**Impact to a large corporation (100 out of 1,000,000 records)**
Proportion of total affected	100% – entire customer base	0.01% – minor segment
Operational impact	Very high – likely halts core services	Low – operations may continue
Reputational damage	High – breakdown of trust	Low – if seen as an isolated issue
Legal/regulatory implications	Potentially very high	Potentially very high – but may be managed through established compliance processes
Public attention	Low – however customers may feel more personally impacted due to their close relationship to the business	Variable – high if there is significant media coverage and public scrutiny
Ability to respond	May not have the skills and resources to respond	Likely to have a plan to respond and personally contact individuals impacted

By understanding how data scale influences impact, organisations of all sizes can make informed decisions about what controls should be applied to their data assets and where they should focus their efforts.

3.3.4. Data currency or data timeliness

Data currency refers to how current or up to date a piece of data is. The age of the data, whether it is real-time, recent or several years old, can significantly influence both its value to the organisation and the impact of the misuse, tampering, loss or breach of the data.

Recent data or 'high currency' data, usually has higher impact. If compromised, personal, financial or operational data is more likely to cause harm. For example, releasing current health records or payroll information can result in immediate consequences like fraud or identity theft. Also, releasing future project plans or not-yet-released product data could significantly damage the competitive position of a business, even if the data volume is small.

For an adversary, current data is more usable, resalable or exploitable. This may increase the potential impact.

Older data may have reduced relevance and often the impact is lower if the data is no longer exploitable or linked to active business processes. However, outdated or obsolete data may still be sensitive, for example, historical medical records. If older data is still personally identifiable or sensitive, it must have appropriate protection.

When considering data currency, any legislative requirements relevant to the data held should be considered.

Table 4 provides some examples of how data currency affects the impact of an adverse event.

Table 4: Examples of how data currency affects the impact of an adverse event

Example	Data currency	Impact if leaked or compromised	Potential protection level
Real time patient treatment notes	High currency	High impact: due to the sensitive nature of the information	High protection level
Current customer support records	High currency	High impact: due to the sensitive nature of the information	High protection level
Employee rosters from 10 years ago	Low currency	High impact: due to the potential impact to individuals	High protection level
Current systems logs with no sensitive data	High currency	Moderate to high impact: as security gaps or loopholes can be revealed to an adversary	Moderate to high protection level
Historical system logs with no sensitive data	Low currency	Low impact: as information is old and not sensitive	Low protection level

It is important to apply appropriate protection to data that is current, relevant and sufficiently accurate to support timely decisions or operations to reduce the likelihood and impact of adverse events. Current data may warrant a higher protection, especially if it includes personal, financial or business strategic elements. Over time, historical data may need less protection, but only if it is no longer sensitive or identifiable.

3.4. Consequences of an adverse event

When an adverse event occurs, it can lead to a range of consequences that may affect an organisation's operations, reputation, legal standing and financial stability. By understanding and assessing these potential consequences, organisations can better prepare and mitigate potential losses and maintain compliance with relevant regulations.

This section aims to help organisations understand the potential consequences of adverse events and includes:

- a non-exhaustive list of common consequences of adverse events
- reasons for considering all potential consequences for your data, regardless of the data type
- a detailed description of common consequences and their prominent data types.

For help identifying potential consequences, please see the consequence identification questionnaire in Appendix B: Consequences questionnaire.

3.4.1. Common types of consequences

The list below outlines common types of consequences faced by organisations following an adverse event. It is important to note that different data types involved in an adverse event can have different consequences.

For more complex scenarios, users are encouraged to consult resources such as those provided by the NIST or the International Organisation for Standardisation or engage a data risk specialist.

For links to additional resources, please see the Risk Assessment module: Further reading.

The IDCF's consequence list has been compiled from the information available in existing standards and frameworks, such as:

- NIST Special Publication 800-30 Guide for Conducting Risk Assessments
- NIST Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations
- Australian Prudential Regulation Authority (APRA) Prudential Practice Guide CPG 234 Information Security
- industry best practice sources such as MITRE ATT&CK Matrix for Enterprise.

For quick reference, the eight consequences are listed below. To assist with making an assessment based on these eight consequences, click on one of the listed items, or refer to Risk Assessment module: Conducting a consequence assessment.

1. **Privacy consequences**
    - Privacy consequences refer to the harm caused when an individual's privacy is compromised, such as when personal information is accessed, disclosed, altered or misused.
2. **Confidentiality loss**
    - Loss of confidentiality occurs when sensitive or private information given in confidence is accessed, disclosed or shared without authorisation.
3. **Reputational damage**
    - Reputational damage is the harm to an organisation's public image or the erosion of stakeholder's trust.
4. **Legal**

- Legal consequences refer to the legal penalties, sanctions or regulatory action resulting from the failure to adhere to data protection laws, industry standards or contractual obligations.

5. **Financial loss and penalties**
   - Financial consequences refer to the monetary losses an organisation faces due to an adverse event.
6. **Operational disruptions**
   - Operational disruptions are the interruptions to an organisation's normal operational activities caused by an adverse event.
7. **Organisation strategy**
   - Strategic consequences refer to long-term obstructions that may impede an organisation's ability to achieve its organisational objectives.
8. **Security**
   - Security consequences refer to the exposure of vulnerabilities in an organisation's systems that arise because of an adverse event. For example, data about an organisation's systems could help adversaries find weak points in their system security.

Consequences can be connected, with one triggering others. This compounding effect may result in multiple consequences occurring together and escalating in severity.

Privacy and confidentiality are often thought of as principles-based concepts to be protected. These consequences can be both direct and indirect, representing the primary impact of an adverse event or triggering other consequences like reputational or strategic consequences. For example, if an adversary stole an organisation's customer data, the direct consequence may be identity theft. Subsequently, the identity theft may lead to financial consequences for both the individual and the organisation. The IDCF includes privacy and confidentiality as consequence types to capture these distinct forms of harm. It supports organisations to understand the potential for cascading events and subsequent broader consequences and impact.

It should also be noted that the above consequences can have national security implications. For example, foreign actor access to a dataset may allow them to use it for **sabotage** (access to controlled systems), **espionage** (theft of intellectual property (IP), sensitive information or bulk data for coercion of individuals), or **foreign interference** (data used against national interests, such as election interference, coercion of a political organisation or targeted information campaigns). While the national security implications may not always be front of mind for organisations, adversaries' access to data from multiple sources over time can pose serious risks to organisations, individuals and national security.

3.4.2. Data types and their role in identifying consequences

Consequences of an adverse event may not be immediately obvious. Adverse events of any type can have wide ranging consequences.

The types of consequences resulting from an adverse event will be influenced by the type of data involved. Knowing the data type involved in the event is helpful in focusing on the most obvious potential consequences of the event. However, too much focus on the type of data can lead to missing other, linked or connected consequences.

For example, an organisation encounters a breach of its business activity data. The organisation assessed the consequence as causing financial loss and/or operational impact. Because the organisation based its consequence assessment on the 'data type', they overlooked privacy consequences because the 'business activity' data included personal information about employees.

This is why the IDCF encourages consideration of each potential consequence for **all data types**.

For more information on understanding how types of data influence consequences, please see the Risk Assessment module: Understanding your data.

3.4.3. Conducting a consequence assessment

When conducting a data risk assessment, consideration should be given to the types of data held and the risks associated with that data. An organisation should consider the consequences of an adverse event to itself and other groups the data relates to. Below are questions for the eight consequence types referenced earlier that an organisation can use to identify potential risks in their data. For each consequence type, specific potential consequences of adverse events, typical data types and examples of how an adverse event could impact the organisation are outlined.

Privacy consequences

If you answer yes to any of the questions below, this may indicate a potential privacy consequence associated with an adverse event. A thorough risk assessment should be undertaken.

- Is this data influenced by the actions of individuals?
- Is it possible to infer something regarding an individual from the data?
- Does the data contain personal or sensitive information, for example names, addresses, health details or opinions about individuals that is subject to privacy laws?
- Could individuals be harmed by the exposure of this data, for example identity theft or harassment?

Privacy consequence refers to the harm caused when an individual's privacy is compromised. Privacy consequences occur when information is accessed, disclosed, altered or misused in ways that interfere with an individual's privacy. Privacy consequences are particularly relevant when organisations collect, store or process data that can directly or indirectly identify individuals. This can include data collected for other purposes. When assessing impact, the IDCF advises focusing on the potential privacy consequences of an adverse event rather than solely on the compliance with legal requirements. This is because an adverse event can occur while being compliant with laws and regulations.

Types of data that contribute to privacy consequences

Any data that relates to people, measures human behaviour or is influenced by human actions can cause privacy consequences if compromised. This includes personal information, data that reflects human activity and data shaped by human activity.

Types of data that are considered personal information

Data that can identify a person, is about a person or can be linked to an identifiable individual is considered personal information. For example:

- full name, address, phone number, date of birth
- identification numbers such as tax file numbers
- financial and banking details
- health and medical records
- biometric data such as fingerprints
- email addresses, login credentials, IP addresses
- other information as defined in the *Privacy Act 1988*.

Types of data that reflect human activity

Data that intentionally measures or captures human activity may carry privacy risks. It can also be personal information under the *Privacy Act 1988*. For example:

- usage records of services
- shared location data
- social media 'check-ins'
- CCTV footage and location tracking
- location data generated by human actions, such as vehicle tracking or transaction locations
- vehicle number plates, images or counts
- other transactional based data such as use of services, purchasing histories and so on.

Types of data that are shaped by human activity

Some data is collected for purposes unrelated to individuals, yet it may still be shaped by human behaviour. For example, individuals' actions can influence sensor readings, usage patterns or system outputs. Additionally, data may unintentionally reveal insights about people and their activities, even if they were not the original focus of the data collection. For example:

- electricity usage for billing purposes may reveal types of devices a household uses, times of use and house occupancy. For example, electric vehicles and air conditioners
- live seating plans, office occupancy, booking or availability records
- vehicle data.

Note: According to ASD's Securing customer personal data, personal data includes a broad range of information that could identify an individual. Often, personal data is greater than the sum of its parts, as when seemingly innocuous data is aggregated or combined it can be used to form a more complete picture about an individual. Therefore, what constitutes personal data may differ based on whether a person can be reasonably identified given the context.

Potential consequences	Examples of privacy consequences in practice
Interference with privacy can have serious consequences for both individuals and organisations. Consequences include: **For individuals:** • identity theft or fraud • emotional distress or reputational harm • revelation of previously hidden behaviours. **For organisations:** • regulatory action, for example those under the *Privacy Act 1988* • compensation claims or legal action by the individuals • damage to reputation and loss of business.	• A HR database is compromised, exposing employee records, leading to identity theft, fraud and targeted phishing attacks. • Customer contact details are mistakenly emailed to the wrong person, breaching privacy obligations and resulting in reputational damage, customer distrust and regulatory penalties. • Client documents are stored in cloud storage without encryption, making them vulnerable to unauthorised access and potentially exposing sensitive personal information or confidential business information, such as legal or medical records. A breach results in the erosion of client trust, legal action, regulatory penalties and long-term reputational damage to the organisation. • Origin destination information from ride hailing services (e.g. taxis) reveals locations visited by a household, unintentionally disclosing patterns such as regular hospital visits or attendance at places of worship. This leads to inferences about health status, beliefs and routines, raising serious privacy concerns for customers or the service.

Confidentiality consequences

If you answer yes to any of the questions below, this may indicate a potential confidentiality consequence associated with an adverse event. A thorough risk assessment should be undertaken.

- Would sensitive or confidential information be disclosed to unauthorised parties if this data were exposed?
- Could competitors, criminals or unauthorised users benefit from accessing this data?

Loss of confidentiality occurs when sensitive information given in confidence is accessed, disclosed or shared without authorisation. This can happen due to data breaches, insider threats or inadequate access controls, and often leads to serious consequences across multiple domains.

Types of data that contribute to confidentiality consequences and their impact

Confidential information is any data or information that is not publicly available and is intended to remain undisclosed by an organisation or individual. Confidential information may be subject to a confidentiality agreement or implied confidentiality under common law. More broadly, it includes data or information that is to be kept internal to an organisation or a group of people. Examples include:

- **Internal business documents:** Exposure can reveal strategic plans or internal changes potentially weakening competitive position and damaging stakeholder confidence.
- **Financial records and reports:** Leaks of revenue, profit margins or forecasts can influence investor sentiment, cause market instability or affect negotiations and partnerships.
- **Trade secrets or proprietary information:** Theft or disclosure of confidential processes or formulas may lead to loss of competitive advantage, reputational damage and legal issues.
- **Legal documents and contracts:** Public access to confidential agreements or litigation documents can compromise negotiations, expose liabilities and harm legal standing.
- **Sensitive client or customer information:** Breaches involving client data can erode trust, lead to contractual breaches, regulatory penalties or lawsuits.
- **Information and data shared confidentially by other parties:** Mishandling shared sensitive data undermines trust and may result in the loss of business relationships or reputational damage for failing to uphold confidentiality.

Potential consequences	Examples of confidentiality consequences in practice
The potential consequences of compromised data containing confidential information can be significant and wide-ranging. These consequences may be legal, financial, reputational, operational or strategic in nature. Consequences for organisations include: • breach of confidentiality agreements • financial loss and legal penalties • damage to reputation and stakeholder relationships • negative media coverage or social media backlash • competitive disadvantage from exposed proprietary information.	• A staff member mistakenly sends a confidential client report to an external email address. This breaches contractual confidentiality obligations, leading to legal action or financial penalties. • An employee copies information when they leave the organisation, or a former employee using retained login credentials accesses proprietary information. Proprietary data or trade secrets are then leaked to competitors, harming innovation and market advantage. • Sensitive board meeting minutes are stored unencrypted on a shared drive, USB or laptop which is lost or stolen. This exposes strategic decisions and financial forecasts that may trigger reputational damage and expose vulnerabilities exploitable by competitors. • Customer transaction records are accessed by unauthorised staff without a business need. This is a confidentiality breach and violates privacy regulations resulting in fines and mandatory breach notifications. • An employee accidentally shares a spreadsheet containing employee salaries and performance reviews with all staff. This undermines internal trust, triggers workplace tension, grievances and resignations. • A software developer uploads confidential source code to their public GitHub repository. This exposes proprietary algorithms, trading logic or authentication methods, allowing competitors to replicate or exploit the organisation's intellectual property. This leads to competitive disadvantage, lost market share and erosion of investor confidence, particularly in sectors where technology is a key differentiator.

Reputational consequences

If you answer yes to any of the questions below, this may indicate potential reputational consequences associated with an adverse event. A thorough risk assessment should be undertaken.

- Could an adverse event lead to a loss of trust or confidence in the organisation?
- Does your organisation have a proactive plan in place to manage such a loss before it happens? Can you respond quickly and effectively?

Reputational consequence refers to damage to an organisation's public image and the erosion of stakeholder trust. This consequence often results from incidents involving data misuse, tampering, loss, breaches or non-compliance with data protection standards. Even when no laws or compliance requirements are violated, poor data handling, incident response management or a perceived lack of accountability can lead to significant reputational damage.

Types of data that contribute to reputational consequences and their impact

Certain types of data, when lost, breached or exposed, are particularly damaging to an organisation's reputation. It can signal weak data governance and poor organisational accountability. Examples include:

- **Personal information**: Exposure of names, addresses or identification numbers can lead to identity theft and loss of public trust. This could make individuals feel violated and unsafe, especially where vulnerable individuals are affected.
- **Financial data:** Leaks involving credit card numbers, bank details or payment records can lead to fraud and identity theft, often resulting in loss of customer trust, regulatory scrutiny and reputational damage.
- **Health records:** Breaches of personal medical data can cause significant emotional distress, public outrage and violations of patient confidentiality. This can be particularly damaging for healthcare providers.
- **Internal communications:** Leaked emails, chat messages or internal logs can reveal unprofessional behaviour, poor decision making or controversial opinions, sparking media backlash and reputational damage.
- **Intellectual property or trade secrets:** The loss or theft of proprietary designs, algorithms or trade secrets can undermine competitive advantage, reduce investor confidence and portray the organisation as vulnerable.

Potential consequences	Examples of reputational consequences in practice
Reputational consequences can have wide-reaching effects on an organisation's ongoing success. Its relationship with customers may be impacted and individuals may feel violated and unsafe. Consequences for organisations include: • customers' loss of confidence in digital services and platforms • customers' concerns about data misuse and ongoing security • loss of customer loyalty and brand credibility • decreased market share and sales performance • increased scrutiny from investors, media and regulators • difficulty attracting and retaining talent.	• A company suffers a data breach and is widely criticised for not advising their customers, resulting in regulatory fines, the potential for class action lawsuits and long-term erosion of brand reputation. • Personal customer details are leaked and discussed in the media, causing widespread outrage, damaging public trust in the company and a sharp decline in customer retention. • Stakeholders begin to question the integrity of leadership due to privacy violations which lead to board scrutiny, executive turnover and difficulty raising capital. • Social media campaigns call to boycott the company after a breach of sensitive community data. Public backlash can lead to halted sales, partner disengagement and long-term brand damage. • Release of synthetic or fake data which looks real and is misinterpreted by the public as having actual personal data included. Public misunderstanding erodes user confidence in data governance practices prompting customer attrition and regulatory scrutiny.

Legal consequences

If you answer yes to any of the questions below, this may indicate potential legal consequences associated with an adverse event. A thorough risk assessment should be undertaken.

- Would the exposure of this data violate any laws or regulatory requirements?
- Could the organisation face fines, lawsuits or regulatory investigations due to the adverse event?
- In the case of an adverse event, would you need legal advice?

A company must comply with data protection laws, industry standards or contractual obligations. Failure to comply may result in legal consequences, such as legal penalties, sanctions or regulatory action. Mishandling data or having a data breach increases the risk of increased liability and lawsuits.

Types of data that contribute to legal consequences and their impact

Certain types of data, when lost or exposed, can result in breaches of laws, compliance, contracts or non-disclosure agreements, leading to legal claims or regulatory action. Examples include:

- **Personal information:** Exposure of personal information such as names, addresses, Medicare numbers and tax file numbers may trigger regulatory action under the *Privacy Act 1988*, as well as compensation claims from affected individuals.
- **Health information:** Medical records and treatment details are sensitive information and must have a higher level of protection. Disclosure of health data may breach privacy or health laws and lead to costly remediation, regulatory penalties and legal action.
- **Financial data:** Exposure of bank account details or credit card information can lead to financial theft, trigger fraud investigations and result in significant penalties under different regulations, potentially damaging customer trust and financial stability.
- **Authentication credentials:** Loss of usernames, passwords and biometric data, may lead to breaches of security protocols and non-compliance with industry standards. Even when an organisation complies with necessary security standards, it may still be the victim of an adverse event, as new threats regularly emerge. This can result in costly remediation efforts, legal liabilities and loss of certification or closure of the business.

Potential consequences	Examples of legal consequences in practice
Failure to comply with legal or regulatory requirements can lead to serious consequences for organisations. Consequences for organisations include: • regulatory investigations and enforcement action • civil litigation including class action lawsuits • contract termination or a business partner withdrawing from a contract • mandatory audits or public reporting obligations • loss of operating licenses in certain sectors.	• A healthcare provider accidentally discloses patient test results via email, breaching the *Privacy Act 1988* and triggering mandatory notification under the Australian Government's Notifiable Data Breaches (NDB) scheme. • A cyberattack targeting a financial advisory firm exposing client banking information, resulting in investigations by Australian Securities & Investments Commission (ASIC) for potential breaches of law. • An employer stores employee tax file numbers and personal data in an insecure cloud folder based in a foreign country. The data is later accessed in a breach leading to regulatory fines, mandatory breach notifications, reputational damage and a loss of employee trust.

Financial consequences

If you answer yes to any of the questions below, this may indicate potential financial consequences associated with an adverse event. A thorough risk assessment should be undertaken.

- Could the organisation incur significant costs from fines, legal fees or compensation claims?
- Would business losses, including damage to sales or customer relationships, result from this adverse event?

Financial consequences refer to the monetary losses an organisation may incur due to an adverse event. These losses can arise from immediate costs, such as incident management, incident recovery, investigations and legal fees, as well as long-term costs, such as lost business, regulatory fines and customer compensation. Financial consequences are usually the easiest to measure and often have the biggest impact on an organisation after an adverse event.

