Digital Continuity Plan

Ensuring that your business information remains accessible and usable for as long as it is needed

Australian Government
National Archives of Australia

Your story, our history

Accessible and usable information
Digital continuity

Digital continuity is an approach to keeping and managing digital information to ensure that it can be used in the way that is required for as long as required, and no longer.¹

‘Digital continuity ensures information is complete, available and useable by those with a need for it. It also ensures the information is not kept for longer than needed. Information is useable when you can:

• find it when you need it
• open it when you need it
• work with it in the way you need to
• understand what it is and what it is about, and
• trust that it is what it says it is’.²

Why is digital continuity important?

Government information is both a valuable national resource and a key business asset. For government agencies, information is fundamental to the efficient, effective, transparent and accountable conduct of government business.

For more than a decade, government policy has preferred that services and information be provided to citizens by digital means. Recent policy initiatives such as the Declaration of Open Government and legislative changes are accelerating the requirement. Many government agencies have been using office productivity software and business systems for over 20 years, so creation and internal use of digital information has been mainstream in most agencies for a considerable time.

Effective digital information management improves business outcomes through a range of benefits and other efficiencies, it increases efficiency, improves accountability and legal compliance, and reduces risk.

Your agency can use this document and other more detailed advice to formulate and implement a plan to address digital continuity. Your plan should include a staged or incremental approach to digital continuity, addressing areas of highest business priority and business risk first.

Benefits of digital continuity to your business

Benefits of digital continuity include:

• more efficient and effective business processes
• increased transparency of business activities and greater accountability to government, stakeholders and the community
• reduced storage and other costs
• reduced risks to business of unusable or lost information
• ability to meet the intent of whole-of-government policies.

About the Digital Continuity Plan

The Digital Continuity Plan, based on six Digital Continuity Principles will help agencies to achieve business benefits, including efficiencies and mitigation of risks. Agencies should also see the Office of the Information Commissioner’s Principles on Open Public Sector Information which relate to aspects of digital continuity.

The Digital Continuity Plan:

• identifies the practical outcomes that arise from the Digital Continuity Principles and suggests key actions to achieve these outcomes
• assists all agencies in the ongoing management of digital information while allowing them to address agency-specific requirements and optimise benefits
• links to more detailed advice on how to carry out each action, and identifies useful tools where appropriate.

The plan was developed by the National Archives in consultation with a number of Australian Government agencies.
Elements of digital continuity

Digital continuity
Keeping and managing digital information to ensure it can be used in the way that is required, for as long as required, and no longer.

Digital Continuity Principles
The critical features of effective digital continuity

1. The value of digital information as a business, evidentiary and community resource is understood and the information is managed accordingly.
2. The governance of digital information is integrated with agency governance, with roles and responsibilities clearly defined and allocated.
3. Digital information is authentic and reliable.
4. Digital information is discoverable, accessible and usable.
5. Digital information is managed digitally.
6. Digital information is managed, protected and preserved for as long as required and then disposed of appropriately.

Further information on the Digital Continuity Principles is available on the National Archives website naa.gov.au.

Digital continuity outcomes

• Benefits of digital information to your business, the government and the community are optimised.
• People, processes and technology are aligned to support effective information management.
• Information is fit-for-purpose over its life.

Digital Continuity Plan
Key actions to achieve the outcomes

The key actions in the Digital Continuity Plan are aimed at achieving these outcomes.

Practical guidance
Digital continuity and digital transition
Digital continuity is an approach that focuses on continued management of information that is already in a digital format.

Digital transition addresses the transition from paper and other physical formats to digital formats. Under the digital transition approach, digital formats are preferred over paper formats when reviewing processes or undertaking new initiatives or change.

Advice on making the transition from paper-based information to digital information is available on the National Archives website naa.gov.au.

Key actions
These actions make up the Digital Continuity Plan and are intended to help agencies to achieve the digital continuity outcomes. The actions are not intended as a step-by-step process or as a "one size fits all" solution. Agencies should develop their own staged plans for achieving digital continuity, informed by Check-up 2.0 assessments and shaped by their particular business priorities and risks.

