July 2023
16/F2 v2

High-value and high-risk information and records

1. Define your high-value and high-risk information and records

How your organisation defines its high-value and high-risk information and records depends on its business. This definition should include those information and records needed to carry out your organisation's core functions, make key decisions, and provide future evidence of these.

2. Identify your high-value and high-risk information and records

High-value information and records include those that are critical to your core business – for example, information and records about how your organisation performs legislated functions.

High-risk information and records include those that pose a risk to the way your organisation operates, its business transactions, and how it interacts with other organisations and manages relationships with clients and employees. Poor management of these risks may expose your organisation to major loss of reputation, financial or material loss, or breach of statutory obligations.

For example, your organisation may have business functions that generate high-value and high-risk information and records if it:

- receives significant investment from Government
- makes major contributions to the economy
- performs an activity that impacts on individuals (such as a regulatory, enforcement, health or welfare protection activity where disputes may arise)
- develops policy that will impact on individuals and communities or rights and entitlements
- manages natural resources, the protection and security of the state, or its infrastructure
- uses processes that are targets of corruption or offer potential for corrupt behaviour
- undertakes a major programme of international or national significance.

Useful sources for identifying high-value and high-risk business functions include your organisation's:

- risk register
- internal and external audit reports
- risk or governance reports
- information and record asset registers.

Make sure you also evaluate high-value information and records that are created by routine business functions. Routine business functions can create information and records that may have value beyond their initial business need, such as public accountability or cultural heritage.

We have issued general disposal authorities (GDAs) that apply to the common corporate functions and activities of many public sector organisations including those functions and activities that may generate high-value information and records.

3. Document your high-value and high-risk information and records

You should document or register your organisation's high-value and high-risk information and record assets in enough detail so they are easily found in future. When documenting them, you could include the following details:

- the extent of the asset – information and records can exist as many interconnecting data sources so you should document what is part of the asset and what is not
- the business unit responsible for the asset, and its accountability
- the business function it supports

- the software and hardware for maintaining this asset – the technology that it may depend on to be accessible
- its dependency on other assets – the separate internal or external information sources necessary for understanding the information asset and its high-value/high-risk uses.

Ensure that your organisation's metadata and audit logs are complete and that the contents match their description.

4. Manage your high-value and high-risk information and records

4.1. Have a plan for long-term management

Taking a strategic and planned approach to managing your organisation's high-value and high-risk information and records is essential to the successful management of these assets over time.

You should have a plan for identifying and documenting high-value and high-risk information and records assets with a level of detail appropriate for their business context and relevant to their size and complexity. This plan should cover not only your immediate needs but also provide a long-term strategy for the management of these assets over time. For example, where the need for the information and records will outlast the life of the system(s) in which they are created and held.

When your organisation no longer has an immediate need for high-value and high-risk information and records, you should routinely export or migrate them to a system suitable for long-term management. You need to ensure that the migration process includes the minimum metadata required to support any long-term accountability needs for evidence of your organisation's business functions and activities.

If your organisation is using software-as-a-service such as cloud computing, you need to make sure that the services are contracted to provide long-term information and records management.

You should also ensure that any disposal processes, such as destroying or archiving information and records, are well managed so that they do not create risks themselves. You should identify and monitor any gaps and shortcomings in your disposal processes. High-risk information and records can sometimes be overlooked in these processes if an assumption is made that the information and records, for example:

- exists when it may not
- sufficiently documents the activity when it may not
- is sufficiently well managed when it may not be.

Your organisation's management of its high-value and high-risk information and records should contribute to its wider risk management frameworks such as those based on ISO 31000 Risk Management.

4.2. Personal information and records

You need to give particular attention to the capabilities of systems that manage personal information and records as these can expose your organisation to significant risk. There are strict legislated rules governing how organisations may retain personal data, how they may use this data, and their ability to report on these both to the individual concerned and to oversight bodies such as the Privacy Commissioner. You need to be aware of these requirements and ensure that any systems managing personal information and records are appropriately secure.