Types of data that contribute to financial consequences and their impact

Certain types of data, if exposed or compromised during an adverse event, can lead to significant financial consequences. Examples include:

- **Financial information:** Exposure of credit card numbers, bank details or tax file numbers can result in fraud, identity theft and direct financial losses for both customers and the organisation.
- **Personal information:** Exposure of personal information such as names, addresses and other personal data may trigger regulatory fines under the *Privacy Act 1988*, as well as compensation claims from affected individuals.
- **Health information:** Disclosure of Medicare numbers or health insurance billing data may breach health or privacy laws and lead to costly remediation, regulatory penalties, loss of customers and legal action.
- **Operational business information:** Loss of trade secrets, source code or research data can cause loss of competitive advantage and financial harm through reduced market value or investor confidence.
- **Business agreements and internal documentation:** Exposure of confidential agreements, audit reports or compliance documentation can result in breach-of-contract lawsuits and fines from regulatory bodies.

Potential consequences	Examples of financial consequences in practice
The financial consequences of an adverse event can be severe and long-lasting. Examples include: **For individuals or customers:** • identity fraud or financial theft requiring costly resolution • emotional stress and loss of confidence in financial institutions or service providers. **For organisations:** • significant financial outlay to respond and recover from the event • long-term revenue loss due to customer attrition or reputational damage • difficulty securing future investment or funding • increased cost of doing business, for example audits, insurance and new controls.	• A financial services firm is targeted in a cyberattack that causes disruption to their trading platform, resulting in a loss of customer trust, financial penalties from regulators and a reduction in market value. • A technology startup has its proprietary source code leaked in a data breach, leading to the loss of competitive advantage, a decline in investor confidence and financial claims from business partners for breach of intellectual property protections.

Operational consequences

If you answer yes to any of the questions below, this may indicate potential operational consequences associated with an adverse event. A thorough risk assessment should be undertaken.

- Would the misuse, tampering, loss or theft of this data disrupt key business operations or processes?
- Could systems or staff be unable to function properly if access to this data was impacted?

Operational disruptions are interruptions to an organisation's normal operational activities caused by an adverse event. This includes the downtime of critical systems, the loss of access to essential assets required for daily operations and the diversion of staff to handle the event. These disruptions can lead to reduced productivity, service delivery failures and increased costs due to emergency response and recovery efforts. Operational consequences often lead to further consequence types.

Types of data that contribute to operational consequences and their impact

Different types of data, if compromised, can lead to significant operational disruptions. Examples include:

- **Customer service data:** Loss or corruption of customer support records can disrupt service and delay issue resolution. This can overwhelm customer support channels and support operations for both impacted and non-impacted customers.
- **Employee and HR data:** Exposure or manipulation of staffing schedules, payroll or personnel records can interfere with workforce management and internal operations.
- **Operational and logistics data:** Breaches affecting supply chain information, delivery schedules or inventory systems can halt or delay production and distribution processes.

Types of data that contribute to operational consequences and their impact

- **Business process automation data**: Compromise of automated workflow data, for example Customer Relationship Management (CRM) system inputs, can result in failed transactions and interrupted business functions.
- **IT infrastructure and configuration data:** Breaches involving administrative credentials or access logs may trigger system shutdowns or forced lockdowns and costly recovery efforts, causing significant downtime.

Potential consequences	Examples of operational damage in practice
Compromising operational data can interrupt services, damage efficiency and undermine trust. Examples include: **For individuals or customers:** • service interruptions or delays in receiving goods or support • errors in personal records, billing or communication • frustration with the reliability of services and platforms. **For organisations:** • downtime of essential services or production lines • increased costs from manual workarounds or overtime • damage to customer satisfaction and service level agreements (SLAs) • reduced capacity to respond to market or operational changes.	• A logistics company's route planning system is taken offline by a cyberattack, causing widespread delivery delays, missed deadlines and a backlog of deliveries. This results in the company not meeting contractual obligations with clients, financial penalties and reputational damage leading to the loss of key business accounts. • A financial firm's employee portal is locked down after a phishing attack compromises admin credentials, disrupting payroll processing and internal communications. This leads to compliance investigations and mandatory breach notification to regulators. • An airline suffers a data breach that impacts the flight scheduling system, prompting a temporary shutdown of check-in and flight dispatch systems. This results in compensations for impacted passengers, operational loss and widespread media scrutiny over cyber preparedness.

Strategic consequences

If you answer yes to any of the questions below, this may indicate potential strategic consequences associated with an adverse event. A thorough risk assessment should be undertaken.

- Would the compromise of this data affect the organisation's ability to achieve long-term goals or remain competitive?
- Could the compromise lead to significant changes in business strategy or offerings?

Strategic consequences refer to long-term obstructions that may impede an organisation's ability to achieve its organisational objectives. These events may compromise the competitive position, delay critical projects, or force shifts in organisational strategy. These consequences often arise from a misalignment between data management practices and strategic goals. They also result from the broader impact of the adverse event on organisational direction and reputation.

Types of data that contribute to strategic consequences and their impact
While these data types may initially pose confidentiality or reputational consequences, their cascading effects can lead to strategic consequences for the organisation. Examples include: • **Intellectual property and trade secrets**: Leaking proprietary designs, formulas or patents can erode competitive advantage and force a shift in business strategy. • **Strategic business plans and roadmaps:** Exposure of long-term plans or product development timelines can give competitors an edge and undermine future initiatives. • **Board meeting minutes and executive communications:** Leaks of internal discussions can damage trust, reveal future directions, causing reputational damage or loss of investors. • **Research and Development (R&D) data and innovation pipelines**: Loss of research data or upcoming product prototypes can delay launches, force strategic pivots and lead to competitors getting to market first.

Potential consequences	Examples of strategic consequences in practice
Strategic consequences can undermine long-term goals and damage an organisation's market position. Consequences for organisations include: • loss of strategic agility and focus • damage to brand and market perception • missed opportunities for growth or expansion • costly realignment of resources and shifting business priorities • business closure in severe cases.	• A large-scale breach forces an organisation to delay or cancel a key product launch, resulting in lost market opportunities and significant revenue shortfalls. • Loss of sensitive R&D data compromises a company's competitive advantage, allowing competitors to replicate innovations. • Investor confidence drops following a cyber incident, affecting funding and stock value, and increasing scrutiny from shareholders. • Strategic partnerships are jeopardised due to perceived weaknesses in data governance, leading to withdrawn collaborations and deterring future alliances.

Security consequences

If you answer yes to any of the questions below, this may indicate potential security consequences associated with an adverse event. A thorough risk assessment should be undertaken.

- If an adversary gains access to this data, could they use it to exploit vulnerabilities in other systems or networks?
- Would the exposed data provide adversaries with tools to launch further attacks on the organisation?

Security consequences are the result of adversaries exploiting vulnerabilities in your security systems, which have been revealed by an adverse event. This includes unauthorised access, alteration or destruction of data due to flaws in technical controls, human behaviour or system design that has been identified from the data obtained from an adverse event. It is important to clarify that security consequences focus on specific outcomes that may occur if certain data is compromised, rather than the overall risk to systems. Security compromise may put your organisation at greater risk of future attacks.

Types of data that contribute to security consequences and their impact

Different data types can lead to security related consequences if compromised. Examples include:

- **System configuration files:** Exposure of server, firewall or network configuration data can enable adversaries to identify and exploit vulnerabilities. This can potentially result in full system compromise and prolonged downtime.
- **Authentication credentials:** Leaked access credentials or tokens can allow unauthorised access to systems and sensitive information resulting in data theft, service disruptions or further infiltration across connected platforms.
- **Cryptographic keys:** Exposure of cryptographic keys can result in encrypted communications and data being decrypted or unauthorised persons impersonating authorised persons, undermining data confidentiality, trust and regulatory compliance.
- **Access control lists and privilege data:** Compromise of data describing user roles or permissions can help adversaries escalate privileges or bypass security controls. This can allow them to manipulate records and disable security safeguards.
- **Audit logs and system logs:** Logs can be deleted or altered to conceal malicious activity, hindering forensic investigations and incident response, making it harder to assess the damage or hold perpetrators accountable.
- **Vulnerability scan reports and penetration test results:** Access to this data can provide adversaries with detailed insights into known system weaknesses, making it easier to exploit vulnerabilities. This can potentially increase the chance of a successful attack in the future.

Potential consequences	Examples of security consequences in practice
Security incidents can have both immediate and long-lasting consequences for organisations. Consequences for organisations include: • delayed detection of data breaches • increased risk of repeat attacks due to exposed system vulnerabilities • high costs associated with breach recovery, remediation efforts and security upgrades • exposure to legal action and regulatory action • erosion of trust among customers, partners and investor • ongoing compromise of systems.	• A data breach uncovers unpatched systems, which adversaries later exploit in follow-up attacks. The failure to promptly address known vulnerabilities leads to ransomware deployment across systems causing operational shutdown and costly incident response. • Stolen credentials from another e-commerce site are used in 'credential-stuffing' attacks on other systems. Adversaries use the stolen usernames and passwords to compromise user accounts using the passwords across multiple system platforms, leading to data theft, data tampering and unauthorised transactions. • An organisation uses a misconfigured cloud storage to deploy software which is discovered and accessed by an adversary. The adversary injects malware into the deployable software. The malware provides a foothold for staging impersonation attempts and phishing campaigns targeting staff and clients, increasing the likelihood of further compromise and reputational damage. • Adversaries gain long-term access to internal networks of an organisation when a breach is not contained. This undetected access allows exfiltration of company strategic IT plans allowing adversaries to maintain their foothold in the company's systems.

3.5. Impact assessment

Impact refers to the severity or magnitude of potential damage, harm or loss from an adverse event. It is rated on a scale from very low to very high depending on consequences to an individual or an organisation.

It is important to note that the **likelihood** of an adverse event does not necessarily influence the **impact**. Events with a low likelihood can still result in a very high impact to the organisation.

3.5.1. Why impact assessment is important

By assessing impact, organisations recognise what adverse events they are trying to prevent and in doing so can determine the level of protection required for their data and systems. This involves organisations considering:

- potential consequences
- identifying the areas that would be affected
- rating the severity of the impact.

During the risk assessment process, organisations determine the acceptable likelihood of an adverse event based on the scale of the impact. It is advisable to check your assessment with others or a risk assessment expert to ensure that all aspects have been considered. Early identification and mitigation of risks can minimise long-term damage.

It may be useful to conduct a Privacy Impact Assessment (PIA), if you will be utilising personal or sensitive information. A PIA is a systematic assessment of a project, which can assist in identifying potential impacts that a project might have on individuals, and sets out recommendations for managing, minimising or eliminating those impacts. The OAIC has published a useful Guide to undertaking privacy impact assessments and an Impact Assessment e-learning tool.

Assessing the impact of consequences will:

- **Prepare you for the worst**
  Not all threats can be prevented, but understanding their potential consequences and impact enables you to develop effective response and recovery strategies in advance. This proactive approach minimises disruption and damage.

  For example, recognising that a ransomware attack could shut down operations for days may justify investing in more robust backup solutions.

- **Inform how the data should be classified**
  Assessments help protect sensitive and valuable information by ensuring it is appropriately handled and secured. Australian Prudential Regulation Authority's (APRA) Prudential Standard CPS 234 defines 'sensitivity' as the potential impact of a loss of confidentiality or integrity.

  For example, recognising that a data breach could lead to a significant impact will help you decide the level of required protection.

- **Help prioritise risk management efforts**
  Conducting an impact assessment highlights which consequences could cause the most damage, even if they are unlikely to occur.

  For example, the impact assessment enables organisations to focus their time, budget and resources where they can most effectively reduce the impact of adverse events.

For help determining the impact rating of your data assets if compromised, please see the impact assessment worksheet in Appendix C: Impact rating worksheet.

3.5.2. Types of impacts to consider

Understanding the types of consequences (as referenced in Risk Assessment module: Consequences of an adverse event) that can result from an adverse event is essential to accurately assess impact. The impact can be broadly categorised based on the nature and scope of the harm caused to individuals and organisations, as outlined in Table 5.

By systematically categorising these outcomes, organisations are more equipped to assess risks, better enabling them to safeguard their data.

Table 5: Categories of harmful impacts that can affect individuals and organisations

	Description	Example consequences
Harm to individuals	This refers to any negative impact on an individual or a group of individuals whose personal or sensitive information would be exposed or misused.	**Privacy** and **confidentiality** consequences including: • identity theft or fraud due to personal data exposure • psychological harm or distress • loss of privacy or dignity • physical harm or mistreatment • reputational damage to individuals.
Harm to organisational assets	This includes the loss or damage of an organisation's key resources such as data, intellectual property, systems or facilities, which could impact competitiveness and operations.	**Confidentiality** and **security** consequences including: • theft of intellectual property or confidential business plans • data loss or corruption, reducing decision-making quality • damage to IT infrastructure or networks • loss of physical devices or facilities affecting operations.
Harm to organisational operations	Refers to disruption of day-to-day business activities, impacting an organisation's ability to deliver products, services or meet internal goals efficiently.	**Operational** consequences including: • downtime or delays in critical business processes • inability to serve customers or stakeholders in a timely manner • system performance degradation • inability to restore business functions quickly after an incident.
Harm to an organisation in general	Impacts that affect an organisation's legal standing, reputation, financial stability or long-term strategic position.	**Legal**, **reputational**, **financial** and **strategic** consequences including: • legal or regulatory penalties for non-compliance • financial losses from lawsuits or fraud • loss of customer or partner trust • damage to brand and market reputation • missed business opportunities due to trust erosion.

For more information about the types of consequences, please see the Risk Assessment module: Consequences of an adverse event.

3.5.3. Impact rating scale

An **Impact Scale** measures the severity of the impact if an adverse event occurs. It typically ranges from very low (insignificant) impact to very high (catastrophic) impact. The scale in Table 6 is adapted from NIST SP 800-30 Guide for Conducting Risk Assessments.

Table 6: Impact rating scale

Impact level	What it means	Examples
Very low	Minor inconvenience to individuals or organisation	No personal or business data is leaked
Low	Minor impact with limited consequences to individuals or organisation	Commercial data leak, confidential information leak
Moderate	Noticeable impact to individuals or organisation	System outages, lost productivity, identity theft
High	Serious impact to individuals or organisation	Legal action, high-value data loss, system-wide outage
Very high	Severe, widespread, or long-term consequence to individuals or organisation	Serious physical harm or death, business closure

3.5.4. Using an impact rating table

It is important to consider the entire range of impacts that might result from potential consequences of an adverse event. Understanding your data will help determine the likely level of impact, noting impact may differ within a data type depending on the information it contains. For example, the impact of an adverse event on personal information may depend on the people represented in the data. An impact rating table is a tool to assist in determining the impact and the impact rating of an adverse event.

An impact rating table typically considers harm categories and their corresponding consequences if an adverse event occurs. It describes the severity or impact for those consequences and provides different impact ratings which an organisation can use in the data risk assessment process. For example, consideration of a particular dataset may identify a consequence as ‘identity theft’. However, on assessment the data could only be used to link a person as a customer of the retailer, with no financial loss to the person. This may be determined as a very low impact. Another dataset may be assessed as likely to result in significant theft and fraud, such as the loss of a land title. This may be determined to have a high impact.

Many larger organisations will develop and use impact rating tables to encourage consistent determination of impact. There are no universal impact rating tables and organisations can develop tables unique and specific to their situation.

For more information on different approaches to assessing impact rating, please see the NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments or the UK NCSC Risk management guidance.

Example impact rating table

This section provides a scenario which demonstrates how an impact rating table can be used. Organisations may choose to use this table as a basis to develop a bespoke comprehensive table, modifying it as appropriate.

Table 7 outlines impact ratings for a selection of different consequences for the following adverse event scenario.

Scenario

An organisation is considering the risk of a cyberattack targeting their customer database.

If successful, an adversary could gain access to data on all 2,000 customers and steal sensitive personal information such as names, addresses and bank account details (BSB and account number).

The **consequences** may include:

- **identity theft and fraud** for customers (individuals)
- **serious financial losses** due to fines and legal costs for the organisation
- **major reputational damage to the organisation** leading to a loss of customer trust in the organisation
- **operational disruption** to the organisation while systems are restored
- **possible regulatory investigations** into the organisation's operations and procedures
- damage to the organisation's relationship with financial institutions resulting in ongoing difficulty conducting financial transactions.

The organisation decides the best method for determining the impact rating of an adverse event is to use an impact rating table. They complete Table 7 with the blue cells showing its assessment of consequences and impact rating. In this example, a cyberattack is assessed to have a potentially **moderate impact** to individuals, with **very high potential impact** to the organisation itself.

Table 7: Example use of the partial impact rating table for a cyberattack scenario on an organisation's customer database

Harm category	Consequence	Impact rating				
		Very low	Low	Moderate	High	Very high
Harm to individuals	Privacy consequence: Identity theft	Minimal personal information exposed, no financial loss.	Small data exposure, minor inconvenience.	Personal data stolen, requiring resolution. For example, credit monitoring.	Major identity theft leading to fraud or significant financial loss.	Severe identity theft with long-term legal, financial or reputational damage or loss of life.
	Reputational consequence: Damage to an individual's public image or profile	Insignificant public awareness, no impact.	Minor negative perception, quickly recoverable.	Noticeable reputational damage requiring PR efforts.	Significant loss of public trust, affecting relationships.	Severe reputational harm leading to long-term loss of credibility.
	Financial consequence: Fraud	Negligible financial impact, easily reversed.	Small financial loss, recoverable.	Moderate financial loss, requiring investigation and effort to recover.	Large financial loss, impacting stability.	Devastating financial loss, potentially unrecoverable.
	Privacy consequence: Injury or loss of life	No physical impact.	Minor inconvenience or distress.	Moderate psychological harm or minor injuries.	Significant psychological distress or physical harm.	Fatalities or severe long-term harm.
Harm to organisational assets	Confidentiality consequence: Loss of intellectual property (IP)	Insignificant loss, non-sensitive IP exposed.	Minor impact, non-critical IP accessed.	Loss of moderately valuable IP, affecting competitiveness.	Loss of high-value IP, causing competitive disadvantage and loss of market position.	Critical IP lost, severely harming market position or resulting in business failure.
	Security consequence: Data integrity compromised	Minor data discrepancies, no operational impact.	Small errors requiring correction.	Moderate data integrity issues causing operational inefficiencies.	Major data corruption affecting decision-making.	Severe integrity loss leading to critical system failures.
	Confidentiality consequence: Data theft (customer or organisational data)	Insignificant data exposed, no operational impact.	Small amount of non-sensitive data leaked.	Moderate data exposure requiring remediation.	Major data breach affecting business or customers.	Large-scale data breach with severe financial, legal or reputational consequences.
Harm to organisational operations	Operational consequence: Business disruption	No disruption, quick recovery.	Minor disruption, affecting a small part of operations.	Moderate disruption, impacting efficiency or productivity.	Significant disruption, affecting core business functions.	Complete operational failure, requiring disaster recovery.
	Operational consequence: System performance degraded	No noticeable performance impact.	Minor degradation, slightly affecting efficiency.	Moderate impact, reducing system effectiveness.	Significant system slowdown, affecting critical functions.	Severe system degradation leading to operational failure.
Harm to organisation in general	Legal consequence: Regulatory non-compliance	No regulatory issues.	Minor non-compliance, easily rectified.	Moderate non-compliance, requiring intervention.	Major regulatory violations leading to fines.	Severe legal consequences, potential lawsuits, or loss of business license.
	Financial consequences: Revenue loss, production loss, fraud	Negligible financial impact.	Minor financial loss, recoverable.	Moderate financial impact, requiring budget adjustments.	Significant financial strain, affecting growth.	Catastrophic financial loss, risking insolvency.
	Reputational consequence: Damage to brand.	No reputational impact.	Minor negative perception, temporary issue.	Moderate reputational harm, requiring management efforts.	Major brand collapse, long-term reputational damage.	Irreparable reputational damage.
	Strategic consequences: Loss of competitive advantage and trust relationships.	No effects on business strategy.	Slight deviation or delay in planned initiatives.	Moderate pivot or change in market positioning.	Major strategic disruption, loss of key stakeholders.	Long-term loss of mission viability, market exit or leadership turnover

Key	Deselected impact rating	Selected impact rating

3.6. Understanding adverse events

This section provides a more detailed explanation of the concept of adverse events and outlines some common examples. These examples have been compiled from information available from the MITRE ATT&CK Matrix for Enterprise.

3.6.1. What is an adverse event?

An adverse event is an event with negative consequences to your data. There are different types of adverse events which may affect the confidentiality, integrity or availability of the data. Examples include:

- data theft, such as copying data or stealing a device (loss of **confidentiality**)
- manipulation or modification of the data within your system (loss of data **integrity**)
- deletion or encryption that makes the data inaccessible (loss of data **availability**).

An adverse event can trigger a cascade of other events, affecting an organisation across multiple levels. These events may arise at various stages of the data lifecycle, from collection to disposal. Examples of cascading events include:

- **Adverse event:** accidental sharing of client data with third parties.
    - **Cascading events:** targeted phishing of your clients using the leaked information.
- **Adverse event:** unauthorised access to a default configured network attached storage (NAS) device which reveals company security arrangements.
    - **Cascading events:** subsequent cyberattacks across your network.
- **Adverse event:** an imposter uses social engineering to obtain personal information about an employee.
    - **Cascading events:** this information is used to convince the company's IT department to reset an employee's access. They use the new authorised employee access to gain access to further data.

