High value and high risk information and records

1 Defining high value and high risk information and records

How organisations define high value and high risk information and records depends on the organisation's business. It will include the information and records needed to carry out core functions, to make key decisions, and to provide future evidence.

2 Identify high value and high risk information and records

High value information and records may include the information and records critical to core business – for example, information and records about how the organisation performs legislated functions, and specify and document core assets.

High risk information and records may be information and records that would risk the way the organisation operates, its business transactions, and how it interacts with other organisations and manages relationships with clients and employees. Poorly managing risks may expose the organisation to major loss of reputation, financial or material loss, and breach of statutory obligations.

For example, an organisation may have business areas that generate high value and high risk information and records because it:

- receives significant investment from Government
- makes major contributions to the economy
- performs direct activity that impacts on individuals (for example, 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 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 include the organisation's:

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

Also evaluate high value information and records that are created by routine business functions. Routine functions can create information and records that have high value beyond its initial business need, such as for accountability, or as a permanent archive.

Archives New Zealand has issued general disposal authorities that apply to the common corporate functions and services of many organisations. These authorities identify the functions undertaken by many organisations that may generate high value information and records.

3 Document high value and high risk information and records

Organisations should document 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 extent of the asset – information and records can exist as many interconnecting data sources, so document what is part of the asset and what is not
- the business unit responsible for the asset, and its accountability
- its business function
- the software and hardware for maintaining this asset – the technology that this asset may depend on to be accessible
- its dependency on other assets – the separate internal or external information sources for understanding an information asset and its high value/high risk uses.

Ensure that metadata and audit logs are complete and contents match their description.

4 Manage 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 high value and high risk information is essential to the successful management of these assets over time.

Organisations should have a plan for identifying and documenting high value and high risk information and records with a level of detail appropriate for their business context and in accordance with their size and complexity. Organisations should ensure that the plan covers immediate needs but also provides a long-term strategy for the management of these assets. The system on which the information and records was created and is held is usually unsuitable for long-term management, because the need for the information and records will outlast the life of the system.

When the organisation no longer has an immediate need for high value and high risk information and records, export them to a system suitable for long-term management. Organisations should do this routinely. Organisations should ensure that the migration process includes reliable data to support long-term needs for accountability, evidence of the significance of the business processes, and their archival value.

If the organisation uses software-as-a-service such as cloud computing, they need to make sure that the system will provide long-term information and records management. Organisations should identify the high value information and records in the system, and the record of actions that are required.

Organisations should ensure that the process for archiving information and records is well managed so that it does not create risks itself. Organisations should identify gaps and shortcomings in archiving processes. High risk information and records can be overlooked because the organisation assumes that the information and records:

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

The organisation’s management of high value and high risk information and records should contribute to the overall risk management frameworks such as those based on ISO 31000 Risk Management.

4.2 Managing personal information and records

Particular attention should be given to the capabilities of systems that manage personal information and records. Personal information and records that are unable to be managed appropriately exposes the organisation to significant risk. There are strict rules governing how an organisation may retain this data, how they may use this data, and their ability to report on these both to the individual concerned and to oversight bodies. Organisations should be aware of these limitations, and ensure that systems managing personal information and records are especially secure.