Focus on the business
Outcome: benefits of digital information to your business, the government and the community are optimised.

- Review your information to understand what information your agency creates, uses and holds and identify accountabilities, opportunities, compliance obligations, cost, value and risks.
  - Develop action plans to address the highest priority issues raised by the information review.
  - Regularly update and evaluate the information gathered in the review.

Focus on people, processes and technology
Outcome: people, processes and technology are aligned to support effective information management.

- Establish a governance framework for digital information which is aligned and integrated with agency governance.
- Define, assign and resource accountable digital information management roles, including senior responsibility.
- Inform, train and support users of information.
- Provide processes, systems and tools that can support effective management and use of information.
- Monitor and review ongoing management of digital information against agency objectives.

Focus on the information
Outcome: information is fit-for-purpose over its life.

- Define, assign and manage appropriate metadata.
- Provide digital information in a format that is accessible and usable.
- Ensure digital information can be exchanged among systems and agencies, and with the community.
- Establish a system of ongoing checks to ensure that digital information remains usable.
- If information is already in a digital format, continue to manage it in a digital format.
- Plan and implement an ongoing program to dispose of information in accordance with the Archives Act 1983 and other legislation.
Focus on the business

Digital information is created, captured and used in the conduct of agency business. Proper management of digital information is not only important for accountability and compliance; it also improves operational and strategic outcomes and provides benefit for government, citizens and other stakeholders.

Review your information to understand what information your agency creates, uses and holds and identify accountabilities, opportunities, compliance obligations, cost, value and risks.

The purpose of an information review is to identify the information that is needed to optimise the achievement of organisational objectives, who it is needed by, how it will be used, its source and how it flows through the organisation and between the organisation and its external environment.3

An information review is carried out to document the digital information created, captured and used in conducting agency business and establish its cost and value. The review also identifies opportunities for use of the information and gaps in information management that will then guide improvement plans.

Ideally, the review should cover business information in all formats across the agency because it can identify opportunities for transforming business processes from reliance on paper to digital formats. However, it is important to ensure that the information reviewed is of material importance to the business so that the cost and effort of the review are worthwhile.

The information review can cover the whole agency in one pass or take an incremental approach, focusing first on those areas of agency business with the highest priority or risk. Periodic reviews, audits, system upgrades and other procurement activities also provide opportunities to review information holdings.

Results of an information review can be used to create an ongoing information asset register (as outlined in the Office of the Australian Information Commissioner’s Open Public Sector Information Principles).
Information in use
When determining what digital information is being created, captured and kept, consider why it is created and where it may be stored. ‘Digital information’ may refer to business transactions, decisions, agenda papers, minutes, advice, policy statements, procedures and a range of other materials. It may be found in many systems including databases, business systems, email accounts, shared folders and hard drives. However, regardless of the type, format or location of the information, it is important that digital information is managed according to its value.

The National Archives provides guidance on the types of digital information to consider and the systems that create, keep and manage digital information. Advice on storing digital records is also relevant.

Accountabilities
An information review should clarify who is responsible and accountable for the digital information that is identified.

Opportunities
An information review may help agencies to identify better strategic or operational outcomes. For example it can:

- identify opportunities for improvement through analysis of strategic or operational performance information
- lead to more effective services to government, citizens and other stakeholders by providing better quality information, better informed and more consistent decisions, better use of information among systems or agencies, or faster responses
- identify opportunities to remove duplicated information
- lead to more efficient services by improving access to required information or information flows.

Agencies can also realise benefits by transitioning to digital information management.

Compliance obligations
A good understanding of the legal, policy, contractual and other obligations imposed on the creation, capture, management and use of information is essential for accountability and managing risk.

Compliance obligations can cover a range of aspects of information management including:

- capture, creation, management and destruction or retention of records and information
- privacy and security of information
- use of information
- disclosure, discovery, sharing and publication of information.