For more information on data breaches, please see the OAIC's What is a data breach? or ASD's What is a data breach?.

3.6.2. Different adverse events

Adverse events can be both intentional and unintentional and it is important to consider both when classifying data. Below is a non-exhaustive list of adverse event types that can compromise your organisation's data. They are grouped into three categories, *Physical*, *Authorised Person* and *Cyber*.

For help identifying potential adverse events that can occur in your data environment, please see the adverse events identification questionnaire in Appendix D: Adverse event identification questionnaire.

Physical events

Theft of devices or documents

Stolen computers, hard drives or printed documents may expose sensitive data, especially if they lack encryption or secure storage.

Unauthorised physical access

Intruders or unauthorised persons entering secure workspaces or server rooms can steal, copy or damage critical information.

‘Dumpster’ diving

Criminals and opportunists may search through discarded materials to recover printed reports, notes or storage media to find valuable or sensitive information not properly destroyed.

Tailgating

An unauthorised person enters a secure area by following an authorised employee. This often happens when someone holds the door open as a courtesy, allowing the unauthorised person to access company computers.

Authorised person events: Insider threats

Malicious insider

Employees, former employees, business associates or contractors who have legitimate access to the organisation’s systems and intentionally steal, leak, destroy or misuse data. These actions are often motivated by financial gain, revenge or espionage. This may include whistleblowers or disgruntled employees.

In some cases, employees may be manipulated or coerced by adversaries to gain access to sensitive information.

Negligent insider

Individuals who unintentionally compromise security due to carelessness, lack of security awareness or failure to follow security protocols. For example, an employee who falls for a phishing attack may have their account hijacked by adversaries, allowing access to sensitive data using stolen credentials.

Third party misuse or negligence

Vendors, suppliers or service providers with access to an organisation’s systems may misuse their access or become compromised themselves, creating a backdoor into the organisation’s systems.

Foreign ownership control and influence (FOCI)

Suppliers, vendors or service providers from other countries may be subject to extrajudicial direction, coercion, exploitation or influence from their home governments. This could allow foreign governments direct access to sensitive and critical datasets. It could also disrupt the confidentiality, integrity and availability of information systems and services, leading to widespread and harmful consequences.

For more information on FOCI risks, please see the Department of Home Affairs Foreign Ownership, Control, or Influence Risk Assessment Guidance.

Authorised person events: Human error (unintentional or accidental)

Incorrect addressing and authoring of emails or files

Sending information to the wrong recipient, by entering the wrong email address or attaching the wrong file, can lead to sensitive data being unintentionally exposed.

Improper data sharing

Sharing confidential files through unsecured channels, for example, unencrypted email or public links can make the data vulnerable to interception or uncontrolled forwarding.

System or cloud misconfiguration

Incorrectly configuring a private folder to make it publicly accessible on cloud services can unintentionally expose sensitive files to internet users.

Unpatched systems or software

Failing to install security updates allows adversaries to exploit known vulnerabilities in your systems, often without needing any user interaction.

Cyber events: Unauthorised access

Credential stuffing

Adversaries use stolen usernames and passwords, often obtained from other breaches, to gain access to systems. The risk increases when users reuse credentials or do not change them regularly across different systems.

Brute-force attacks

Adversaries use automated tools to guess passwords by trying numerous combinations until successful. This threat is heightened when credentials are weak (non-complex) or short.

Privilege escalation

An adversary or an insider exploits system vulnerabilities to gain access to data or systems beyond their authorised level.

Orphaned account abuse

Accounts belonging to former employees, contractors or vendors can pose a threat if their accounts are not disabled following their departure from the organisation.

Cyber events: Social engineering attacks

Pretexting

A social engineering method where an adversary pretends to be trustworthy, such as impersonating an IT technician or auditor, to manipulate individuals into revealing sensitive information or granting access.

Phishing

Fake emails, messages or websites designed to trick people into disclosing credentials, clicking malicious links or downloading infected files.

Cyber events: Network and system attacks

Structured Query Language (SQL) injection or command injection

These attacks exploit weak input validation in websites or applications, allowing adversaries to run unauthorised commands and potentially access or modify databases.

Domain Name System (DNS) spoofing

Adversaries redirect users from legitimate websites to fraudulent ones by tampering with how computers look up addresses online, tricking people into sharing sensitive information.

Man-in-the-middle (MitM) attacks

A form of malicious activity where the adversary secretly accesses, relays and possibly alters the communication between two parties who believe they are communicating directly with each other.

Denial of service/Distributed denial of service (DoS/DDoS)

When legitimate users are denied access to computer services (or resources), usually by overloading the service with requests. While not typically used to breach data, they can serve as a distraction during a simultaneous data breach.

Cyber events: Malware and ransomware

Trojan horses or spyware

Malicious software that appears harmless but secretly records data or creates a backdoor, allowing adversaries to access the system later.

Keyloggers

A type of spyware that covertly records everything typed on a keyboard, including passwords and personal information.

Ransomware

Malicious software that locks or encrypts files and demands payment to unlock them, often causing severe disruption to business operations.

Rootkits or backdoors

Hidden malware that allows adversaries to maintain long-term control over your systems, even if users change passwords or reboot.

For more information on cyber and authorised person event types, please see ASD's threat information.

3.6.3. Adverse events in practice

Scenario: A small healthcare clinic is subject to a data breach.

The clinic uses a common medical practice software solution to store sensitive patient data, including medical histories, prescriptions and appointment details.

Examples of adverse events that could lead to data breaches include:

- Physical event – unauthorised access

  An adversary attends the clinic and has an appointment with a medical professional. The medical professional leaves the room without locking the computer. The adversary gains access to the medical practice management software and emails patient records to their personal account.

- Authorised person event – human error

  An elderly patient is moving into aged residential living and asks for a copy of their medical records to be saved onto a USB. The medical records are saved to the USB and left at the reception desk for the patient to collect. The patient's son attends the clinic for a regular appointment and is provided with the USB containing their parent's medical records.

- Cyber event – social engineering

  The clinic receives an email that appears to be from a patient requesting their medical records are transferred to another clinic by email. The adversary follows up with a phone call providing details that indicate the person is the patient who sent the email. The clinic staff email the medical records to the email address provided by the adversary resulting in the patient's medical records being released to the adversary.

3.7. Further reading

The following resources are provided for further reading.

3.7.1. Detailed guides

- *Office of the Victorian Information Commissioner (OVIC)* *Practitioner Guide: Information Security Risk Management*

  The guide outlines the process of conducting a Security Risk Profile Assessment (SRPA), which is a critical requirement under the *Privacy and Data Protection Act 2014* (PDP Act)

- *Royal Australian College of General Practitioners (RACGP)* *Performing a threat analysis*

  Offers a detailed guide on performing a threat analysis for general practice settings. It covers how to identify potential threats to the practice's information and systems, assess the likelihood of these threats occurring and implement preventative measures to mitigate risks.

- *Cyber and Infrastructure Security Centre (CISC)* *Risk Assessment Advisory for Critical Infrastructure*

  This resource presents a condensed, six-step risk assessment methodology for assessing data storage and processing risks.

- *National Institute of Standards and Technology (NIST)* Special Publication 800-30 Revision 1 *Guide for Conducting Risk Assessments*

  This provides a comprehensive framework for conducting risk assessments and forms a key part of the NIST Risk Management Framework (RMF) used to ensure the security of US federal information systems.

- *Cyber Security Agency of Singapore* *Guide to conducting cybersecurity risk assessment for critical information infrastructure*

  This guide provides guidance on how to perform a cybersecurity risk assessment on critical information infrastructures. The scope of this guidance focuses only on the areas of risk framing, assessment and treatment.

- *UK National Cyber Security Centre* *risk management guidance*

  This website provides a detailed guide on conducting basic risk assessments and managing risks, particularly in the context of cyber security. This website was designed to help organisations, including small to medium businesses, identify, analyse and manage risks effectively.

- *Department of Finance* *Commonwealth Risk Management Framework*

  This framework provides a unified structure to help Commonwealth entities identify, assess, and manage risk in a connected and consistent way.

- *Australian Energy Market Operator (AEMO)* *Australian Energy Sector Cyber Security Framework (AESCSF)*

  This framework is a voluntary, tailored maturity-assessment framework to help energy organisations benchmark, assess, and improve their cyber resilience using both international standards and Australian-specific controls.

Tools and templates

- *ASD's Australian Cyber Security Centre Exercise in a Box*

  This website provides a platform called 'Exercise in a Box' that allows businesses and organisations to simulate various cybersecurity incidents. Exercises guide users through realistic scenarios to learn about different types of cybersecurity threats and how to respond.

- *Australian Government digital.gov.au Risk assessment and mitigation plan resource*

  These risk assessment and mitigation plan assist organisations in assessing the risk of a breach. It will help ensure that risks are identified, managed, and communicated effectively across stakeholders.

- *Australian Charities and Not-for-profits Commission (ACNC) cyber security toolkit for charities*

  ACNC offers this toolkit for charities to help them strengthen their cybersecurity practices.

- *Office of the Australian Information Commissioner (OAIC)* Guide to undertaking privacy impact assessments and Privacy Impact Assessment e-learning tool

- *New Zealand (NZ) Government Risk Assessment Process Report Template*

  This example template is from the NZ government's risk assessments for government organisations, setting up a successful risk assessment guidance. It is equally helpful for organisations to systematically identify, assess and manage risks associated with their information systems or services.

4.
Data Security Levels module

Data Security Levels (DSLs) are the primary classification of the Industry Data Classification Framework (IDCF). This module outlines the six DSLs and provides rules regarding data classified under the IDCF, an overview of various types of cyber threats and information for system administrators.

4.1. Introduction

DSLs are the foundation and the primary data classification method of the IDCF. A DSL label indicates the required level of protection for the data to ensure the desired level of confidentiality, integrity and availability is maintained. The higher the level, the stronger the protection required, with level 0 indicating no protection and level 5+ indicating extremely high protection.

If an organisation enters into an agreement which requires them to use the IDCF when handling or receiving data, they are responsible for storing the data on systems with protection levels that meet the relevant DSL guidance.

4.1.1. Key terms

The following key words and phrases are used in this module.

Table 8: Data Security Level key terms

Key term	Definition
Adverse event	An accidental or malicious event with a negative consequence that compromises the confidentiality, integrity and availability of data. A data breach is one type of adverse event. This is based on the definition in NIST SP 800-61r3.
Authorised person event	The actions of authorised people with potential to cause an adverse event, for example, error or accident, social engineering, user focused cyber-events (phishing, unauthorised software), intentionally embedded employees and blackmail.
Cyber event	Cyber (including network) actions with potential to cause an adverse event. **Common cyber event**: A transitory cyber event that utilises common techniques against published vulnerabilities. For example, exploitation of a well-known vulnerability in unpatched software (including operating systems). **Moderate cyber event**: An intentional cyber event over a short period (days) that utilises less common and/or targeted techniques. For example, identifying, targeting, profiling and engaging an employee with customised content to manipulate them to provide credentials or perform compromising actions. **Complex cyber event**: An intentional cyber event, possibly over an extended period (months or years). Significant effort is invested to achieve a specific aim, using highly skilled methods, and/or developing new techniques. For example, placing hidden entry points (backdoors) in software that will be used by an organisation. This entry point is later used to bypass standard security controls and gain unauthorised access to a system or application.
Data breach	The unauthorised movement or disclosure of sensitive private or business information, including personal information under the *Privacy Act 1988.* For more information see ASD's glossary and information on data breaches.
Event	An action, occurrence or change involving data that may cause an impact.
Event likelihood	The chance or probability, expressed qualitatively, of an event resulting in an adverse event.

Key term	Definition
Label	A visible indicator in physical or electronic form applied to data to communicate its DSL classification.
Labelling	The process of applying a label to data.
Likelihood of an adverse event	Technically this is the probability (qualitatively) of an event resulting in negative consequences (an adverse event). It is independent of the probability of the event. If an organisation experiences a higher frequences of events, the frequency of adverse events may increase.
Physical event	Physical actions with potential to cause an adverse event. For example, theft, fire, physical access and the installation of unauthorised devices.
Protection/protective security	A combination of physical and cyber security measures to reduce the likelihood of an adverse event.
Risk appetite	The amount of risk an organisation is willing to accept or retain in order to achieve its objectives. This is based on the definition in the PSPF which is derived from the Department of Finance Element 2: Risk Management Framework.
Security	When unqualified (no description of the type of security, for example 'national' security), it is an abbreviation for protective security as defined above.

4.1.2. About Data Security Levels

A DSL:

1. communicates the protection required to reduce the likelihood of adverse events
2. reflects an assessment of inherent risk in the data and the organisation's chosen protection level.

Data owners typically classify data at a DSL by considering the protection required for event type (discussed below). They reflect the likelihood accepted by an organisation of an adverse event involving that data. The assessed risk is based on the consequences, impact and likelihood of adverse events as well as the nature of the data. A DSL must be applied for data to be considered classified under the IDCF.

Data must be stored and used in an environment that meets or exceeds the specified level of protection. The required controls to maintain that level of protection may change over time.

4.2. Events

An event is an action, occurrence or change involving the data that may cause an impact. Events are considered under three categories of physical, cyber and authorised person events.

4.2.1. Physical event

A physical event is an event that involves a physical action. It could be an action by a person, including an adversary or authorised person, for example, theft of devices. It could also be naturally occurring events such as flood or fire which may cause data to become unavailable.

4.2.2. Cyber events

A cyber event is an event that generally occurs or is initiated through a device, system or network, or other remote electronic means. A person may still be involved but the actions do not require physical presence with the device or system. Cyber events are split into three subtypes as defined in the glossary and discussed below.

DSLs reflect the level of protection required to reduce the likelihood of an adverse event to a level accepted by an organisation. Because there is a broad range of cyber threats, the IDCF considers cyber threat events by their complexity and general frequency.

- Common cyber events are frequent threats, often encountered daily.
- Moderate cyber events are less common, require greater technical skill and resources to execute, and are harder to prevent.
- Complex cyber events are highly sophisticated and often involve planning, advanced techniques and coordinated efforts. They are harder to prevent or detect but are less likely to be attempted.

It is important to note that both technology and adversary capabilities evolve rapidly in this field. The examples provided below are not exhaustive and reflect the state of play as of 2025. Readers should regularly review their understanding of advice to stay current. Additionally, it is also important to recognise that a specific organisation may experience higher frequency of moderate or complex cyber events.

Common cyber event

Description

Many common cyber events are opportunistic and non-targeted. Adversaries typically launch them at scale across multiple organisations using pre-written scripts or automated tools, requiring minimal effort. These threat events target unsuspecting users or published vulnerabilities of systems that lack basic security protections. Attempts often occur daily.

Examples

- Unpatched software exploits: Exploiting well-known, published vulnerabilities in network devices, applications or operation systems.
- Credential-based attacks: Involving the use of stolen or orphaned, enabled accounts without an active owner, username-password combinations, or brute force attack on commonly used passwords. These attacks can target accounts belonging to standard users or administrators.
- Common social engineering: Opportunistic targeting of users with fake messages or website pop-ups. This includes email attacks through spam and phishing techniques. They often lead to threats like ransomware, spyware or joining computers to larger networks of computers (botnets) conducting further exploits.
- Drive-by download: A user unintentionally downloads malicious code simply by visiting a compromised website. No interaction or clicking is required.
- Network port scanning for vulnerabilities: Remotely scanning any device directly connected to the internet, including an organisation's internet router, firewall, web server or service Application Programming Interface (API) for weaknesses to exploit.

Moderate cyber event

Description

Moderate cyber events are harder to detect and prevent than common ones. Adversaries invest more time and resources to achieve specific objectives, often targeting organisations or industries. They use stealthier, customised tools and techniques, although some attacks may still occur randomly or in a non-targeted manner.

Examples

- Privilege escalation: Exploiting flaws in the system to escalate account privileges to access sensitive data, infiltrate additional systems and conceal malicious activities.
- Living off the land: Leveraging legitimate software, for example PowerShell, bash, cron and rundll32.exe or other system tools, to carry out malicious actions. These are often entirely in memory to evade detection by traditional security measures.
- Targeted social engineering: Attempting to identify, profile and engage a targeted individual to manipulate them. For example, manipulating an employee with customised content leading them to provide credentials or perform compromising actions, through fake websites or malicious macros. This includes tactics like spear phishing and whaling.
- Impersonation: Simple targeted impersonation to reset passwords of individuals or porting a mobile service to a SIM card that will be controlled by an adversary are ways they might seek to gain authorised user's credentials.
- Denial-of-service attacks: Disrupting the normal operation of a system, application or network by overloading its resources or exploiting vulnerabilities, thereby preventing legitimate users from accessing the services.
- Network traffic exploits: Exploiting known vulnerabilities in the network layer to intercept, redirect or manipulate data in transit. Techniques such as man-in-the-middle attacks and 'DNS spoofing' exploit lack of encryption or weakness in protocol design, allowing adversaries to eavesdrop on or alter communications.

Complex cyber event

Description

Complex cyber events are highly targeted, strategic attacks often carried out by well-funded, highly skilled adversaries. Motivations vary and are often unpredictable. These operations involve extensive planning, advanced techniques and customised tools, unfolding over months or even years**.**

Examples

- Supply chain attacks: By compromising trusted third-party components, for example software updates, libraries or AI models, before they are deployed by the targeted organisation, an adversary can infiltrate the targeted systems through seemingly legitimate means.
- Zero-day exploits: Exploiting software vulnerabilities that are known only to adversaries to gain access to systems or data. These exploits are unknown to the software vendor or developer, security specialists or the public at the time of the attack. No patch or fix exists.
- Backdoor attacks: Use of hidden entry point, created intentionally or unintentionally left open, to bypass standard security controls and gain unauthorised access to a system or application.
- Deepfake social engineering: Using AI-generated audio, video, or images to impersonate trusted individuals to deceive targets to provide credentials or perform harmful actions.
- Advanced Persistent Threat (APT): A type of structured, prolonged and multi-stage cyber-attack typically carried out by state-sponsored or well-funded adversaries. Their objective is to maintain long-term, undetected access to targeted systems for espionage, data theft and sabotage.

4.2.3. Authorised person event

An authorised person event is an event caused by a person who is permitted access to the data. It could be accidental or intentional.

4.2.4. About the detailed event model

This module primarily presents the DSLs in terms of the minimum level of protection required to reduce risk to an organisation. The DSL represents the required protection controls to ensure the likelihood of an adverse event is reduced to a level accepted by the organisation.

It is likely that the required level of protection will need to increase over time in response to the evolving threat environment.

For example, an organisation wants to reduce the likelihood that a phishing email, a common cyber event, will result in negative consequences**.** It requires **very high** controls against common cyber events. These controls should protect against a phishing email, ensuring that the likelihood of the email getting through spam filters **and** the recipient acting on the email to trigger an adverse event is **very low**.

Over time, phishing emails may evolve to evade current filters. The likelihood the email will get through the filters and cause negative consequences will increase beyond the **very low** threshold. This means the required level of protection will need to be increased to ensure the evolving threat of phishing emails is maintained at a **very low** likelihood. The practical implementation requirements of '**very high**' protection may increase or change over time.

More information on specific DSL event models is included in the relevant subsections.

4.3. DSL overview

Table 9 outlines the level of protection required for each DSL for various types of adverse events. It demonstrates the link between a DSL and its associated level of required protection. For example, data classified at DSL-0 has **very low protection** requirements. This means that the organisation accepts that there is a **very high likelihood** of an adverse event.

Table 9: Protection level requirements for each Data Security Level (DSL) by types of adverse events

Data Security Level	Protection level requirements				
	Physical	Cyber			Authorised person
		Common	Moderate	Complex	
DSL-0	Very low	Very low	Very low	Very low	Very low
DSL-1	Medium	Very low	Very low	Very low	Low
DSL-2	Medium	High	Medium	Low	Medium
DSL-3	High	Very high	High	Medium	High
DSL-4	Very high	Very high	Very high	High	Very high
DSL-5+	As agreed between parties.				

As illustrated in Figure 6, a higher DSL indicates a greater level of required protection against an adverse event, regardless of its type. This results in a lower likelihood of an event becoming an adverse event.

