Records Management Risk Assessment
Offsite data storage

Australian Government | NATIONAL ARCHIVES OF AUSTRALIA

Your story, our history

This template lists the principal records management risks that may need to be considered when choosing offsite data storage. Agencies can conduct a risk assessment using this template, or they may use the information it contains as the basis for populating their own template.

Only common records management risks are addressed in this template.

Agencies may have other records management risks that apply specifically to their business functions. In addition, other general risks relating to outsourcing and data storage will need to be considered.

Other sources of advice include:

- *Outsourcing digital data storage: Storing Commonwealth records in Data Centres, Digital Repositories and in the Cloud*
- *Risk Management: principles and guidelines* (Australian Standard for Risk Management, AS/NZS ISO 31000:2009)
- 'Security risk management', *Australian Government Protective Security Policy Framework* (Attorney-General's Department)
- Advice on Managing the Recordkeeping Risks Associated with Cloud Computing (Australasian Digital Recordkeeping Initiative)
- Australian Government Data Centre Strategy 2010–2025 (Department of Finance and Deregulation and Australian Government Information Management Office)
- Records Issues for Outsourcing including General Disposal Authority 25 (National Archives of Australia)
- National Archives of Australia's general advice on outsourcing.

This template outlines five principal records management risk categories. Within each category, specific risks are listed. Each risk is accompanied by suggested triggers and questions that may aid understanding of the risk and help to evaluate its likelihood and impact. There is also a section for other risks identified by an agency.

Date of assessment:

Purpose of assessment:

Background:

Information recorded here would include, for example, the storage option suggested (data centre, digital repository or cloud), the provider company background, and the type and quantity of information to be stored.

1 Compliance and governance risks

Data held in multiple jurisdictions	Where is your data? Does it matter if it is not in your jurisdiction?
Unclear asset ownership	Is it clear who owns your data (including metadata)?
Breach of regulatory requirements	Is the storage of the data in breach of any relevant legislation?
Audit management	Are controls sufficient to prove, for example, that information has not been tampered with? Are audit logs managed and maintained for a sufficient period of time?
Contract lock-in	Does choosing a particular provider mean that you are required to use particular software, hardware, etc.? Could you move easily between providers?
Unclear roles and responsibilities	Are roles and responsibilities defined?

Other risks	

Risk assessment		
Likelihood	*Consequence*	*Risk rating*

2 Technical risks

Loss of readability and usability	Consider, for example, hardware and software compatibility, format changes, and migration issues.
Network breaks	What are the procedures and priorities during a network break?
Disruptions	What are the chances of service disruptions?
Backups	What is the backup plan, how often are backups taken, how long are they kept?
System monitoring	Is monitoring of systems sufficient for the value of information stored (for example, intense monitoring for vital information)? How long would it take to be aware of systems being breached, failing or otherwise disrupted?
Disaster recovery plan	Is there a disaster recovery plan? Is this sufficient for the data stored?
Insecure or ineffective deletion of data	What are the risks if a copy of your data remains with the provider? Is it possible for data stored to be deleted to the level required?
Ability to retrieve data	Can you easily retrieve your data in a timely manner?
Network congestion	With more people using the service, will the service slow down? Whose data has priority?

Other risks

Risk assessment

Likelihood	*Consequence*	*Risk rating*

3 Access risks

Unauthorised access	Who can access your data? How will you know?
Authentication and authorisation	What controls are in place? What form of authentication is used? Who has authorisation to give access?
Loss of access	Consider, for example, adequacy of backups, and what happens if the company goes out of business.
Legal • Subpoena • Discovery	Who else is using servers you may use? If the server is subpoenaed by another organisation could your data be accessed? Would you have access to your data during the subpoena process?
Security • Physical security • Data and network security	Consider location, monitoring arrangements (physical and virtual), firewall protection, session management, etc. What policies and procedures need to be in place to satisfy your data security requirements? Have you consulted the Australian Government Protective Security Policy Framework and the Australian Government Information Security Manual?

Other risks	

Risk assessment		
Likelihood	*Consequence*	*Risk rating*

4 Data loss risks

Metadata mismanagement	Is process metadata sufficient for evidential and security purposes? Are both the data and metadata managed?
Ability to restore data	Is there a possibility data may be corrupted? Is there a process for restoration? Which data take priority?
Return of records	Is this in the contract? Is there a time period set for compliance?
Physical environment	Consider what mitigation elements are in place, for example, alarms, ventilation, and other environmental controls.

Other risks	

Risk assessment		
Likelihood	*Consequence*	*Risk rating*

5 Provider organisational risks

Third party subcontracting	Is any use of cross-provider services transparent? Are they covered by the contract conditions? Does this affect the security of your data?
Storage provider ‘health’	Could the provider go out of business?

Other risks	

Risk assessment		
Likelihood	*Consequence*	*Risk rating*