A good starting place to identify accountabilities is legislation that affects how your agency manages its information and information needed for legal proceedings.

Cost and value
It is important to understand the cost and value of the information that is created, captured and used. The value of digital information may vary throughout its life depending on:

- business requirements (the need for accountable and transparent decision-making within agencies)
- government requirements (the need to meet policy initiatives or fulfill compliance obligations)
- community obligations (the need for information to be made available to the community for use or reuse in innovation, research or projects, and the level of transparency required).

The Office of the Australian Information Commissioner issues paper entitled Towards an Australian Government Information Policy states, ‘the value of information is generally increased, rather than decreased, by making it available. It is therefore in the national interest to get maximum value from public sector information by making it publicly available for creative reuse.’
In this context, cost and value are not necessarily financial, although it is helpful to assign indicators of relative importance, such as ‘major significance’ or ‘vital’, so that priorities for action and investment in risk mitigation can be assessed. A good example of a non-financial approach to the value of information is the business impact levels in the Australian Government Protective Security Governance Management Guidelines.

**Risks**

Effective digital information management will reduce risks. Two types of risk should be considered:

- the risks associated with business activities
- the risks associated with managing digital information.

Further information on managing risks is available on the National Archives website naa.gov.au.

**Develop action plans to address the highest priority issues raised by the information review**

Actions on any gaps and opportunities identified in the information review need to be prioritised. The initial information review provides a baseline for monitoring progress.

**Update and evaluate the information gathered in the review regularly**

The information gathered for the review can be useful in the ongoing governance of digital information. Reviews should be conducted periodically to make sure that the information remains current and useful, progress is tracked and further issues are identified, and incorporated into your agency’s governance framework.
To ensure digital continuity, the vital organisational elements of people, processes and technology must be aligned.

Establish a governance framework for digital information which is aligned and integrated with agency governance

A digital information governance framework outlines how information assets are to be managed to support agencies’ outcomes. The governance framework identifies and addresses risk and compliance issues and optimises the value of the information for as long as it is required.

“The way Government information is used, communicated and stored is critical to the operations of the Australian Government and has implications for privacy, copyright, knowledge management, security, history and accountability.”

To effectively manage digital information, digital continuity needs to be integrated with existing agency governance. Governance of digital information should be included into governance areas such as:

- ICT
- security
- risk
- business continuity
- accountability.

This could involve considering information management requirements into mechanisms such as ICT project gateway reviews.

The Office of the Australian Information Commissioner’s Principles on Open Public Sector Information recommends effective information governance.
Define, assign and resource accountable digital information management roles, including senior responsibility

To manage digital information effectively, various roles need to be performed. These must be clearly identified and assigned, and adequately resourced.

Accountability for digital continuity and implementation of the Digital Transition policy should be assigned to a member of senior management.

Specialist information management roles include strategic oversight of digital information and operational aspects such as access control, information quality and conformance with standards, obligations and commitments.

All staff create, maintain and use digital information as part of their work activities. It is essential that they are provided with clear and detailed information on correct processes and ongoing education so that information is managed effectively and efficiently.

As the work environment changes, including by staff turnover, the roles and skills of information management specialists need to be reviewed. In some cases additional training and resources may be needed.

More information on information management roles and advice on helping staff with their records management responsibilities is available on the National Archives website naa.gov.au.

Inform, train and support users of information

The easier it is for users to understand, use and manage the processes and technology, the more effective their information management will be. A number of steps can be taken to support users:

- Give users ongoing support and education about correct processes.
- Consider ways to encourage good digital information management behaviour and provide positive reinforcement and role models.

This might involve:

- providing induction training for new starters on issues such as records management, email management, information security, privacy and ethical use of information
- providing advice and guidance to staff on more effective ways to find, use or manage information
- incorporating information management responsibilities into individual performance agreements
- incorporating relevant information management requirements into local work procedures.