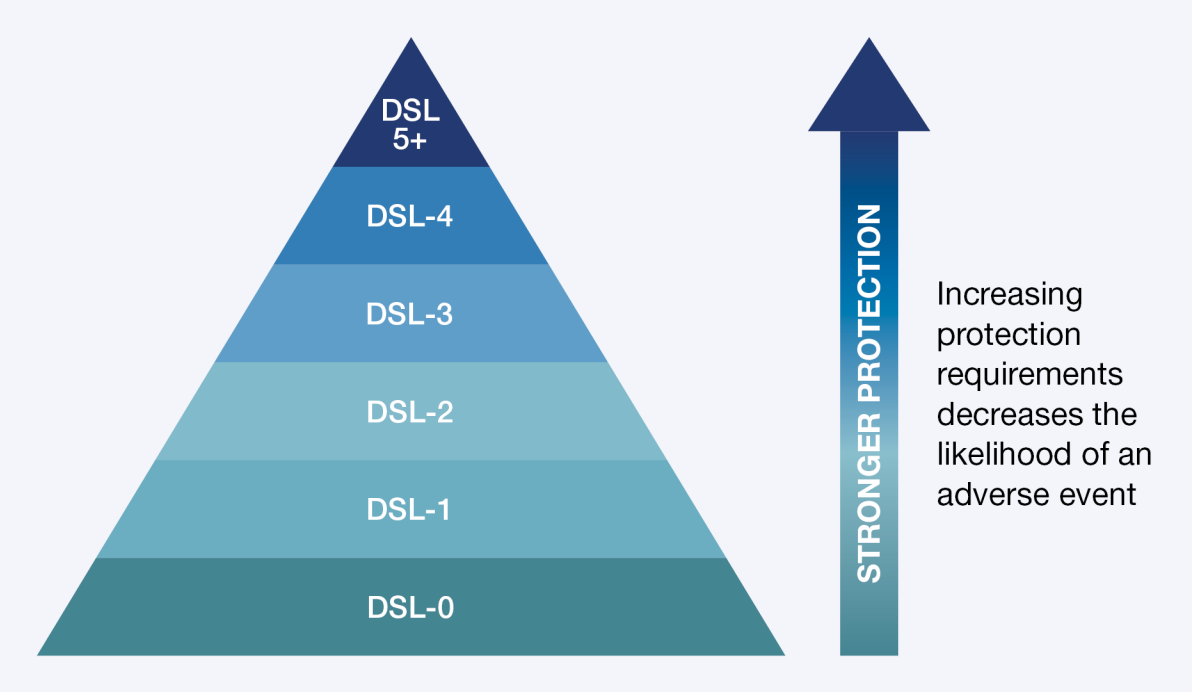

Figure 6: Relationship between Data Security Level (DSL), the protection requirements and the likelihood of an adverse event

For more examples of DSLs in operation, please see the IDCF website.

4.4. Selecting a DSL classification for data

A DSL label can be applied to communicate the level of protection required for data. Organisations will choose the appropriate DSL based on:

- the level of inherent risk, potential impact or potential harm from the data
- their risk appetite and level of acceptable risk for the organisation
- a balance of risk against return on investment or ability to do business.

The IDCF provides guidance on risk assessment to help organisations identify impact and harm. Organisations may use this guidance to help them to determine the appropriate DSL for data. Organisations can use alternative risk assessment processes or existing organisational policy to decide the level of protection required. The level of protection is chosen to reduce the likelihood of an adverse event to a level accepted by the organisation.

This module provides examples in which a DSL is applied to data based on a moderate risk appetite. Organisations with higher or lower risk appetite may choose to classify similar data at a lower or higher DSL respectively.

For more information on risk assessment, please see the Risk Assessment module.

4.5. Appropriate systems and environments

The IDCF does not prescribe specific controls to protect data at each DSL. This gives organisations the freedom to choose their preferred controls and methods in meeting the DSL protection levels.

The choice of controls should be **equivalent** to the levels provided by the proposed standards listed below and as suggested against each DSL.

As the IDCF may be used in relationship with other organisations, any system owner claiming system alignment with a DSL must provide assurance that it meets the appropriate data security level requirements to parties concerned. It is a data owner's responsibility to seek assurance that the data recipient's systems meet the requirements for the assigned DSL. This might occur through a statement of system security implementation that is recommended as part of the IDCF and a data sharing agreement.

The requirement for DSL classified data to be stored in appropriate systems always applies. This includes when data is transferred or communicated between systems. When data is transferred, the devices or systems being used to transfer the data must also have appropriate protections for the DSL of the data.

For an example statement of system security, please see the DSL module: Statement of system security.

For more information on communication and the movement of data, please see the DSL module: Communication and movement of data.

4.5.1. Related cyber security frameworks and standards

Australian Signals Directorate guidance

Most security frameworks begin with a minimal security baseline and organisations may apply more mature controls as needed within their operational contexts. DSL-0 reflects baseline of cyber security settings, whereas DSL-5+ reflects the most mature cyber security controls under the IDCF.

ASD produces the Information security manual (ISM), which is a cybersecurity framework that an organisation can apply, using their risk management framework, to protect their information technology and operational technology systems, applications, and data from cyberthreats. The ISM is intended for chief information security officers, chief information officers, cybersecurity professionals and information technology managers.

ASD has developed prioritised cyber risk mitigation strategies, in the form of the strategies to mitigate cybersecurity incidents, to help organisations protect themselves against various cyberthreats. The most accessible of these mitigation strategies are the Essential Eight.

The ASD's Essential Eight framework focuses on cyber security controls. Systems that have successfully implemented and are maintained at the Essential Eight maturity level listed against each DSL section and at Table 16 would meet the appropriate cyber requirements.

For ASD's comparison of maturity levels, please see the Essential Eight maturity model Appendix D: Comparison of maturity levels.

Center for Internet Security Critical Security controls

Center for Internet Security Critical Security Controls (CIS) are a prescriptive, prioritised and simplified set of best practices that can be used to strengthen an organisations cybersecurity posture. Cybersecurity practitioners from around the world use the CIS Controls and/or contribute to their development via a community consensus process. The CIS controls are organised into three Implement Groups and are designed to help organisations prioritise security controls based on their

needs. These controls are regularly updated to remain effective in modern computing environments, such as cloud-based computing, virtualisation, and remote working arrangements.

Protective Security Policy Framework

The Protective Security Policy Framework (PSPF) is the protective classification framework used within Australian Government non-corporate Commonwealth entities. It is also used by some corporate Commonwealth entities, adapted by many Australian state governments, and used by some industries when dealing with government. The IDCF seeks to provide some alignment with the PSPF, serving as good guidance on the protection requirements for DSL-3 and DSL-4, and for physical protections across other DSLs.

It is important to note that the PSPF is designed for government and is based on an assessment of the value, importance or sensitivity of the information by considering the potential damage that would arise if the information's confidentiality was compromised and assigning the corresponding protective marking or security classification. This is done in accordance with PSPF Requirement 0036 that requires the Accountable Authority of each non-corporate Commonwealth entity to determine their entity's tolerance for security risks. Ongoing access to the designated security classification requires the commensurate security clearance. In contrast, DSLs focus **only on the level of protective security controls needed**. The DSLs do not directly reflect national security or business impact.

The PSPF also outlines physical security zones that are suitable for 'OFFICIAL: Sensitive' and 'PROTECTED'. The description of these security zones provides detailed guidance for physical controls appropriate for DSL-3 and DSL-4, respectively. Organisations are encouraged to consult a qualified cyber security professional or an Infosec Registered Assessors Program (IRAP) Assessor to ensure their systems have appropriate controls implemented.

Cloud based services including productivity suites

Cloud service providers offer guidance on implementing appropriate levels of security that align with industry standards. Under their shared responsibility model, providers manage the security of the cloud infrastructure, while users are responsible for the security configurations of their cloud instances. It is essential for users to ensure that appropriate security options are selected to meet their specific security requirements.

Below is a list of major cloud service providers.

- Microsoft 365
  - **Microsoft guide** provides detailed guidance on configuring cloud options to meet the Maturity Levels of the Essential Eight.
- Google Workspace
  - Google Workspace environments can be secured by implementing appropriate controls from the **CIS Google Workspace Benchmarks**.
- Amazon Web Services
  - AWS Cloud Adoption Framework (CAF) offers a structured approach to cloud service adoption and includes a **Security Maturity Model**. This enables customers to assess and improve their security posture.
- Windows 365
  - Windows 365 is a Desktop-as-a-Service (DaaS) that enables the creation of Cloud PCs compliant for holding data with the PSPF PROTECTED classification, refer to **Microsoft's Configuration guidance for Windows 365**. Compared with traditional laptop environments, it offers enhanced security by reducing the risk on events related to unauthorised physical access to the data. It enforces zero trust security principles, refer to **ASD's Foundations for modern defensible architecture**, and integrated security measures such as multi-factor authentication (MFA) and data loss protection (DLP).

For more information on configuration, please see the relevant DSL in the DSL module: Data Security Levels.

4.6. Absence of a DSL label

The absence of a DSL label means the data is unclassified and is an indication that a risk assessment has not been conducted for the data under the IDCF. It also means the data does not default to being classified at DSL-0.

Data without a DSL label should be handled according to organisation policy. Organisations using the IDCF will have undertaken a risk assessment and applied a DSL label to the data.

4.7. Data Security Levels

The following sections describe each DSL and give examples of the types of data you may classify at a DSL. They also explain the risk profiles in relation to adverse events. While the IDCF does not prescribe specific controls for protecting data at each DSL, it provides examples of appropriate systems and environments to meet the required protection level.

4.7.1. DSL-0: Data Security Level 0

DSL-0 represents the **lowest** data security level. Data classified at DSL-0 requires **very low** protection measures against physical, cyber or authorised person events. It has been assessed by an organisation to have little or no confidentiality, integrity or availability concerns.

Data classified at DSL-0 does not need any deliberate or planned protection, however regular security practices, such as locking of devices or placing devices in unobtrusive places, should still occur. While any system is suitable for handling DSL-0 data, this classification does not automatically make the data suitable for public release and is not permission to do so. The lack of protection requirements is likely to result in the data becoming readily available and organisations accept there is a **very high likelihood** of an adverse event.

DSL-0 might be used for copies of data where confidentiality is not required. The original data may be classified at a higher DSL to maintain integrity and availability while copies are classified at DSL-0 to indicate the copy carries low risk. For example, the original version of a publication is stored securely in an organisation's computing facilities with a DSL-2 label but with a DSL-0 labelled copy emailed to stakeholders.

It is important to note that the DSL-0 label indicates the minimum requirements of protection. DSL-0 data will often be held in systems with some controls.

Table 10 provides a summary of the protection levels required for adverse event types under DSL-0. For many organisations, this classification may be appropriate for data suitable for public release.

Table 10: DSL-0 protection level requirements by types of adverse events and potential data types

Data Security Level	Protection level requirements				
	Physical	Cyber			Authorised person
		Common	Moderate	Complex	
DSL-0	Very low	Very low	Very low	Very low	Very low
Potential Data Types	Based on an organisation with a **moderate tolerance of risk**, the following are examples of data that might be classified at DSL-0. • Publicly available information about an organisation, such as contact details, websites, social media data and Australian Business Number (ABN). • Publications of an organisation such as annual reports, media releases, product catalogues and service outage alerts. • Open-source software and documentation like public GitHub repositories, licence agreements and developer guides. • AI models that have been publicly released for use and customisation. • Research datasets associated with a publication where the data must also be published.				

Detailed event model

Likelihoods of each event type under DSL-0 are discussed below.

Physical events

No protection is required to prevent physical access to data and systems, making unauthorised access highly likely if the data is stored at this minimum. DSL-0 classified data can be disclosed through printed materials, accessed through unattended hardware, or through opportunistic or targeted theft. There is also no consequence if this type of data is unavailable during a system downtime. A physical event has a **very high likelihood** of impacting confidentiality, integrity and/or availability.

Cyber events

No intentional cyber protection is applied and access to data might be readily available through the network. This means there is a potential for data to be modified without authorisation, impacting its integrity. There is potential for the data to become unavailable and the organisation has determined this is an acceptable risk. The data may be discovered by search engines or shared links. A cyber event has a **very high likelihood** of impacting confidentiality, integrity and/or availability.

Authorised person events

DSL-0 classified data does not need to be under the control of an authorised person. However, in most organisations, data will likely be controlled by an authorised person regardless of the DSL label applied. DSL-0 indicates there is no concern regarding unauthorised access to the data and the distinction between authorised and unauthorised persons has no significance. There is a **very high likelihood** that any persons with minimal skills will be able to access and/or modify the data in these systems. An authorised person event has a **very high likelihood** of impacting confidentiality, integrity and/or availability.

For more information on the IDCF's detailed event model, please see the DSL module: Events.

Appropriate systems and environments at DSL-0

DSL-0 classified data requires **very low** protection and can be handled in any system or environment.

Essential Eight Maturity Level 0 - Cyber controls

- A system at Maturity Level 0 is acceptable for hosting data classified at DSL-0.

Protective Security Policy Framework (PSPF)

- DSL-0 has no direct parallel in the PSPF.

Configuring common systems

Mobile devices

- Mobile devices, such as laptops, mobile phones and portable storage devices are not required to have login/password protection.
- Data classified at DSL-0 can be kept on devices as clear text or in unencrypted files.

Access controls and users

- Access controls or user restrictions do not need to be applied when accessing DSL-0 classified data.

Users

- Users can access DSL-0 classified data anytime, from anywhere and without training.
- No specific authorisation is required however users are expected to understand the IDCF and their broader obligations.
- There are no protection measures preventing users from modifying or disposing of the data.

4.7.2. DSL-1: Data Security Level 1

DSL-1 is a **very low** security level with a focus on physical security protections. Data classified at DSL-1 has been assessed by an organisation to require minimal protection. It has **very low** cyber protection requirements, though cyber protection may still be utilised.

Generally, DSL-1 is not a level considered suitable for day-to-day business. Only physical and authorised person events are purposefully controlled. Other events, such as everyday cyber events, are not directly controlled and remain unaddressed, resulting in a **very high likelihood** of an adverse event.

Data classified at DSL-1 requires controls that protect against opportunistic physical events, such as casual theft, but not against targeted attacks or attacks by highly motivated adversaries. It requires little to no protection for planned physical or cyber events. DSL-1 requires minimal oversight of authorised persons, except to ensure that those in physical possession of a device are approved by the organisation and aware of basic physical security. DSL-1 classified data is likely to have very low impact if confidentiality or integrity is breached. The availability of this data is the highest concern but can be compromised through the loss of the physical storage device or system.

Most systems and devices can be managed to suit DSL-1 classified data. A focus on simple physical controls with a **low** level of requirement means even a USB storage device can meet these protection requirements. However, as a low effort level of protection, systems or devices designed only for DSL-1 carry significant risk. Organisations should be extremely careful if they have accepted to carry this level of risk in their day-to-day operations.

Table 11 provides a summary of the protection levels required for adverse event types under DSL-1. For many organisations, this classification may be appropriate for an encrypted copy of data (excluding the encryption key), some hardcopy originals and small quantities of low sensitivity data.

Table 11: DSL-1 protection level requirements by types of adverse events and potential data types

Data Security Level	Protection level requirements				
	Physical	Cyber			Authorised person
		Common	Moderate	Complex	
DSL-1	Medium	Very low	Very low	Very low	Low
Potential Data Types	Based on an organisation with a **moderate tolerance of risk** the following are examples of data that might be classified at DSL-1. • A copy of public data that has value because of the resources invested in collecting it. • Encrypted data excluding the encryption key. • Data soon to be released to the public. • Small quantities of low sensitivity data. Note that data in encrypted form without the encryption key, may be classified at DSL-1. This does not imply the data, when decrypted, would also be DSL-1.				

For more information on classifying data containers, please see the DSL module: Classifying data containers.

Detailed event model

Likelihoods of each event type under DSL-1 are discussed below.

Physical events

Controlling physical access to data and systems seeks to minimise physical events to hardware by opportunistic adversaries. For example, a physical event can include theft, accidentally leaving a laptop or USB storage device in a public space, or someone adding an unauthorised device to your office.

In cases where the environment may not prevent access to devices by unauthorised persons, other measures should be in place to control physical access. For example, a laptop removed from the security of the office or home might be kept in the possession of an authorised person or in a locked bag. Authorised persons are trusted with physical access to devices. DSL-1 may not protect against a planned theft.

Overall, the controls should ensure a **medium likelihood** of an event resulting in negative consequences.

Cyber events

Cyber protection is not required. The organisation accepts that all cyber event types have a **very high likelihood** of resulting in negative consequences. For example, a laptop or a mobile phone holding only DSL-1 data does not require any cyber controls and there is a **very high likelihood** that the device will be compromised if a cyber event occurs.

Authorised person events

Any physical access to a device holding data should be restricted to authorised users who are trusted and trained to maintain the physical security of the data. Devices that hold DSL-1 classified data are expected to be handled the same as a personal mobile phone.

For more information on the IDCF's detailed event model, please see the DSL module: Events.

Appropriate systems and environments

DSL-1 classified data has **very low** cyber protection requirements. There are no standards, frameworks or guides related to cyber controls. It is anticipated that devices suitable for DSL-1 would be always in the possession of an authorised person or located in a secure location such as a locked drawer or premises.

Essential Eight Maturity Level 0 - Cyber controls

- A system at Maturity Level 0 is acceptable for hosting data classified at DSL-1 **provided the physical protection requirements are met**.

Protective Security Policy Framework (PSPF)

- DSL-1 has no direct parallel in the PSPF.
- Section 24 of the PSPF, Security Zone 2 (entity office area) provides good guidance on physical controls.

Configuring common systems

Mobile devices

- Mobile devices, such as laptops, mobile phones and portable storage devices should be in possession of an authorised user and stored securely when unattended.

Cloud based services

- Most cloud services provide physical protections that meet DSL-1.

Access controls and users

DSL-1 access control is entirely physical. Possession of the device should be restricted to authorised users. Once physical access is gained, the data could be readily available.

Users

- Users (staff) should be aware of their obligations under DSL-1 to keep devices safe. This includes:
- ensuring devices remain in their possession or unattended devices are in a secure environment, such as a locked drawer or known location in a secured building
- preventing accidental loss, such as leaving the device somewhere.

4.7.3. DSL-2: Data Security Level 2

DSL-2 is a **low** to **medium** security classification for data. DSL-2 data requires protection controls to be implemented for cyber and authorised person events. DSL-2 requires controls that protect against opportunistic threat events rather than targeted or highly motivated threat events. DSL-2 provides little protection for targeted planned events.

Most organisations should be able to implement systems appropriate for DSL-2 classified data. Regular review of systems and user proficiency is required to ensure protection is maintained. DSL-2 systems may be appropriate for daily use. For example, where an organisation holds data that is not sensitive, confidential, or which has low business impact. It is the responsibility of the data owner to conduct a risk assessment on the data to decide whether DSL-2 is an appropriate classification. Adopting DSL-2 balances risk and cost when compared to implementing higher DSLs.

Table 12 provides a summary of the protection levels required for event types under DSL-2. For many organisations, this classification may be appropriate for non-sensitive data.

Table 12: DSL-2 protection level requirements by types of adverse events and potential data types

Data Security Level	Protection level requirements				
	Physical	Cyber			Authorised person
		Common	Moderate	Complex	
DSL-2	Medium	High	Medium	Low	Medium
Potential Data Types	Based on an organisation with a **moderate tolerance of risk**, the following are examples of data that might be classified at DSL-2. • Regular business correspondence such as daily emails and meeting agendas. • Financial information such as general expense receipts and some internal budgets. • Draft reports of a general nature. • Internal general staff communication. • Internal organisational policy.				

Detailed event model

The DSL-2 event model builds on and includes the event model of DSL-1. Likelihoods of each event type under DSL-2 are discussed below.

Physical events

Controlling physical access to data and systems seeks to minimise physical events to hardware by opportunistic adversaries. Physical access threats are mitigated by ensuring unauthorised individuals are unlikely to achieve physical access. In cases where physical measures may not prevent access, such as a mobile device, other measures should be in place to prevent access to data when the device is powered off or locked. Unlocked, powered on devices must have physical measures in place, such as the protection provided by the presence of an authorised person. Authorised persons are generally trusted with physical access to devices, whereas unauthorised persons are not trusted with physical access to devices.

Overall, there is a **medium likelihood** a physical event will result in negative consequences. An organisation's use of DSL-2 is an acceptance by the organisation of this likelihood for a physical adverse event.

Cyber events

To understand cyber events at DSL-2, the IDCF draws from ASD's Essential Eight's Maturity Level 1. Any cyber event which is in scope of Essential Eight's Maturity Level 1 should be controlled. Maturity Level 1 is described as:

> The focus of this maturity level is malicious actors who are content to simply leverage commodity tradecraft that is widely available in order to gain access to, and likely control of, a system. For example, malicious actors opportunistically using a publicly-available exploit for a vulnerability in an online service which had not been patched, or authenticating to an online service using credentials that were stolen, reused, brute forced or guessed.
>
> Generally, malicious actors are looking for any victim rather than a specific victim and will opportunistically seek common weaknesses in many targets rather than investing heavily in gaining access to a specific target. Malicious actors will employ common social engineering techniques to trick users into weakening the security of a system and launch malicious applications. If user accounts that malicious actors compromise have special privileges they will exploit it. Depending on their intent, malicious actors may also destroy data (including backups).

While the IDCF defines cyber events using Essential Eight, implementation of controls can be drawn from any other equivalent sources. The IDCF uses the term adversaries to refer to the Essential Eight's malicious actors.

This maturity level focuses on cyber controls that may protect against **common cyber events** but focusses less on **moderate** and **complex cyber events**. As such, controls should reduce the likelihood of **common**, **moderate** and **complex cyber events** resulting in consequences to **low**, **medium** and **high** respectively.

Authorised person events

Any access, both physical and cyber, to the data should be:

- restricted to authorised users
- on a need-to-know basis. Access may be managed at a group level.

An organisation may want to consider the risk and cost of implementing access controls.

Where physical access is difficult to control, protections should be implemented to maintain authorised person access only. This will ensure that there is a **medium likelihood** that an unauthorised person would be able to access the data on a device that is powered off or locked.

All authorised persons should be trained in basic data and device handling principles. The training should also cover the management of common cyber risks, including those related to email, the use of portable data devices and the importance of regular system updates. Annual refresher training should be considered.

For more information on the IDCF's detailed event model, please see the DSL module: Events.

Appropriate systems and environments

The IDCF provides a non-exhaustive list of guidelines and examples that are suitable for DSL-2. These guides and examples inform the kinds of controls required for the level of protection for DSL-2. The IDCF does not define specific systems and environments suitable for mitigating DSL-2 threats.

Standards, frameworks and guide examples

Approaches that currently meet the protection requirements and associated likelihoods of DSL-2 are listed below. Each approach offers benefits and has potential risks and should be used as a guide only. It is important to note that there are other standards and frameworks which offer guidance on implementing security that meets the desired protection levels of Table 12. Organisations may use compensating and alternate controls, providing that they can demonstrate that the combined controls meet the required protection level of DSL-2.

Essential Eight Maturity Level 1 - Cyber controls

- A system at Maturity Level 1 is acceptable for hosting data classified at DSL-2 provided **physical and authorised person controls are also met**.

Protective Security Policy Framework (PSPF)

- DSL-2 has no direct parallel in the PSPF.
- Section 24 of the PSPF, Security Zone 2 (entity office area) provides good guidance on physical controls.

Center for Internet Security (with appropriate physical controls)

- The use of **CIS Controls Implementation Group 1 (IG1)** in enterprise Information Security Management Systems (ISMS) that implement ISO 27001 or the NIST Cybersecurity Framework are considered acceptable for meeting the cyber security requirements of DSL-2.

For further details on CIS Controls, please see CIS Critical Security Controls V8.1.

To evaluate system configurations, consider the use of CIS-CAT® assessment tool.

Configuring common systems

Laptop and desktop

Physical controls would include:

- encrypted filesystems that are unlocked by either secured hardware or user password, such as Bitlocker™ for Windows™ or FileVault™ on MacOS™. This is to ensure that if someone gained physical access to the data storage device, it would be unlikely they would be successful in extracting data.

Cyber controls would include:

- regular software updates
- strong passwords
- multifactor authentication.

A physically secure desktop may not need the encrypted filesystem controls for DSL-2 as the physical controls may provide an adequate substitute. However, they may be adopted as good practice.

Cloud based services including productivity suites

Generally, the listed cloud-based services will:

- provide sufficient physical protections
- require configuration of cyber protections
- require organisations to manage user access.

Microsoft 365

- By following the Microsoft Guide for implementing Maturity Level 1 of the Essential Eight, Microsoft 365 can be configured to have DSL-2 appropriate cyber controls.

Google Workspace

- By implementing the **IG1 controls** outlined in the CIS Google Workspace Benchmark, organisations can configure their Google Workspace to have DSL-2 appropriate cyber controls.

Amazon Web Services

- Cloud services aligned with Phase 1: Quick Wins of CAF Capability have appropriate cyber controls for hosting DSL-2 classified data.

Access controls and users

The more users with access to the data, the greater the attack surface area. Although authorised users are generally trusted, DSL-2 accepts a **medium** likelihood of an adverse event through authorised users. While 'need-to-know' is the preferred principle for data access and control, DSL-2 allows for security approaches such as having broader access enabled to larger groups with a potential need-to-know. DSL-2 allows a less detailed approach to access control and restriction of users, based on an organisation's risk appetite.

For example, a personal assistant in a small organisation might have access to personnel data so staff can be contacted in an emergency or a receptionist might have general access to the entire client database to allow contact as needed.

In general, the effort applied to maintaining appropriate access controls is lower for the organisation and may impact the speed of updates in access control. For example, removal of access when people change teams or roles may be a lower priority, resulting in users maintaining unrequired access when they no longer have a need-to-know. There is also little or no concern regarding the risk of system administrators being able to access the data.

Users

Users and staff are a potential vulnerability in a system and organisations should take steps to ensure staff do not contribute to adverse events. DSL-2 tolerates a **medium likelihood** of an authorised person's actions resulting in an adverse event. DSL-2 permits **medium risk**, allowing a balance between staff training and the time and cost involved. This aspect of management relies on doing what is practical and achievable, rather than aiming for a strict benchmark.

Need-to-know – may-need-to-know

- 'Need-to-know' is the ideal principle, however a 'may-need-to-know' approach is accepted.
- This approach to data access offers flexibility across an organisation to allow individuals access to data when they 'may-need-to-know'.
- Allowing more users access to data that is not required for their role increases the risk and leads to a **medium risk** level.

Training and compliance

Many systems and applications do not have security controls in place to enforce protection, increasing the likelihood of a security breach due to a lack of staff training and awareness. For example, a staff member may copy business data to a USB storage device to work on at home using their personal computer, sync a work cloud to a home computer or accidentally email the incorrect file.

This risk is expected to be managed in systems utilised for DSL-2 classified data by providing staff with general training and awareness of good data practices and common cybersecurity threats. A DSL-2 system is unlikely to have built in user prevention mechanisms to stop user actions that may result in an adverse event being successful.

4.7.4. DSL-3: Data Security Level 3

DSL-3 classification is a medium level security classification for data. Data classified at DSL-3 requires controls that protect against regular, untargeted and opportunistic events with at least **high** protection against all events except complex cyber events. **Medium** protection against highly motivated adversaries and harder to detect planned events is required but there will remain vulnerabilities to complex cyber events.

Most organisations can achieve and maintain DSL-3 security with appropriate investment and commitment. DSL-3 is the standard used by organisations with a moderate risk tolerance for handling sensitive or confidential information, or information that could have a moderate impact in an adverse event.

Table 13 provides a summary of the protection levels required for event types under DSL-3. For many organisations, this classification may be appropriate for sensitive data.

Table 13: DSL-3 protection level requirements by types of adverse events and potential data types

Data Security Level	Protection level requirements				
	Physical	Cyber			Authorised person
		Common	Moderate	Complex	
DSL-3	High	Very high	High	Medium	High
Potential Data Types	Based on an organisation with a **moderate tolerance of risk**, the following are examples of data that might be classified at DSL-3. • Personal and sensitive information as defined in the *Privacy Act 1988*. • Confidential intellectual property (IP), trade secrets or similar IP that do not have patent or other intellectual property protections and that do not require special protection. • Sensitive financial information. • Market-sensitive information that has not been published, especially if it could be used for insider trading. • Information about a person that may be used to infer disease status, minority associations, cultural or religious affiliations, substance use or dependence, or political party membership. This is sensitive information under the *Privacy Act 1988*. • Internal organisation deliberations intended for a small team, for example the executive team. • Personnel files, especially those relating to individual staff members.				

Detailed event model

The DSL-3 event model builds on and includes the event model of DSL-2. Likelihoods of each event type under DSL-3 are discussed below.

Physical events

Physical access to data, systems and hardware must be controlled to reduce physical adverse events by adversaries who have targeted the organisation but who will cease when protection measures are found to be too great.

At DSL-3, protection measures should consider one of the following two options.

1. For systems or devices in secure environments, unauthorised access is to be highly unlikely.
2. For systems or devices in a less secure environment, such as laptops and mobile phones, they should be protected to ensure an adverse event will be unlikely.

   For example, access to unattended hardware and opportunistic or targeted theft by adversaries with moderate skills. If this type of adverse event could occur, protection is needed to ensure the event will not impact confidentiality or integrity of the data, and availability should be easily recovered.

   If an adversary takes possession of the device, control measures should reduce the chance of them accessing the contained data, even when using advanced techniques such as removing the data storage component of the device. This may be through measures such as encryption at rest and automatic or remote locking of devices.

Strong physical controls such as authorised access areas, security gate access in large organisations and escorted visitor access should reduce the likelihood of physical access by adversaries. The **likelihood** of unauthorised physical access should be reduced to **low**. At DSL-3, authorised people are trusted with physical access to devices.

Cyber events

For understanding cyber events, DSL-3 draws from Eight's Maturity Level 2. Any cyber event which is in scope of Essential Eight's Maturity Level 2 should be mitigated. Maturity Level 2 is described as:

> The focus of this maturity level is malicious actors operating with a modest step-up in capability from the previous maturity level. These malicious actors are willing to invest more time in a target and, perhaps more importantly, in the effectiveness of their tools. For example, these malicious actors will likely employ well-known tradecraft in order to better attempt to bypass controls implemented by a target and evade detection. This includes actively targeting credentials using phishing and employing technical and social engineering techniques to circumvent weak multi-factor authentication.
>
> Generally, malicious actors are likely to be more selective in their targeting but still somewhat conservative in the time, money and effort they may invest in a target. Malicious actors will likely invest time to ensure their phishing is effective and employ common social engineering techniques to trick users to weaken the security of a system and launch malicious applications. If user accounts that malicious actors compromise have special privileges they will exploit it, otherwise they will seek user accounts with special privileges. Depending on their intent, malicious actors may also destroy all data (including backups) accessible to a user account with special privileges.

While the IDCF defines cyber events using Essential Eight, implementation of controls can be drawn from any other equivalent sources. The IDCF uses the term adversaries to refer to the Essential Eight's malicious actors.

This maturity level focuses on cyber controls that may protect against **common** and **moderate cyber events** but focusses less on **complex cyber events**. As such, controls should reduce the likelihood of **common**, **moderate** and **complex cyber events** resulting in consequences to **very low**, **low** and **medium** respectively.

Authorised persons

Any access, both physical and cyber, to the data should be:

- restricted to authorised users
- on a need-to-know basis. For example, only users who need access to the data are granted access as authorised users.

Where physical access is difficult to control, protections should be implemented. This will ensure a **low likelihood** that an unauthorised person who accesses the storage device or system would be able to access the data.

All authorised persons should be trained in handling data under the IDCF and in managing cyber, physical and accidental or unintentional risks that may cause an adverse event. Training should highlight the risks from email and social engineering. Authorised persons should be aware of the relative value of DSL-3 classified data, the potential impact of an adverse event on that data and recognise the business need to be vigilant. Regular refresher training is recommended.

When data is classified at DSL-3 to protect integrity, but confidentiality does not need strong protection (such as published data), authorised persons are those who need to modify the data rather than those with a general need-to-know for confidentiality reasons.

For more information on the IDCF's detailed event model, please see the DSL module: Events.

Appropriate systems and environments

The IDCF provides a non-exhaustive list of guidelines and examples that are suitable for DSL-3. These guides and examples inform the kinds of controls required for the **level** of protection for DSL-3. The IDCF does not define specific systems and environments suitable for mitigating DSL-3 threats.

Standards, frameworks and guide examples

Approaches that currently meet the protection requirements and associated likelihoods of DSL-3 are listed below. Each approach offers benefits and has potential risks and should be used as a guide only. It is important to note that there are other standards and frameworks which offer guidance on implementing security that meets the desired protection levels of Table 13. Organisations may use compensating and alternate controls, providing that they can demonstrate that the combined controls meet the required protection level of DSL-3.

Essential Eight Maturity Level 2 - Cyber controls

- Systems that have successfully implemented and maintained Maturity Level 2 of the Essential Eight would meet the cyber requirements of DSL-3. For detailed description of these controls, refer to ASD's Essential Eight maturity model, Appendix D: Comparison of maturity levels.
- Note that meeting DSL-3 also requires the implementation of additional physical and authorised person controls which are not covered by the Essential Eight.

Protective Security Policy Framework (PSPF)

- DSL-3 has strong parallels with the PSPF 'OFFICIAL: Sensitive' marking . For further guidance, please see the PSPF.
- Australian government systems have a minimum requirement of Essential Eight, Maturity Level 2. This means any system that is suitable for Australian government is suitable for DSL-3. This includes systems used by government for PSPF 'OFFICIAL: Sensitive'. For detailed guidance, refer to Section 9.3 of the PSPF.

Center for Internet Security (with appropriate physical controls)

- The use of **CIS Controls Implementation Group 2 (IG2)** in enterprise Information Security Management Systems (ISMS) that implement ISO 27001 or the NIST Cybersecurity Framework are considered acceptable for meeting the cyber security requirements of DSL-3.

For more information, please see the CIS Critical Security Controls V8.1.

To evaluate system configurations, consider using the CIS-CAT® assessment tool.

Configuring common systems

Laptop and desktop

Physical controls would include:

- encrypted filesystems are either hardware locked or require user passwords to unlock access to the filesystem (Such as Bitlocker™ for Windows™ or FileVault™ on Apple's MacOS™.)
- BIOS/UEFI settings to help secure the laptop
- an operating system that locks the laptop and desktop when unattended
- a data storage device for which data extraction would still be very unlikely even with physical access to the hardware.

Cyber controls would include:

- regular software updates
- strong passwords or passphrases
- multifactor authentication
- laptops and desktops with only authorised user accounts (no extra accounts such as family members)
- no unauthorised software, including personal software, such as games
- restricted administrator access. (Normal user accounts do not have administrator access.)

A physically secure desktop may not need all these control measures for DSL-3, as the physical controls may provide an adequate substitute. Adoption of these controls for a physically secure desktop is considered good practice.

Cloud based services including productivity suites

Generally, the listed cloud-based services will:

- provide sufficient physical protections, though some attention to location of the solution may be required
- require configuration of cyber protections
- require organisations to manage user access.

Microsoft 365

- By following the Microsoft Guide for implementing Maturity Level 2 of the Essential Eight, Microsoft 365 can be configured to have DSL-3 appropriate cyber controls.

Google Workspace

- By implementing IG1 and IG2 controls outlined in the CIS Google Workspace Benchmark, organisations can configure their Google Workspace to have DSL-3 appropriate cyber controls.

Amazon Web Services

- Cloud services aligned with Phase 3: Efficient of CAF Capability have suitable cyber controls for hosting DSL-3 data.

Access controls and users

The more users with access to the data, the greater the attack surface area. Access to DSL-3 data should be restricted to a 'need-to-know' basis to minimise the potential for adversaries to target users as a means of gaining access. To manage this risk, user access must be actively managed, especially as roles change. Where administrators have technical access to all data, strong vetting should be considered and privileged access to systems must be securely logged and regularly audited.

For more information, please see ASD's Control ISM-1509 and ISO 27002, Clause 8.2 Privileged Access Rights.

Users

Users and staff are a potential vulnerability in a DSL-3 system. DSL-3 requires **high** protection to prevent authorised user's actions causing an adverse event. Significant management is needed to ensure **low likelihood** of an authorised person adverse event.

Need-to-know principle

- The overriding principle of users at DSL-3 is 'need-to-know'.
- Access should be limited to individuals with a legitimate business need.
- Systems **must have** appropriate permissions and access controls to ensure access is managed.
- User access should be added and removed as required to meet the 'need-to-know' principle.
- Basic vetting such as employment checks should occur to ensure users will act appropriately.

Training and compliance

Many systems and applications do not prevent actions by users that might have an unintended impact, making it easy for untrained or unaware staff to breach security measures through lack of awareness. For example, emailing DSL-3 classified material to a system only suitable for DSL-2 or copying DSL-3 classified material to a USB storage device to work on at home using an insecure personal computer.

At DSL-3, users are potentially the weakest link. This risk is expected to be managed in systems suitable for DSL-3 data by providing general training and raising awareness of good data practices and common cybersecurity threats. Preventing access to portable storage devices, such as USBs should be considered.

4.7.5. DSL-4: Data Security Level 4

DSL-4 is a **high** security classification for data. Data classified at DSL-4 requires **very high** protection controls as it is likely to be highly desirable to adversaries and cause significant impact if there is an adverse event. Adversaries may be highly motivated and may go to significant effort, or employ those who can, to gain access and cause an adverse event. Other actors may recognise the potential value of the data and seek to cause an adverse event to profit from the sale of the data. DSL-4 recognises that while a **complex cyber event** is more difficult to protect, it still requires **high protection** to ensure an adverse event is unlikely.

Breached data holds a strong possibility of ending up in the hands of those who can cause significant harm. Data corruption would also cause significant harm. DSL-4 systems are designed specifically for data of significant risk. Access to data at DSL-4 will most likely involve an intentional process and a specific, justifiable purpose.

Very high levels of protection are required with a recognition that complex cyber events require significant effort to prevent and a **high** level of protection against those events is sufficient. In many situations, consideration will need to be given to the control of jurisdictional and foreign influences over data systems and solutions. This will include the location of infrastructure, and the citizenship of authorised users and those maintaining systems. Consideration may include the exposure of risk to actions of foreign states such as subpoenas and the control of users that have access to the system.

For most organisations, DSL-4 will be beyond normal day-to-day operations. Where an organisation holds this type of data, it is likely to be in specialised systems designed for the specific data.

Data classified at DSL-4 is likely to be highly sensitive with the potential for significant impact if an adverse event is successful, requiring specially designed systems for protection.

Table 14 provides a summary of the protection levels required for adverse event types under DSL-4. For many organisations, this classification may be appropriate for highly sensitive data.

Table 14: DSL-4 protection level requirements by types of adverse events and potential data types

Data Security Level	Protection level requirements				
	Physical	Cyber			Authorised person
		Common	Moderate	Complex	
DSL-4	Very high	Very high	Very high	High	Very high
Potential Data Types	Based on an organisation with a **moderate tolerance of risk**, the following are examples of data that might be classified at DSL-4. • Nationally important data which could have an impact on society or services in general. • Highly confidential intellectual property (IP), particularly valuable IP, trade secrets or similar IP, especially that might be subject to export controls or is core to an organisation. • Sensitive financial information. • Market-sensitive information prior to publication, especially if it could be used for insider trading. • Information that may be used to infer disease status, minority associations, cultural or religious affiliations, substance use or dependence, or political party membership (this information constitutes sensitive information under the *Privacy Act 1988)* where the impact would be serious and/or significant. • Internal organisation deliberations that would not be suitable for a wide audience. • Sensitive personnel files, especially those related to staff members with a public profile.				

Detailed event model

The DSL-4 event model builds on and includes the event model of DSL-3. Likelihoods of each event type under DSL-4 are discussed below.

Physical events

Physical access to data and systems requires significant control so physical events have a **very low likelihood** of having negative consequences. This includes attempts by highly motivated adversaries seeking physical access to systems.

Most common mobile devices are unlikely to meet the DSL-4 requirements. Where physical measures may not prevent access, other strong measures should be in place to prevent access to any data on those devices. Threats from physical access on fixed devices are mitigated by ensuring unauthorised individuals are extremely unlikely to achieve physical access. Authorised persons are both vetted and trusted before physical access to devices and infrastructure is approved.

For hardware outside strong physical controls, other strong controls should be implemented to prevent nearly all possible events such as, theft and disassembly of hardware, access using known passwords and the actions by individuals with significant skills, for example a black hat hacker or state actors.

Cyber events

To understand cyber events at DSL-4, the IDCF draws from ASD's Essential Eight's Maturity Level 3. Any cyber event which is in scope of Essential Eight's Maturity Level 3 should be mitigated. Maturity Level 3 is described as:

> The focus of this maturity level is malicious actors who are more adaptive and much less reliant on public tools and techniques. These malicious actors are able to exploit the opportunities provided by weaknesses in their target's cybersecurity posture, such as the existence of older software or inadequate logging and monitoring. Malicious actors do this to not only extend their access once initial access has been gained to a target, but to evade detection and solidify their presence. Malicious actors make swift use of exploits when they become publicly available as well as other tradecraft that can improve their chance of success.
>
> Generally, malicious actors may be more focused on particular targets and, more importantly, are willing and able to invest some effort into circumventing the idiosyncrasies and particular policy and technical controls implemented by their targets. For example, this includes social engineering a user to not only open a malicious document but also to unknowingly assist in bypassing controls. This can also include circumventing stronger multi-factor authentication by stealing authentication token values to impersonate a user. Once a foothold is gained on a system, malicious actors will seek to gain privileged credentials or password hashes, pivot to other parts of a network, and cover their tracks. Depending on their intent, malicious actors may also destroy all data (including backups).