The National Archives website contains advice about supporting users. The Keep the Knowledge – Make a Record eLearning module is also available to educate agency staff about general records management concepts.

The State Records Authority of New South Wales offers a free online training package about basic digital records management concepts (available at http://elearning.records.nsw.gov.au/digital-recordkeeping-concepts/index.html). This is aimed at New South Wales public sector employees but the overall concepts provide a foundation on understanding digital information.

Provide processes, systems and tools that have capability to support effective management and use of information

Digital continuity requires ongoing management of information with processes, systems and tools in place to support this.

The best way to align processes, systems, tools and information to achieve optimum business outcomes is by using an enterprise architecture approach.
To use digital information effectively, users must be able to access and use information when they need it, and in the way they need it. To achieve this, business processes, systems, and tools must support the users of the information.

**Processes**
Work processes should allow digital information to be created, captured, used, and managed as part of normal work activity or by appropriate business systems with minimal impact on staff. The less complicated or onerous the processes are, the more likely it is that they will be followed.

Agencies should give staff clear instructions on how to create, capture, describe, and use digital information.

**Systems**
Business systems create, capture, and manage digital information. For systems to effectively manage information for as long as it is needed, specific functionality is required. Systems can automate or simplify many of the requirements of effective information management. ISO 16175 Principles and functional requirements for records in electronic office environments provides internationally agreed standards and is endorsed by the National Archives for use in the Australian Government.

A consistent information or data architecture across business systems can be part of your enterprise architecture.

Systems should effectively support access to and use of information. Effective search and retrieval tools should be provided and products should be integrated so that information can be readily reused, transferred, or exchanged.

**Tools**
Information management tools include standards; policies and procedures; indexing, classification, and categorisation mechanisms; authorisation and control mechanisms; and checklists.

These tools may be specific to particular aspects of digital information management, for example, they may ensure that information is:

- accessible for use and reuse
- discoverable
- authentic and reliable
- secure and private, or
- managed in accordance with intellectual property rights.

Some tools may help with:

- controlling access to sensitive information
- building and maintaining user ‘pick lists’ and other ways to categorise information when saving or searching
- applying AGLS metadata to public information.

A range of Australian Government agencies have responsibility for, and provide advice on, aspects of information management.

**Monitor and review ongoing management of information against agency performance criteria**

The National Archives’ online assessment application Check-up 2.0 can be used to monitor and review digital information management capability and some aspects of digital continuity.

Your agency should supplement Check-up 2.0 assessments with its own specific performance criteria.

Agency-specific criteria could include:

- assessing the impact of change on information management
- surveys or other measures of user behaviour, attitudes, and understanding
- sampling information quality.
To ensure that digital information remains accessible, usable and secure over its lifetime, it needs to be actively managed from creation to deletion.

**Define, assign and manage appropriate metadata**

For digital information to be considered authentic and reliable, it must be available and usable in context. Digital content should not be kept without contextual information on when it was created, who created it or why it was created. Metadata provides the context for digital information that allows it to be accessed, used and reused.

A significant proportion of metadata can be generated automatically by systems or through specialised work processes. However, users or creators of information may need to assign some metadata themselves.

Metadata must remain associated and managed with the information it describes for the life of the information. Metadata may be changed or added to as the status of the information changes.

**Provide digital information in a format that is accessible and usable**

To assist with continued access to digital information it is important to consider the formats that are used to manage digital information. For example, formats that are likely to become obsolete, are not widely supported or require proprietary software for access pose risks to the usability of information. Immediate business requirements and long-term uses of the information should determine the appropriate technical solution.

You should explore all technical solutions to determine what best suits your business needs. For example, it is important to consider the number of different file formats that you are using for digital information and determine if these are sustainable.

**Focus on the information**
Ensure information can be exchanged among systems and agencies, and with the community

It is important to understand the systems used to create, maintain and read digital information, as this will help your agency to decide what systems it needs to access current, past and future digital information.