While the IDCF defines cyber events using Essential Eight, implementation of controls can be drawn from any other equivalent sources. The IDCF uses the term adversaries to refer to the Essential Eight's malicious actors.

This maturity level focuses on cyber controls that may protect against **common**, **moderate**, and **complex cyber events.** Controls should reduce the likelihood of **common**, **moderate** and **complex cyber events** resulting in consequences to **very low**, **very low** and **low** respectively.

Authorised persons

Any access, both physical and cyber, to the data must be strictly controlled and managed to ensure authorised access only. Access to data should:

- be restricted to authorised users, verified through multiple methods such as multi-factor authentication at each login
- follow a strict need-to-know principle, granting access only to users with a legitimate business requirement
- be minimised by assigning additional roles to existing users rather expanding the authorised user base.

Access to data or systems by administrators should occur under the supervision of another administrator or authorised user. Administrator access must be governed by access controls, active logging or strong administrator vetting.

Physical controls should ensure only authorised persons have physical access. In rare cases where physical access is difficult to control, there should be a **very low likelihood** that unauthorised persons would be able to access the data.

All authorised persons **must** receive training on DSL-4 requirements and cyber risk management. This includes principles for handling sensitive data and understanding the serious consequences of mishandling it. The training must include understanding of how manipulation, social engineering, or personal influence can be used to create compromising situations potentially over extended time periods. Organisation should offer trusted contacts or secure channels for authorised persons to get help if they suspect manipulation or compromise. Annual refresher training is mandatory.

For more information on the IDCF's detailed event model, please see the DSL module: Events.

Appropriate systems and environments

Standards, frameworks or guides

Approaches that meet the protection requirements and associated likelihoods of DSL-4 are listed below. Each approach offers benefits and potential risk and should be used as a guide only. It is important to note that there are other standards and frameworks which offer guidance on implementing security that meets the desired protection levels of Table 14. Organisations may use compensating and alternate controls, providing that they can demonstrate that the combined controls meet the required protection level of DSL-4.

Essential Eight Maturity Level 3 - Cyber controls

- Systems that have successfully implemented and maintained Maturity Level 3 of the Essential Eight controls would meet the cyber requirements of DSL-4. For detailed descriptions of these controls, refer to ASD's Essential Eight maturity model, Appendix D: Comparison of maturity levels.
- Note that meeting DSL-4 also requires the implementation of additional physical and authorised person controls which are not covered by the Essential Eight.

Protective Security Policy Framework (PSPF)

- DSL-4 level has strong parallels with the PSPF 'PROTECTED' marking. A system that is suitable for Australian Government PSPF 'PROTECTED' classified material is likely to be suitable for DSL-4.
- For detailed guidance, refer to Section 9.3 of the PSPF, Minimum Protections and Handling Requirements. With the exception that Australian Government security clearances are not directly applicable to the IDCF and alternative vetting would be appropriate.
- The PSPF provides good guidance on physical security zones that are suitable for 'PROTECTED'.
- Organisations seeking to meet the PSPF 'PROTECTED' level of protection as an addition to meeting DSL-4 level of security are encouraged to consult a qualified cyber security professional or an Infosec Registered Assessors Program (IRAP) Assessor to ensure their systems have appropriate controls implemented.

Center for Internet Security (CIS) Controls (with appropriate physical controls

- The use of **CIS Controls Implementation Group 3** (IG3**)** in enterprise Information Security Management Systems (ISMS) that implement ISO 27001 or the NIST Cybersecurity Framework are considered acceptable for meeting the cyber security requirements of DSL-4.

For more information, please see the CIS Critical Security Controls V8.1.

To evaluate system configurations, consider using the CIS-CAT® assessment tool.

Configuring common systems

Laptop and desktop

While it may be possible to design a secure laptop computer at DSL-4, the process is complex and beyond the scope of this document. A qualified security professional would be required for this task. While it is possible to configure a desktop or workstation level computer and provide the necessary physical protections, setup and maintenance of these systems are likely to be conducted by security specialists. The strong control requirements require careful consideration and justification.

Cloud based services

The location of cloud services must be carefully considered, as many DSL-4 data applications may involve control of jurisdictional and foreign influences. Services should be hosted in an appropriate country based on the nature of the risk. For Australian organisations under DSL-4, Australian based infrastructure is likely highly desirable and may be insisted upon by data owners as part of a data sharing agreement and the statement of system security.

Generally, the listed cloud-based services will:

- provide physical location and security solution options with sufficient physical protections, though these will need to be chosen rather than being the default
- require configuration of cyber protections
- require organisations to manage user access.

Windows 365

- When configured to meet PROTECTED requirements, Windows 365 can serve as a suitable platform for handling DSL-4 data.
- To maintain DSL- 4, systems would be accessed through thin clients that do not hold any data from the DSL-4 system on local storage.

Microsoft 365

- By following the Microsoft Guide for implementing Maturity Level 3 of the Essential Eight, Microsoft 365 may be DSL-4 appropriate. Note that this may need to be negotiated with the data recipient. System designers need to consider the entire ecosystem, including any local hardware that might cache or sync data in the cloud.

Google Workspace

- By implementing the **IG1, IG2 and IG3 controls** outlined in the CIS Google Workspace Benchmark, organisations can configure their Google Workspace to be DSL-4 appropriate. System designers would need to consider the entire ecosystem, including any local hardware that might cache or sync data in the cloud.

Amazon Web Services

- AWS offers a Prescriptive Guidance on Reaching Essential Eight and a sample conformance pack template to help customers specifically achieve Essential Eight's Maturity Level 3 in a cloud native way. Once implemented, organisations can use AWS Audit Manager to review their Essential Eight controls. AWS cloud services that adhere to this guide are considered appropriate for DSL-4.

Access controls and users

DSL-4 requires that access to data is restricted to those with a need-to-know. Potential restrictions on how data is accessed and how much data can be accessed at a time should be considered.

Users

Users and staff are potential vulnerabilities in a system. DSL-4 requires strong access controls to ensure a **very low likelihood** of an authorised person's actions resulting in an adverse event. This requires **very high protection**. Users and administrators must be highly trusted individuals, unlikely to be influenced or manipulated by external factors. All users and staff should complete a vetting process which examines character and external loyalties. This could be achieved through Australian government security clearances, however if eligibility requirements are not met, other private services may provide appropriate vetting.

Need-to-know principle

- The 'need-to-know' is the overarching principle of users accessing data classified at DSL-4.
- Access should only be provided to those with a legitimate business need.
- DSL-4 systems are likely to be separate from systems used for an organisation's daily operation.
- Access to DSL-4 systems **must** be strictly managed and monitored, with appropriate permissions and access control.

Training and compliance

A DSL-4 system should make it very difficult for users to remove data from the environment. All persons authorised to access and handle this type of data must be trained and understand their responsibilities. Systems supporting DSL-4 material are expected to manage this risk, potentially through regular audits and authorisation from another party before data leaves the environment.

4.7.6. DSL-5+: Data Security Level 5+

DSL-5+ is a **very high** security level for data. Data classified at DSL5+ has been assessed and deemed to be extremely sensitive and must be stored in specially designed and specified environments. It indicates that the data carries significant risk, requiring protections beyond that offered by DSL-4.

This level is rarely applicable to business operations. It enables organisations with **very high-risk** data to indicate this risk within the IDCF. However, the DSL-5+ marking does not prescribe how this type of data should be protected. Protection must be determined by the data owner and agreed between parties.

Table 15: DSL-5+ protection level requirements by types of adverse events and potential data types

Data Security Level	Protection level requirements				
	Physical	Cyber			Authorised person
		Common	Moderate	Complex	
DSL-5+	As agreed between parties.				

4.7.7. Overview of potential DSL controls

Table 16 provides an overview of the potential controls an organisation could implement to align with their assessed DSL. The table can be used as a comparison between the required protections for each DSL and provide guidance when setting up suitable systems and environments within the organisation.

Table 16: Overview of potential DSL controls

DSL	Standards, Frameworks or Guides		Access and user controls	Configuring common systems - devices	Configuring common systems - cloud
DSL-0	Essential Eight	Maturity level 0	Unrestricted	Not applicable	Not applicable
DSL-1	Essential Eight	Maturity level 0	• Physical controls only (see section 24 of PSPF). • Users should be aware of their obligations under DSL-1 (for example, locking devices in a known location).	**Mobile devices** – should be in possession of an authorised user and stored securely when unattended.	**Cloud based servers** – Physical protections by cloud service providers.
	PSPF	No parallels – however section 24 Security Zone 2 (entity office area) may inform physical controls			
DSL-2	Essential Eight	Maturity level 1	• 'Need-to-know' or 'may need-to-know' principle. • General training and awareness of good data practices and common cybersecurity threats.	**Devices**: Encrypted filesystems that are unlocked by secured hardware or user password. **Cyber**: • regular software updates • strong passwords • multifactor authentication.	Microsoft 365 configured to Essential Eight's maturity level 1. CIS Google Workspace with IG1 control implemented. Amazon Web Services aligned to *Phase 1: Quick Wins* of CAF Capability.
	PSPF	No parallels – section 24 (Security Zone 2 (entity office area) may inform physical controls			
	CIS	Controls IG1 in enterprise Information Security Management Systems (ISMS) that implement ISO 27001 or NIST Cybersecurity Framework.			
DSL-3	Essential Eight	Maturity level 2	• 'Need-to-know' principle. • User access is actively managed. • Administrators are subject to strong vetting. • Regular auditing. • General training and awareness of good data practices and common cybersecurity threats.	**Physical:** • encrypted filesystems are either hardware locked or require user passwords to unlock • BIOS/UEFI settings on laptops • Autolocking of operating system • data storage device with data extraction controls **Cyber:** • regular software updates • strong passwords or passphrases • multifactor authentication • laptops and desktops with only authorised user accounts • no unauthorised software • restricted administrator access	Microsoft 365 configured to Essential Eight's maturity level 2. CIS Google Workspace with IG1 and IG2 controls implemented. Amazon Web Services aligned to *Phase 3: Efficient* of CAF Capability.
	PSPF	Systems and environments suitable for PSPF 'OFFICIAL: Sensitive'			
	CIS	Controls IG2 in enterprise Information Security Management Systems (ISMS) that implement ISO 27001 or NIST Cybersecurity Framework.			
DSL-4	Essential Eight	Maturity Level 3 (with additional physical and authorised person controls)	• 'Need-to-know' principle. • Restrictions to data access, amount of data access at a time should be implemented • Users and administrators must be highly trusted • All users and staff should be vetted • Data should be difficult to remove from environment • Authorised persons should be trained and understand their responsibilities • Regular audits • Authorisation requirements before data leaves environment	Controls are complex and are beyond the scope of the IDCF. It is recommended that a security professional be consulted.	Windows 365 cloud PC configured compliant to PSPF 'PROTECTED'. Microsoft 365 configured to Essential Eight's maturity level 3. CIS Google Workspace with IG1, IG2 and IG3 controls implemented. Amazon Web Services configured to Essential Eight's maturity level 3.
	PSPF	Systems and environments suitable for PSPF 'Protected'			
	CIS	Controls IG3 in enterprise Information Security Management Systems (ISMS) that implement ISO 27001 or NIST Cybersecurity Framework.			
DSL-5+	Data classified at DSL-5+ requires protections beyond DSL-4. It has been assessed that it will cause extreme harm if there was an adverse event. DSL5+ will be used by data owners on data types that, if held by government, would receive a security classification of 'SECRET' or 'TOP SECRET' under the PSPF. DSL-5+ is **not** an equivalent or industry version of PSPF 'SECRET' or 'TOP SECRET'. The IDCF does not provide guidance on how DSL-5+ data should be protected. Any protection requirements must be determined by the organisation and accompany the data. When sharing DSL-5+ data with trusted entities, storage and protection requirements of the data must be negotiated as part of the data sharing agreement.				

4.8. Data security levels: rules

While use of the IDCF is voluntary, for DSLs to be effective, a common set of default rules is required. As stated in the code of conduct, these rules are intended to apply to all users of the IDCF, except where a formal agreement between the data owner and data recipient permits otherwise.

For more information on the code of conduct, please see the Introduction: Code of conduct.

4.8.1. Rules

These rules apply where there is an agreement, whether in writing or implied, to use the IDCF for handling data. An agreement may be implied if an organisation advertises that it uses the IDCF.

These rules may be modified by agreement between a data owner and a data recipient.

1. A data owner is responsible for seeking assurance that the data recipient's systems meet their claimed DSL protection level.
2. Any data labelled with a DSL must be stored in a system that provides protection at or above the specified level. For example, DSL-2 data must be stored in systems that meet DSL-2 requirements or exceed them.
3. Only the data owner or those they authorise may declassify data or reclassify data to a lower classification.
4. A data recipient may reclassify data to a higher level.
5. A data recipient may classify any unclassified data they receive, as though they were the data owner.
6. New data created using IDCF classified data by a data recipient must, by default, be classified and labelled at the same DSL as the originating data or the highest level of all the originating data. The original data owner retains the same rights over any reclassification of the derived data, as if they had created the data themselves.

4.8.2. Guide to using rules

These are the default rules of the IDCF, however variations may be negotiated between the data owner and data recipient. For example, if a data recipient plans to create another data product based on the original classified data, both parties may agree to classify the derived data product at a lower DSL. This may be appropriate in cases where the derived data product is a summary of the data and removing the risk to the data owner.

4.9. Data security levels: guidance

This section presents high-level information to guide the usage of DSLs. It covers common circumstances encountered by users of the IDCF. These are suggestions only and are designed to help users consider how they apply the DSL labels.

4.9.1. Communication and movement of data

Devices, systems and methods that are used to move data must meet the data's DSL classification protection requirements. In other words, when data is moved out of the originating system into a system or device designed to transport the data, the transport device/system must also meet the DSL classification protection requirements of the data. Appropriate solutions are readily available for data classified up to DSL-3 though care and diligence is still required. For example, transferring DSL-2 classified data to a plain USB storage device is inappropriate due to the DSL-2 requirement to prevent access to data if the USB is lost. Transferring to strong password encrypted USB storage device will likely meet DSL-2 protection requirements. Higher DSL classifications may require greater security protections.

For communication network transfers, the communication technology must align with the DSL protection requirements. End-to-end encryption is generally sufficient provided there is sufficient trust in the encryption keys. If unsure, consult a security specialist.

Generally, the movement of data between systems should be controlled to ensure the provision of appropriate DSL classified systems. While some systems may prevent the use of USB storage devices or the emailing of sensitive documents, controls are likely to be based on policy and staff training.

Email

An email's DSL label must reflect the highest classification required by its content or attachments. Internal organisational emails are likely to be as secure as their email system. However, security may not be guaranteed when exchanging emails across organisations. Email systems do not always ensure secure end-to-end encryption.

Organisations typically accept the risk of email interception for small amounts of data classified up to and including DSL-3. End-to-end encryption of email is possible, but it is often technically challenging to implement. An alternative is to encrypt attachments in secure containers with trusted cryptographic key sharing.

The technical possibilities of email interception are beyond this guide, users are encouraged to acknowledge the risk of email interception, particularly as a complex cyber risk.

For more information on email security, please see ASD guides on Email security and Email usage.

4.9.2. Classifying data containers

Data is often held in containers, such as zip files. A container's DSL may differ from the classification of the data inside. If the file is **not encrypted**, the container typically inherits the highest DSL of its contents. In addition to this:

- Where the collection of data in the container is more valuable, has greater impact in an adverse event and requires higher protection than the individual files, a higher DSL than the DSL of the underlying data may be used.
- If the container uses strong encryption that prevents access to the data without the cryptographic key, you may classify the container at a lower DSL than that of the data stored within. The cryptographic key should be classified at a DSL appropriate to the data it protects.

Note a container's DSL label does not necessarily reflect the classification of its contents.

For example, a dataset is classified at DSL-4, placed in an encrypted container file and the cryptographic key for unlocking the data is assigned DSL-4 and is held apart from the container. The data inside the container remains at DSL-4. Assuming strong encryption, the likelihood of an adverse event is lower because the data within the container cannot be accessed without the key. The container is classified at DSL-1. It can be transferred on a USB storage device without the cryptographic key.

After transport, the data on the USB storage device is placed on a DSL-4 appropriate system, where the file is decrypted. The USB storage device is erased. Once decrypted in the DSL-4 system, the data retains its original DSL-4 classification.

In this example the cryptographic key(s) remain classified at DSL-4 as it can unlock the encrypted data. It must be transferred using a method appropriate under DSL-4.

4.9.3. Data for publication

The publication of data poses a challenge to classification systems. The integrity of the 'original' data needs to be protected and the published data often needs to have high availability. This implies a strong security requirement. However, because the data has been published, there are weak or no confidentiality requirements and public access is often granted. In addition to this, when the data is copied, that is when a data recipient receives the data, the integrity and availability requirements do not carry to the copy of the data.

The suggested guidance is for data owners to set a policy and utilise their right to reclassification or declassification of data. Potential approaches organisations can take to manage this situation include:

- Classifying the original data on the location of the publication, for example on a website, with the appropriate DSL label.
- Set a policy for the data to be declassified on copy. This means removing all IDCF labels and markings on the published view.
- Reclassify the copied data to DSL-0.

For example, original data is published on a website may be classified at DSL-3. The website's system provides protection to the availability and integrity of the data at an appropriate for DSL-3. The system authorises public access to the data. When users read, copy or use the data, the copies would be declassified and no longer subject to the IDCF. In these situations, it is unlikely that a IDCF data sharing agreement between the data owners (the website publisher) and the data receivers will be in place. Although the DSL label can be disregarded when there is no data sharing agreement, declassification is seen as best practice.

4.9.4. Assessing systems

When assessing the level of security or protection provided by an IT facility or a system, organisations should consider the entire system.

For example, consider an organisation that uses a cloud-based service that synchronises users' cloud storage with their laptop hard-drive. There are three components to the system: the cloud service, the laptop, and the network and protocols used for synchronisation. The system's overall level of protection is the weakest protection provided by each of the three components. The cloud service synchronising client is likely to be using strong encryption resulting in high or very high protection. Assuming the laptop and network provide a lower level of protection than the cloud, they are the weakest point in the assessment.

In contrast, if there is an intentional separation between the cloud and laptop systems, where the data is always stored on the cloud service and not copied to the laptop, the two systems could be assessed independently. For example, a system may pair a secure cloud PC with a thin client (see Appendix A: Glossary for definition) as an access point. The data does not get copied onto the thin client. The cloud PC and thin client could be assessed independently at different classification levels. A lower-level thin client would generally not impact the level of the cloud PC and the data stored within that environment.

This is something small and medium-sized organisations need to be aware of. If an organisation's data might find its way onto personnel home computers, instead of remaining in the cloud, those home computers also need to meet the protection requirements of the original data. Organisations may reduce this risk by implementing a policy against organisational data being transferred onto home devices.

4.9.5. Streamlined classification and the risks

To simplify the handling of new data, organisations may choose to triage data and apply a maximum potential DSL without conducting a full data risk assessment. This may simplify the use of the IDCF and reduce costs. However, this approach may lead to data being classified at a higher DSL than required and unnecessary protections applied to the data. An organisation can consider lowering the DSL for the data following the completion of a full data risk assessment at a later date.

For organisations using a single primary system that has been properly determined to be suitable for data to a particular DSL, this approach may save time and cost.

Avoid under-classifying data, that is data classified at a lower DSL than required, as it poses significant risk.

Organisations should not use this approach to determine the suitability of a system for a particular DSL. If a quick assessment of a system is required, there should be full confidence the system meets or exceeds the DSL that will be used.

4.10. Statement of system security

The IDCF is a voluntary framework that does not have a compliance or regulatory component. This may provide organisations with greater flexibility in solutions and may help reduce costs. Data owners are responsible for ensuring that data recipients' systems meet the requirements for storing data at a given DSL. Data recipients are responsible for providing assurance that their systems meet the level of protection required by a given DSL. This assurance process typically takes place during the development of a data sharing agreement or as part of a contractual agreement.

This section provides the data recipient with a standardised template to describe their systems security features for consideration by the data owner or their customers.

4.10.1. Why use a statement of system security?

As the IDCF does not impose regulatory requirements or an assurance process, systems used to store data are not formally assessed against DSL requirements.

This is an intentional design feature that:

- ensures flexibility of solutions
- keeps participation costs low
- avoids unnecessary and expensive compliance processes.

However, this approach means there is no guarantee that an organisation is using systems appropriate for the designated DSL. The IDCF recommends the data owner require a '*Statement of system security*' from the data recipient as part of their due diligence in ensuring the data recipient's systems are appropriate for the DSL of the shared data. This statement should seek to demonstrate or justify the recipient's systems alignment with the assigned DSL.

4.10.2. Statement of system security

A statement of system security is a summary that outlines how specific systems meet the requirements of a given DSL, confirming their suitability for storing data at that level.

The level of detail of the statement depends on the requirements of the data owner. For smaller organisations, it may be as simple as listing the controls applied to business-owned hardware and configuration options in cloud infrastructure. For larger organisations, it might involve referencing compliance and audit results with a recognised standard, particularly those outlined in the

DSL module: Data Security Levels. For example, the results of an assessment or other evidence that systems meet CIS IG2 could be used to show system are appropriate for DSL-3 data.

The Statement of System Security template shows one way a data recipient could present this information. Other formats may also be acceptable. The data owner will decide what evidence is accepted.

There is no requirement for a statement of system security to be comprehensive. Some information can be indicative, especially when additional documentation, such as policies, can be provided to offer further assurance. This will be part of the negotiation process as the assurance is for a data owner. The information required will be determined by the assurance required by the data owner during the negotiation process.

For an example Statement of System Security template, please see Appendix E: Statement of system security.

5.
Markers module

Markers are an optional way for organisations to communicate information about context, the nature of risk and security requirements of data beyond the core Data Security Levels (DSL). This includes handling, sensitivity and dissemination restrictions. This module explains the three categories of markers and provides guidance on how an organisation can use them.

Before reading this module, please see the **DSL module**. It provides foundational context necessary for understanding the material covered here.

5.1. Introduction

Markers are an optional, additional classification in the Industry Data Classification Framework (IDCF). They provide a secondary classification scheme that complements the core DSLs, which are compulsory under the IDCF. They provide extra information and context about the nature of risk and handling of data.

Markers are different from a DSL label. When using markers within the IDCF, markers always follow a DSL label, for example **DSL, Marker**. If there is no DSL label before a marker, this indicates that the data hasn't been classified under the IDCF and the marker may have a different definition to those listed below.

The IDCF has three categories of markers, **integrated**, **adopted** and **user defined**, which are described in this module.

5.1.1. Key terms

The following key words and phrases are used in this module.

Table 17: Markers key terms

Key term	Definition
Classification	The process of placing data in a class. In the IDCF, this means applying a data security level (DSL) label and optionally applying markers based on a risk assessment.
Confidentiality	Preserving authorised restrictions on data access and disclosure, including means for protecting personal privacy and proprietary information. This is based on the NIST definition.
Data owner	The individual or organisation that owns or originally collected, curated, generated or classified the data.
Data recipient	The individual or organisation that receives data from a data owner.
Industry	A collective term for many organisations operating in a common area of the economy and for all organisations together. For example, the health industry or Australian industry.
Integrity	A property whereby data has not been modified in an unauthorised manner since it was created, transmitted or stored. This is based on the NIST definition.
Label	A visible indicator in physical or electronic form applied to data to communicate its DSL classification.
Marker	A visible indicator in physical or electronic form, applied to data to communicate a secondary classification, such as specific handling, sensitivity or dissemination requirements.
Marking	The process of applying a marker to data. See the Markers module for more information.
Organisation	An entity. This includes a business, company, association, sole trader, partnership or government, for example Corporate Commonwealth Entities and State and Territory to the extent they can use the IDCF.
Risk	The likelihood of a consequence that may result in impact from an event.
TLP	Traffic Light Protocol

5.1.2. Markers are optional

A data owner can decide if and when to apply a marker when classifying data under the IDCF. Where markers have been applied, internal organisational policy should determine how those markers inform data handling.

In a data sharing arrangement between organisations, the data recipient may disregard markers applied by the data owner (sender) unless otherwise agreed. Before sharing data, a data owner should negotiate and seek agreement with a data recipient on the use of markers and their implications for handling. Without an agreement, or where agreement to use the IDCF has been reached but there is no specific agreement on marker usage, the data recipient may disregard markers. A data recipient may subsequently add markers for their internal use, provided those markers are consistent with the markers already agreed with the data owner.

An agreement on markers may cover all categories of markers, a subset of markers, or clarify the default approach under the IDCF that markers can be disregarded.

For more information on respecting DSLs and markers, please see the Introduction: Code of conduct.

5.1.3. Marker categories

The IDCF markers are grouped into three categories according to their origin:

- **Integrated markers** are defined by the IDCF and, where agreed, are recognised by anyone using the IDCF based on the definitions provided below. There are 11 integrated markers:
    - six describe the nature of risk
    - five describe dissemination limitations that are commonly used.
- **Adopted markers** are defined and published by another organisation. There is currently one set of adopted markers in the IDCF which provide general guidance on sharing data across organisational boundaries.
- **User defined markers** are defined outside the IDCF and have not been formally adopted by the IDCF. They are defined or used locally by an organisation for business-specific classification, without common recognition by other IDCF users. They enhance the adaptability of the IDCF, enabling flexible local expansion of markers beyond **integrated** and **adopted**.

5.2. Details about markers

A marker may convey specific meaning regarding the nature of the risk in the data, potential compliance, regulatory or legislative concerns, requested access restrictions, or other meanings determined by an organisation. Markers also describe handling, sensitivity and dissemination restrictions. Unlike DSLs where only one can be applied, multiple markers may be attached to data and can be used at any DSL. The presence of a marker suggests management and handling practices that should be followed professionally or contractually.

Certain markers may not be appropriate for some DSLs, for example, adding the integrated marker 'Personal Privacy' on DSL-0 data. It is the responsibility of the data owner to ensure consistency of the application of markers.

5.2.1. Marker design

An IDCF marker can be identified because the data will also have a DSL label attached, for example **DSL, Marker**, indicating it has been classified under the IDCF. Integrated markers are defined in this module, adopted markers are defined by existing protocols and user defined markers are set by organisations or industries. Adopted and user defined markers use a prefix in their naming convention followed by a colon and then the marker **(DSL, Prefix: Marker)**.

For more information about prefixes, please see the Markers module: Marker prefixes.

5.2.2. Integrated markers

The IDCF has identified and defined **integrated markers** which are commonly used across industry. There are two groups of integrated markers.

The first group of six **integrated markers** are defined in Table 18. These markers help identify the nature of risks associated with the data, particularly regarding compliance, regulatory or legislative concerns. While they mainly come from the Rights Type Scheme of the Australian Government Recordkeeping Metadata Standard (AGRkMS), they have been adapted to better suit industry.

The second group of five **integrated markers** are defined in Table 19. They help describe dissemination restrictions for data, indicating that only particular individuals should view it.

Table 18: Integrated markers related to the nature of risks associated to the data

Integrated markers	Descriptions
Confidential	Data that is assessed to be confidential, particularly where obligations to maintain confidence arise in contract and equity. The data should be handled in a manner consistent with that obligation and access should be limited to authorised personnel with a legitimate business need.
Cultural	Data with cultural significance that needs sensitive handling in accordance with relevant cultural protocols or permissions. Data recipients should refer to accompanying information regarding handling of the data ensuring the data is accessed, used and shared in a manner that respects cultural ownership and context.
Embargo	Data that cannot be released or disclosed until a specific time, date, event or approval condition is met. The embargo condition must be clearly documented elsewhere and enforced through access controls until the restriction is lifted.
Intellectual Property	Data containing propriety information, trade secrets or other materials protected by intellectual property rights. Access to the data should be restricted to authorised personnel on a need-to-know basis and handled in accordance with contractual and legal obligations.
Legal Privilege	Data that is restricted to legal personnel and covered by legal professional privilege. Access to the data should be on a need-to-know basis and the data should be handled in a way that preserves confidentiality and privilege.
Personal Privacy	Data that contains or that may be considered ‘personal information’ (including ‘sensitive information’) under the *Privacy Act 1988*. This may include data that may not be ‘personal information’ in the current data setting but may become ‘personal information’ when combined with other datasets. Data should be handled according to organisation policy regarding ‘personal information’, the *Privacy Act 1988*, and any contractual or regulatory privacy obligations.

Table 19: Integrated markers related to the dissemination restrictions for data

Integrated markers	Descriptions
Public	Data that is already in the public domain, can be placed in the public domain, or is approved for public release. There is no requirement for technical dissemination controls on this data. This marking does not imply DSL-0, nor does it imply a waiving of all rights. Data integrity and availability may need high security levels to protect the underlying data. Data use may still be subject to a licence or law.
Internal	Data that is accessible only within the organisation, including authorised employees, contractors or affiliates. Data should not be shared with external parties to the organisation without appropriate approval or reclassification.
Finance Only	Data restricted to the finance team and authorised or approved auditors. Access should be limited to finance personnel and auditors under confidentiality obligations.
Executive Only	Data that can be accessed only by executive leadership.
Board Only	Data intended strictly for board members.

5.2.3. Adopted markers

The IDCF adopts the set of markers known as the Traffic Light Protocol (TLP) referenced by ASD. The authoritative definition of these is authored by FIRST as found at TLP V2.0. The markers are colour coded, with both the foreground and background being defined and include a 'TLP' prefix. While the TLP V2.0 formatting is preferred, users can consider changes to the black background and removing the text colour where these are impractical or difficult to achieve.

The markers are:

- **TLP:RED** : For the eyes and ears of individual recipients only, no further disclosure.
- **TLP:AMBER+STRICT** : Limited disclosure, recipients can only spread this on a need-to-know basis within their organisation.
- **TLP:AMBER** : Limited disclosure, recipients can only spread this on a need-to-know basis within their organisation and its clients.
- **TLP:GREEN** : Limited disclosure, recipients can spread this within their community.
- **TLP:CLEAR** : Recipients can spread this to the world, there is no limit on disclosure.

5.2.4. User defined markers

User defined markers are defined by organisations for specific use cases within their organisation and by agreement in wider settings. They are not defined by and have no official standing in the IDCF. Data handling of these markers is not covered by the IDCF or the IDCF Code of Conduct.

For more information on the IDCF Code of Conduct, please see the Introduction: Code of conduct.

Organisations or industries can define and use their own set of **user defined** markers to augment the set of **integrated** and **adopted** IDCF markers. They can also transition existing markers to use within the IDCF.

There are two parts that make up a user defined marker, the prefix and the marker. The prefix should be common for any set of user defined markers. It helps identify the author of the marker and the set to which it belongs. A user defined marker will have the form **Prefix: Marker**.

By using a unique prefix, organisations can ensure their markers are distinct and easily identifiable. The use of a prefix helps avoid confusion, especially when similar markers might be defined elsewhere with different meanings across various organisations or industries.

Organisations should maintain clarity, consistency and relevance of their markers. To ensure their data can be handled in a way that is consistent with the marker conditions, the data owner should ensure the definitions and handling expectations of the markers are accessible to all stakeholders. If an organisation wants a data recipient to adhere to their user defined marker conditions, an agreement should be entered into before sharing the data.

For more information on marker prefixes, please see the Markers module: Markers prefixes.

5.2.5. Marker formatting

The IDCF provides a simple set of rules for formatting markers. All other marking decisions are flexible. For example, physical or electronic documents may have visual markers placed anywhere on the document.

An example company ‘A Bright Company’ (ABC) is used in the following examples.

The rules for marking are:

- Markers can be applied using any font. They are not case sensitive and using bold text is optional. It is preferred that words start with a capital letter. For example, ABC:ClientX is the same as abc:clientx.
- There are no spaces before the colon.
- Spaces after the colon are allowed. For example, ‘ABC:ClientX’ is the same as ‘ABC: ClientX’.
- Markers are separated from each other and from the DSL by a comma followed by a space. For example, ‘DSL-3, Confidential, ABC: ClientX’.
- A single marker is not to be split over multiple lines.
- There is a strong preference for integrated markers to follow the case formatting used in this document. A physical stamp might use all capitals.
- There is a strong preference for adopted markers to be formatted based on the rules or guidelines of their defining document.

For more information on placing markers on documents, please see the Introduction: Labelling and marking.

5.2.6. Marker prefixes

Integrated markers

These markers do not have a prefix. For example, A Bright Company using the integrated marker **Confidential** with the label DSL-3 would use **DSL-1, Confidential**.

Adopted markers

These markers use an existing prefix defined under the adoption. Markers under the adopted Traffic Light Protocol would use the prefix of TLP. For example, A Bright Company might use **DSL-3, TLP:AMBER.**

User defined markers

User defined markers **must** include a prefix. Organisations or industries are free to define their own markers with a chosen prefix. The prefix should be chosen to help identify the organisation that has defined the marker. There is no way to formally register or reserve user defined markers or the prefix.

The prefix should only contain alphanumeric and period characters. If a long prefix can be tolerated, a unique prefix can be generated by using the reverse domain name notation for the organisation's domain.

For example, A Bright Company might use **DSL-3, ABC:ClientX**. In this example, **ABC** is the company acronym and is used as the prefix to identify ABC as the owner of the marker. **ClientX** is the marker which has a specific meaning defined by the company.

For guidance on how to use and combine DSL labels and markers, please see the Introduction: Labelling and marking.

For guidance on how to create markers, please see the IDCF website**.**

6.
Appendices

Appendix A: Glossary

The following glossary contains key terms and acronyms used in the IDCF accompanied by a meaning or definition. Some terms have been defined here based specifically on their meaning within the framework.

Term	Meaning/definition
Adversary	A person, group, organisation or government that conducts an adverse event. This is based on the NIST definition. Note that some frameworks refer to an adversary as a malicious actor.
Adverse event	An accidental or malicious event with a negative consequence that compromises the confidentiality, integrity and availability of data. A data breach is one type of adverse event. This is based on the definition in NIST SP 800-61r3.
AI	Artificial intelligence
APRA	Australian Prudential Regulation Authority
ASD	Australia Signals Directorate
ASIC	Australian Securities & Investments Commission
Assets	An item that is protected due to its perceived or actual value. Assets include data**,** information, systems, or infrastructure that have value to an organisation.
Authorised person event	The actions of authorised people with potential to cause an adverse event, for example, error or accident, social engineering, user focused cyber-events (phishing, unauthorised software), intentionally embedded employees and blackmail.
Availability	Timely and reliable access to data.
BIOS	Basic Input/Output System. Firmware in older computers to initialise hardware and initiate the boot process.
Classification	The process of placing data in a class. In the IDCF, this means applying a data security level (DSL) label and optionally applying markers based on a risk assessment.
Classified data	Data classified with a DSL. In the IDCF, this term does not mean data that has a government security classification.
Confidentiality	Preserving authorised restrictions on data access and disclosure, including means for protecting personal privacy and proprietary information. This is based on the NIST definition.
Consequences	The outcomes of an event. For example, identity theft might be a consequence of a loss of personal information.
Cryptographic key	A parameter used in conjunction with a cryptographic algorithm that determines its specific operation. An entity with knowledge of the key can reproduce or reverse such operation, while an entity without knowledge of the key cannot.

Term	Meaning/definition
Cyber event	Cyber (including network) actions with potential to cause an adverse event. **Common cyber event**: A transitory cyber event that utilises common techniques against published vulnerabilities. For example, exploitation of a well-known vulnerability in unpatched software (including operating systems). **Moderate cyber event**: An intentional cyber event over a short period (days) that utilises less common and/or targeted techniques. For example, identifying, targeting, profiling and engaging an employee with customised content to manipulate them to provide credentials or perform compromising actions. **Complex cyber event**: An intentional cyber event, possibly over an extended period (months or years). Significant effort is invested to achieve a specific aim, using highly skilled methods, and/or developing new techniques. For example, placing hidden entry points (backdoors) in software that will be used by an organisation. This entry point is later used to bypass standard security controls and gain unauthorised access to a system or application.
Data breach	The unauthorised movement or disclosure of sensitive private or business information, including personal information under the *Privacy Act 1988*. For more information see ASD's glossary and information on data breaches.
Data owner	The individual or organisation that owns or originally collected, curated, generated or classified the data.
Data protection	The process of safeguarding data from negative consequences that compromise its confidentiality, integrity and availability.
Data recipient	The individual or organisation that receives data from a data owner.
Declassify/declassification	The process of removing the classification from classified data to become unclassified data.
DSL	Data Security Level(s)
Event	An action, occurrence or change involving data that may cause an impact.
Event likelihood	The chance or probability, expressed qualitatively, of an event resulting in an adverse event.
FOCI	Foreign ownership, control and influence
Hacking	The gaining of unauthorised access to a computer network or electronic device.
IDCF	Industry Data Classification Framework
Impact	The level of harm expected to result from the consequence(s).
Industry	A collective term for many organisations operating in a common area of the economy and for all organisations together. For example, the health industry or Australian industry.
Inherent risk	The risk of an event before security controls have been implemented.
Integrity	A property whereby data has not been modified in an unauthorised manner since it was created, transmitted or stored. This is based on the NIST definition.

Term	Meaning/definition
IP	Intellectual property
Label	A visible indicator in physical or electronic form applied to data to communicate its DSL classification.
Labelling	The process of applying a label to data.
Likelihood of an adverse event	Technically this is the probability (qualitatively) of an event resulting in negative consequences (an adverse event). It is independent of the probability of the event. If an organisation experiences a higher frequences of events, the frequency of adverse events may increase.
LLMs	Large language models
Marker	A visible indicator in physical or electronic form, applied to data to communicate a secondary classification, such as specific handling, sensitivity or dissemination requirements.
Marking	The process of applying a marker to data. See the Markers module for more information.
Metadata	The information that describes the characteristics of data, such as its structure, for example data format, syntax, semantics, or its content, for example type of data, date or location of collection. This is based on the NIST definition.
Nationally important data	Data that in the case of an adverse event would have nationally significant impact.
National security	National security is about protecting our territory and institutions and ensuring the safety of all Australians. For more information, see PM&C's National security.
NCSC	UK National Cyber Security Centre
Need-to-know	The principle of restricting an individual's access to only the data they require to fulfil the duties of their role. This definition is from ASD's glossary.
NIST	US National Institute of Standards and Technology
Organisation	An entity. This includes a business, company, association, sole trader, partnership or government, for example Corporate Commonwealth Entities and State and Territory to the extent they can use the IDCF.
Physical event	Physical actions with potential to cause an adverse event. For example, theft, fire, physical access and the installation of unauthorised devices.
Protection/protective security	A combination of physical and cyber security measures to reduce the likelihood of an adverse event.
PSPF	Protective Security Policy Framework
Reclassify/reclassification	The process of changing a data's classification due to a change in its sensitivity, context or value, or due to changes in the risk appetite of the organisation holding the data. In the IDCF, this means changing the DSL label or a marker based on a risk assessment. Reclassification may be restricted to

Term	Meaning/definition
	the data owner, unless otherwise agreed. Declassification is a special case of reclassification (see definition above).
Risk	The likelihood of a consequence that may result in impact from an event.
Risk appetite	The amount of risk an organisation is willing to accept or retain in order to achieve its objectives. This is based on the definition in the PSPF which is derived from the Department of Finance Element 2: Risk Management Framework.
Security	When unqualified (no description of the type of security, for example 'national' security), it is an abbreviation for protective security as defined above.
Sovereign	Independent, supreme control and power, as found in the government of a state or nation.
Staff	An informal term for someone connected with the ownership or operations of an organisation, including a worker as defined under the *Work Health and Safety Act 2011*. This includes: • an employee • a contractor or subcontractor • an employee of a contractor or subcontractor • an employee of a labour hire company who has been assigned to work in the person's business or undertaking • an outworker • an apprentice or trainee • a student gaining work experience • a volunteer.
SME	Small and medium-sized enterprises
Thin client	A simple computer or software providing access over a network to a dedicated server. A thin client does not store or process data or applications locally. It only transmits inputs, such as keyboard and mouse events, to the server, then displays the server's outputs on a local monitor.
TLP	Traffic Light Protocol
Unclassified data	Data that has not been classified with a DSL. Such data may not have been risk assessed and may carry unknown risk. In the IDCF, this term does not mean data without security requirements.
UEFI	Unified Extensible Firmware Interface. Firmware in a computer to initialise hardware and initiate the boot process. The modern replacement for BIOS, see definition above.

Appendix B: Consequences questionnaire

This questionnaire can be used to identify potential consequences to your organisation if an adverse event occurs. Consider the data your organisation holds when completing this questionnaire.

Answering yes or unknown to any of the questions below may indicate potential risks to your organisation's data. The mitigation of these risks should be prioritised and/or further risk assessment should be undertaken.