When digital information needs to be exchanged with other agencies or shared with the community, or transferred or migrated to other systems within your agency, it will be important that the business context, processes, systems and standards used to create, maintain and interpret the digital information are understood.

Systems
The Australian Government Interoperability Framework documents the methods for digital information interchange among agencies and systems.

Machinery-of-government and other changes
Digital information is vulnerable during times of change, and it is important to consider the impact of any changes – for example staff turnover (recruitment and loss); amalgamation and separation of agencies; increase or decrease in responsibilities; or the introduction or update of IT systems – on digital information.

The Australian Public Service Commission, the Department of Finance and Deregulation, and the Department of Education, Employment and Workplace Relations, in consultation with the Department of the Prime Minister and Cabinet and the National Archives, have produced a good practice guide entitled Implementing Machinery of Government Changes. It is available on the Australian Public Service Commission website apsc.gov.au.

The National Archives provides advice on the records management requirements as a result of machinery of government changes. The advice is available on the National Archives website naa.gov.au.

The Defence Signals Directorate also provides guidance on change management and security of systems in its Information Security Manual. The advice is available on their website dsd.gov.au.

Establish ongoing checks to ensure digital information remains usable
A regime of ongoing checks of information is necessary, particularly following change, to ensure that any issues affecting the usefulness of information are identified in a timely manner and corrective action is taken.

Regular, automatic integrity checks should be performed to ensure information has not been inadvertently changed. This should be included in tests of your business continuity plan. When information is converted to new formats, it is recommended that a manual comparison of a sample of the information be carried out.

The General Records Authority 31: Source (including original) records after they have been copied, converted or migrated (GRA 31) provides more information on quality assurance measures.

If information is digital, continue to manage it as digital
E-government requires more responsive, comprehensive and integrated government operations and service delivery. An underlying assumption is that information that is received or provided digitally in the course of e-government operations will be processed and managed digitally throughout its useful life. Agencies need to ensure that processes, systems and tools can manage digital information effectively for as long as the information is needed.

This might involve:

- establishing a policy that information in a digital format should continue to be managed in a digital format
- assigning responsibilities, establishing controls and providing software functionality to ensure that digital information is managed for as long as it is required, not just during the active phase of use.
Plan and implement an ongoing program to dispose of information in accordance with the Archives Act 1983 and other legislation

Effective digital continuity includes disposing of digital information when it is no longer needed. The larger the volume of digital information that is kept, the more difficult it will be to access relevant information when it is needed. There are avoidable risks associated with keeping information longer than required. This may include inappropriate disclosure, and legal discovery or FOI requests.

Permission to keep, destroy or transfer Commonwealth records to the National Archives is provided through records authorities issued by the Archives under the Archives Act 1983. For practical purposes, all information created, sent and received in the course of carrying out the business of your agency should be considered a Commonwealth record.

Records authorities are legal documents that indicate how long records need to be kept. Your agency should have an ongoing program to dispose of information using appropriate records authorities.

Under the normal administrative practice provision of the Archives Act, records that are duplicates, unimportant or of a short-term and facilitative nature can be destroyed.

Agency-specific or general legislation may direct that a particular action be taken for some information or records.

Destroying digital information is often not easy. ‘Deletion’ does not equal ‘destruction’: with some effort, digital information can be recovered after deletion. This needs to be accounted for in digital information management policy and practices and a risk assessment should be carried out.

There is a detailed process for destroying these records identified by the risk assessment as needing to be securely and completely destroyed. Specific advice on sanitisation and destruction is available from the Defence Signals Directorate Information Security Manual.

Footnotes

1. This definition is derived from the UK National Archives Digital Continuity Project available from http://www.nationalarchives.gov.uk/information-management/our-services/dc-what-is.htm
Contact

More information on digital continuity is available from naa.gov.au or through the Agency Service Centre via recordkeeping@naa.gov.au or (02) 6212 3610.

Join GAIN Australia (Government Agencies Information Network) for online updates and discussion. Contact gainaustralia@naa.gov.au to request access.

Follow us naa_digital