Consequence type	Yes	No	Unknown
Privacy consequences			
Is this data impacted by the actions of individuals, for example customer records that can be handled by employees?	☐	☐	☐
Could something be inferred about an individual from the data?	☐	☐	☐
Does the data contain personal or sensitive information, for example names, addresses, health details or opinions about individuals, that is subject to privacy laws?	☐	☐	☐
Could individuals be harmed by the exposure of this data, for example identity theft, coercion and or/blackmail?	☐	☐	☐
Confidentiality consequences			
If this data were exposed, would sensitive or confidential information be disclosed to unauthorised parties?	☐	☐	☐
Could competitors, criminals or unauthorised users benefit from accessing this data?	☐	☐	☐
Reputational consequences			
Could an adverse event lead to a loss of trust or confidence in the organisation?	☐	☐	☐
Are there gaps in your organisation's planning for responding to adverse events?	☐	☐	☐
Would your organisation face challenges responding quickly and effectively to an adverse event?	☐	☐	☐
Legal consequences			
Would the exposure of this data violate any laws or regulatory requirements?	☐	☐	☐
Could your organisation face fines, lawsuits or regulatory investigations due to an adverse event?	☐	☐	☐
In the case of an adverse event, would the organisation require legal advice?	☐	☐	☐
Financial consequences			

Consequence type	Yes	No	Unknown
Could your organisation suffer significant costs from fines, legal fees or compensation claims?	☐	☐	☐
Would business losses, including damage to sales or customer relationships, result from an adverse event?	☐	☐	☐
Operational consequences			
Would the loss or theft of this data disrupt key business operations or processes?	☐	☐	☐
Could systems or staff be unable to function properly if access to this data was impacted?	☐	☐	☐
Strategic consequences			
Would the loss of this data affect your organisation's ability to achieve long-term goals or remain competitive?	☐	☐	☐
Could the adverse event lead to significant changes in business strategy or offerings?	☐	☐	☐
Security consequences			
If adversaries gained access to this data, could they use it to exploit vulnerabilities in other systems or networks?	☐	☐	☐
Would the exposed data provide an adversary with tools to launch further attacks on the organisation?	☐	☐	☐

For more information regarding types of consequences, please see the Risk Assessment module: Consequences of an adverse event.

Appendix C: Impact rating worksheet

This worksheet is designed to help organisations identify and assess the potential impact of an adverse event on their data before it is shared, stored or transmitted via email, cloud services or physical media.

By asking targeted questions across key aspects, such as individual harm, asset impact, operational disruption and other general consequences, this tool enables users to:

- better understand the value and sensitivity of their data
- identify potential consequences and impact of an adverse event
- determine an appropriate Data Security Level (DSL) for the data.

Your organisation can improve its ability to manage information and consistently meet compliance obligations by using this worksheet.

Complete sections 1 to 3 to determine the potential impact and harm of an adverse event to your organisation.

Section 1: Understanding your data

Understanding what type of data you are working with is the first step in assessing its value and potential consequences of an adverse event. This section gathers basic context about the type, structure and lifecycle of the data.

For more information on data types, please see the Risk Assessment module: Understanding your data.

1. Select the types of data you want to assess and classify from the list below.
   - ☐ Customer or client records
   - ☐ Employee information
   - ☐ Financial or accounting data
   - ☐ Health or medical data
   - ☐ Legal or contractual documents
   - ☐ Intellectual property or trade secrets
   - ☐ System or technical configuration information
   - ☐ Emails or unstructured communications
   - ☐ AI models or outputs generated by an AI model
   - ☐ Other:
2. Does the data include personal information, such as names and addresses?
   - ☐ Yes
   - ☐ No
3. Is the data current or is the data historical and/or archived?
   - ☐ Current
   - ☐ Historical or archived
   - ☐ Both

4. Is the data subject to any laws or regulations, for example *nationally important data,* which might require data to be physically stored at a location within Australia or controlled by an Australian organisation?

   ☐ Yes

   ☐ No

5. How significant is the size of this data in the context of your organisational operations? Consider the scale and value of the data with respect to your organisation.

   ☐ Entire organisation (> 75% of organisational data holdings)

   ☐ Large portion of the organisation (50% - 75% of organisational data holdings)

   ☐ Moderate portion of the organisation (25% - 50% of organisational data holdings)

   ☐ Small portion of the organisation (< 25% of organisational data holdings)

   ☐ N/A

Section 2: Consequences/impacts

This section provides a checklist that examines four major aspects of harm which may occur if the data is lost or compromised:

- harm to individuals, for example identity theft, coercion and/or blackmail
- harm to organisational assets, for example loss of IP
- harm to an organisation's operations, for example service disruption
- other harm to an organisation, for example fines or lawsuits.

Each area contains targeted questions to help users assess the severity of potential consequences and then assign an impact rating from very low to very high. When completing the section below, ask yourself the following question: *What could happen if this data was compromised?*

For more information, please see the Risk Assessment module: Consequences of an adverse event**.**

Harm to individuals

Describe the potential consequences or harm to people whose personal or sensitive information might be exposed or misused. Consider what could happen if this data was compromised and answer the following questions:

- Could the exposure lead to identity theft?
- Could it result in reputational damage to the individual?
- Could it cause financial loss to the individual?
- Could it lead to physical injury or death?

Please enter your answer here:

Based on the consequences identified, use the following scale to rate the harm to individuals.

☐ **Very low.** Very minor consequences that have little or no lasting effect on an individual. Often these are issues that can be quickly resolved with minimal effort or no harm.

☐ **Low.** Limited impact on an individual, typically easily recoverable. These are manageable consequences that may require minor interventions.

☐ **Moderate.** These consequences have a noticeable impact on an individual, requiring attention and resources to mitigate. There could be issues that might take some time to resolve.

☐ **High.** These consequences have a significant impact on an individual, either financially, reputationally, or operationally, and require substantial effort to mitigate.

☐ **Very high.** Severe impacts that could lead to irreparable damage, significant financial loss, or even the death of an individual. These are critical risks and require extensive mitigation strategies.

Harm to organisational assets

Describe the potential consequences or harm to your organisation's key resources such as data, intellectual property, systems or facilities. Consider what could happen if this data was compromised and answer the following questions:

- Could loss or exposure compromise your organisation's Intellectual Property?
- Could loss or exposure compromise the integrity of the data?
- Could loss or exposure impact your customers?

Please enter your answer here:

Harm to organisational operations

Describe the potential consequences or harm to your organisational operations. Consider what could happen if this data was compromised and answer the following questions:

- Could loss or exposure delay or disrupt an organisational function?
- Could loss or exposure affect decision-making or resource allocation?
- Could loss or exposure affect or degrade system performance?

Please enter your answer here:

Harm to an organisation in general

Describe the potential consequences or harm to your organisation in general. Consider what could happen if this data was compromised and answer the following questions:

- Is the data subject to privacy or sector-specific laws such as the *Privacy Act 1988*, *Security of Critical Infrastructure Act 2018* (Cth) (SOCI), Australian Prudential Regulation Authority (APRA)?
- Are there contractual or regulatory requirements governing how the data must be protected or used?
- Could exposure result in fines, audits or litigation?
- Could loss or exposure damage customer trust or stakeholder relationships?

Please enter your answer here:

Based on the consequences identified above for assets, operations and general categories, use the following scale to rate the harm to your organisation.

☐ **Very low.** Very minor consequences that have little or no lasting effect on your organisation. Often these are issues that can be quickly resolved with minimal effort or no harm.

☐ **Low.** Minor incidents that cause little disruption to your organisation and can be managed or corrected easily with minimal resources but don't disrupt core functions.

☐ **Moderate.** These consequences have a noticeable impact, requiring attention and resources to mitigate. There could be operational or reputational issues that might take some time to resolve.

☐ **High.** Significant consequences that disrupt operations or damage your organisation's reputation or financial health. These require urgent action and may take considerable time to recover from.

☐ **Very high.** Severe impacts that could lead to irreparable damage, significant financial loss or even the collapse of the organisation. These are critical risks and require extensive mitigation strategies.

Section 3: Your impact rating summary

This section brings your impact assessments together and can be used when selecting an appropriate DSL for your data.

For more information on impact ratings, please see the Risk Assessment module: Impact assessment**.**

Fill out the highest applicable rating for each category:

Harm to individuals	Choose an item.
Harm to your organisation	Choose an item.

Note: it is possible to use different approaches when selecting the impact rating to an organisation. For example, an organisation may **use the highest impact rating approach.**

This **conservative approach** involves selecting the **most severe rating** as the overall impact level across all assessed impact areas. For example, assets, operations, legal and reputational. This method ensures that even if only one area suffers significant harm or consequences, the organisation treats the incident with appropriate seriousness. It **prevents underestimating the overall risk** by ensuring that critical effects in one domain are not overlooked due to lesser impacts in others.

Another approach would be to use a method with a composite score, like that provided by National Institute of Standards and Technology (NIST) FIPS 199 publication.

Appendix D: Adverse event identification questionnaire

This questionnaire is designed to help understand the types of adverse events that could affect or compromise the data handled by your organisation. The aim is to raise awareness of potential events and support better data classification and risk management decisions.

If you answer yes or unknown to any of the below questions, then this is a risk to the organisation and should be addressed.

Adverse event type	Yes	No	Unknown
Physical events			
Are laptops, phones or USB drives unencrypted?	☐	☐	☐
Are laptops, documents or portable drives ever left in unlocked areas or vehicles?	☐	☐	☐
Does paper or devices ever get thrown away without securely wiping or shredding them?	☐	☐	☐
Authorised person events: Insider threats			
Do employees of your organisation have access to sensitive or valuable data in your system?	☐	☐	☐
Do those people with access have a valid need-to-know to access the data?	☐	☐	☐
Could an insider (employee, contractor) misuse or leak this data?	☐	☐	☐
Do external vendors or contractors access your systems or data?	☐	☐	☐
Authorised person events: Human error			
Could someone accidentally send sensitive data to the wrong person, for example to the wrong email address?	☐	☐	☐
Are files or folders ever sent or shared outside your team or organisation?	☐	☐	☐
Cyber events: Unauthorised access			
Can data in your system be downloaded or copied without approval or logging?	☐	☐	☐
Is the data accessible through unsecured networks, such as the internet or third-party mobile applications?	☐	☐	☐
Do team members sometimes share accounts or logins to save time and money?	☐	☐	☐
Cyber events: Social engineering attacks			
Have you or other employees received emails pretending to be from trusted contacts?	☐	☐	☐

Adverse event type	Yes	No	Unknown
Have you or other employees been asked to verify a password or payment details through email or phone unexpectedly?	☐	☐	☐
Cyber events: Malware and ransomware			
Could a cybercriminal profit from accessing your data? For example, by selling, leaking or ransoming it.	☐	☐	☐
Have you or other employees received suspicious emails or noticed strange activity? For example, phishing emails asking you to click a link or confirm your details, unexpected logins, unexplained file changes, new users appearing in your system, your computer slowing down, or access from unfamiliar locations.	☐	☐	☐
Could USBs be plugged in to a device or email attachments opened without any scanning or checking?	☐	☐	☐
Cyber events: Network and security attacks			
Have you or other employees ever accessed work-related data using public Wi-Fi or an unsecured network?	☐	☐	☐
Do you or other employees manage any databases that are accessible through web applications, Application Programming Interfaces (APIs) or public-facing portals?	☐	☐	☐

For more information regarding types of consequences, please see the Risk Assessment module: Consequences of an adverse event.

Appendix E: Statement of System Security

Industry Data Classification Framework Statement of System Security	
Organisation name:	**System appropriate to (DSL):** DSL-X
Person responsible:	Assessment type: ☐ Internal ☐ External

System description:

E.g. The system consists of company Windows 11 laptops and Microsoft 365 cloud-based tenancy. Laptops are enrolled and managed through Microsoft Intune.

Assessment basis:

E.g. Self-assessment with system setup based on ….

General basis of security implementation: (select all that apply)

- ☐ Essential Eight Maturity Level ____
- (Physical and authorised user controls required)
- ☐ CIS Controls Implementation Group _____
- ☐ Google Workspace with CIS IG ___
- ☐ Other
- ☐ ISM controls applicability (NC/OS/P/S/TS) _____
- ☐ Microsoft 365 with Essential Eight Maturity Level _____
- ☐ Amazon Web Services Cloud Adoption Framework: Phase _____

Hardware:

Laptop measures:

E.g. Bitlocker, MFA, Domain and Cloud based management or remote erasure.

Mobile phone measures:

E.g. encrypted, biometric lock, enrolled in device management, automatic lock on theft detection, remote locking and erasure.

Other hardware:

E.g. USB storage device: physical protection only.

Description of physical controls:

Description of cyber controls: *E.g. We follow ACSC Essential Eight with a focus on implementing Essential Eight Maturity level 2. All controls in that document have been implemented.*
Description of authorised user controls:
Prepared by:
Assessor details: (Only required if externally assessed. Please attach reports.)

Appendix F: References

Australian Government

- Australian Charities and Not-for-profits Commission
    - Governance Toolkit: Cyber Security (https://www.acnc.gov.au/for-charities/manage-your-charity/governance-hub/governance-toolkit/governance-toolkit-cyber-security)
- Australian Prudential Regulation Authority
    - Prudential Standard CPS 234 Information Security (https://www.apra.gov.au/information-security)
    - Prudential Practice Guide CPG 234 Information Security (https://www.apra.gov.au/information-security)
- Australian Signals Directorate, Australian Cyber Security Centre
    - Deploying AI systems securely (https://www.cyber.gov.au/business-government/secure-design/artificial-intelligence/deploying-ai-systems-securely)
    - Email security (https://www.cyber.gov.au/protect-yourself/securing-your-email/email-security)
    - Essential Eight maturity model (https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight/essential-eight-maturity-model)
    - Essential Eight maturity model Appendix D: Comparison of maturity levels (https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight/essential-eight-maturity-model)
    - Exercise in a Box, Be business ready for a cyber incident (https://www.cyber.gov.au/business-government/exercise-in-a-box)
    - Foundations for modern defensible architecture (https://www.cyber.gov.au/business-government/secure-design/secure-by-design/modern-defensible-architecture/foundations-for-modern-defensible-architecture)
    - Glossary (https://www.cyber.gov.au/learn-basics/view-resources/glossary)
    - Guidelines for email (https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism/cyber-security-guidelines/guidelines-for-email)
    - Guidelines for personnel security (https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism/cyber-security-guidelines/guidelines-for-personnel-security)
    - Information security manual (https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism)
    - Infosec Registered Assessors Program (IRAP) (https://www.cyber.gov.au/business-government/protecting-devices-systems/assessment-evaluation-programs/irap)
    - Mitigating cyber security incidents (https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/mitigating-cyber-security-incidents)
    - Securing customer personal data (https://www.cyber.gov.au/business-government/small-business-cyber-security/securing-customer-personal-data)
    - Threats (https://www.cyber.gov.au/threats)
    - Traffic Light Protocol (TLP) (https://www.cyber.gov.au/tlp)
    - What is a data breach? (https://www.cyber.gov.au/threats/types-threats/data-breaches)

- Data.gov.au
    - Risk Key Concepts, Confidentialised data definition (https://data.gov.au/data-integration/risk/key-concepts)
    - Data integration (https://data.gov.au/data-integration/risk/key-concepts)
- digital.gov.au
    - Risk assessment and mitigation plan (https://www.digital.gov.au/policy-toolkit/resources/risk-assessment-and-mitigation-plan)
- Department of Finance
    - Commonwealth Risk Management Framework (https://www.finance.gov.au/government/comcover/commonwealth-risk-management-framework)
    - Element 2: Risk Management Framework (https://www.finance.gov.au/government/comcover/risk-services/management/risk-management-toolkit/element-2-risk-management-framework)
- Department of Home Affairs
    - *2023-2030 Australian Cyber Security Strategy* (https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy)
    - Cyber and Infrastructure Security Centre, Risk Assessment Advisory for Critical Infrastructure Data Storage or Processing Sector (https://www.cisc.gov.au/resources-subsite/Documents/raa-data-storage-or-processing.pdf)
    - Data retention obligations (https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-retention-obligations)
    - Foreign Ownership, Control or Influence (FOCI) Risk Assessment Guidance (https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/technology-and-data-security/foreign-ownership-control-or-influence-risk-assessment-guidance)
    - Industry Data Classification Framework (https://www.IDCF.gov.au)
    - Protective Security Policy Framework (https://www.protectivesecurity.gov.au)
- Department of the Prime Minister and Cabinet
    - National Security (https://www.pmc.gov.au/international-policy-and-national-security/national-security)
- National Archives of Australia
    - Australian Government Recordkeeping Metadata Standard (https://www.naa.gov.au/information-management/standards/australian-government-recordkeeping-metadata-standard)
- Office of the Australian Information Commissioner
    - Guide to undertaking privacy impact assessments (https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/privacy-impact-assessments/guide-to-undertaking-privacy-impact-assessments)
    - eLearning on conducting a privacy impact assessment (https://education.oaic.gov.au/elearning/pia/welcome.html)
    - Notifiable data breaches (https://www.oaic.gov.au/privacy/notifiable-data-breaches)
    - What is a data breach? (https://www.oaic.gov.au/privacy/your-privacy-rights/data-breaches/what-is-a-data-breach)

- What is personal information? (https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/what-is-personal-information)

International Governments

- Cyber Security Agency of Singapore
  - Guide to conducting cybersecurity risk assessment for critical information infrastructure, February 2021 (https://www.csa.gov.sg/legislation/supplementary-references/#93de221cd42f76b049be7491c03db86e)
- New Zealand Government
  - Risk Assessment Process Report Template (https://www.digital.govt.nz/assets/Standards-guidance/Governance/Risk-Assessment-Process-Template.docx)
- DIGITAL.GOVT.NZ
  - Setting up a successful risk assessment (https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/risk-management/risk-assessments/setting-up)
- United States Department of Commerce, National Institute of Standards and Technology (NIST)
  - Cybersecurity Framework (https://www.nist.gov/cyberframework)
  - Glossary (https://csrc.nist.gov/glossary)
  - Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments (https://csrc.nist.gov/pubs/sp/800/30/r1/final)
  - Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations (https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final)
  - Special Publication 800-61 Revision 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf)
  - Standards for Security Categorization of Federal Information and Information Systems, FIPS 199 (https://csrc.nist.gov/pubs/fips/199/final)
- United Kingdom National Cyber Security Centre
  - Risk management (https://www.ncsc.gov.uk/collection/risk-management)
  - Risk management, A basic risk assessment and management method (https://www.ncsc.gov.uk/collection/risk-management/a-basic-risk-assessment-and-management-method)
  - Risk management, The fundamentals and basics of cyber risk (https://www.ncsc.gov.uk/collection/risk-management/the-fundamentals-and-basics-of-cyber-risk)

Other

- Amazon Web Services
  - AWS Prescriptive Guidance, Reaching Essential Eight maturity on AWS (https://docs.aws.amazon.com/pdfs/prescriptive-guidance/latest/essential-eight-maturity/essential-eight-maturity.pdf)
  - Operational Best Practices for ACSC Essential 8, conformance template (https://docs.aws.amazon.com/config/latest/developerguide/operational-best-practices-for-acsc_essential_8.html)

    - Security Maturity Model v2 (https://maturitymodel.security.aws.dev/en/model/)
- Australian Energy Market Operator
    - Australian Energy Sector Cyber Security Framework (https://www.aemo.com.au/initiatives/major-programs/cyber-security/aescsf-framework-and-resources)
- Center for Internet Security
    - CIS-CAT® Lite tool, Test your Security Configuration (https://learn.cisecurity.org/cis-cat-lite)
    - CIS Critical Security Controls Version 8.1 (https://learn.cisecurity.org/control-download-v8-1)
    - CIS Google Workspace Benchmark (https://www.cisecurity.org/benchmark/google_workspace)
- FIRST Standards Definitions and Usage Guidance Version 2.0
    - Traffic Light Protocol (https://www.first.org/tlp/)
- Information Security Management Systems
    - ISO/IEC 27001:2022 (https://www.iso.org/standard/27001)
    - ISO/IEC 27002:2022 (https://www.iso.org/standard/75652.html)
- Microsoft
    - Configuration guidance for Windows 365 aligned to the ASD Blueprint (https://learn.microsoft.com/en-us/compliance/anz/blueprint-windows365)
    - Microsoft Guide, ACSC Essential Eight (https://learn.microsoft.com/en-us/compliance/anz/e8-overview)
- MITRE ATT&CK
    - Matrix for Enterprise (https://attack.mitre.org/)
- Office of the Victorian Information Commissioner
    - Practitioner Guide: Information Security Risk Management V2.0 (https://ovic.vic.gov.au/resource/practitioner-guide-information-security-risk-management/)
- Royal Australian College of General Practitioners
    - Performing a threat analysis (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/prevention-and-risk-assessment-1/performing-a-threat-analysis)