

Queensland State Archives

Managing Records of Online Resources and Services Guideline

© Queensland State Archives April 2006



Queensland State Archives

Queensland Government

www.archives.qld.gov.au

Connecting people . . .

Managing Records of Online Resources and Services Guideline

Contents

1: Introduction	1
1.1 Authority	1
1.2 Related Legislation, Standards and Policy	1
1.3 How to use and apply this policy and guideline	2
1.4 Guideline Overview.....	4
2: Risk Assessment	5
2.1 Risk Assessment Strategies	5
3: Online Resources and Services Recordkeeping Framework.....	7
3.1 Level 1 - Recordkeeping Fundamentals	7
3.2 Level 2 – Provision of Resources	12
3.3 Level 3 – Basic Provision of Services	15
3.4 Level 4: Transactional Resources and Services	18
4: Approaches for Managing Records of Online Resources and Services	22
4.1 Online Archive	22
4.2 Object-driven Approaches	23
4.3 Event-driven Approaches	24
4.4 Use of content management systems.....	25
5: Feedback and Contact Details.....	26
Appendix A: Glossary	27
Appendix B: References	28
Appendix C: Risk Management Considerations.....	30
Appendix D: Online Recordkeeping Action Checklist.....	34
Appendix E: Recordkeeping System Approaches.....	36

1: Introduction

The online environment is an important mechanism for Queensland Government communication. The online environment is being used to deliver a variety of resources and services, and is becoming a key gateway for client interaction with public authorities. Creating and managing records of online activity is essential to preserve evidence of government activity for present and future generations.

This guideline provides advice for public authorities to ensure that appropriate public records of online resources and services are made, managed and kept. It accompanies the document, *Managing Records of Online Resources and Services: Policy Statement*.

1.1 Authority

The State Archivist has issued this guideline in accordance with s.25 of the *Public Records Act 2002* (the Act). Under s.25 (1) (f) of the Act the State Archivist has the power to make policy, standards and guidelines about the making, keeping, preserving, managing and disposing of public records.

1.2 Related Legislation, Standards and Policy

Principles for creating and maintaining records of online resources and services are given in the accompanying publication, *Managing Records of Online Resources and Services: Policy Statement*.

A number of legislative requirements apply to public authorities and include implications for recordkeeping. The policy statement contains a brief synopsis of each Act.

- [Public Records Act 2002](#);
- [Electronic Transactions Act 2001](#);
- [Evidence Act 1977](#);
- [Information Privacy Act 2009](#);
- [Judicial Review Act 1991](#); and
- [Right to Information Act 2009](#).

Many of the Queensland Government's Information Standards also influence recordkeeping activities in public authorities. *Information Standard 40: Recordkeeping* and *Information Standard 31: Retention and Disposal of Public Records* apply to all public authorities covered by the *Public Records Act 2002* and should be consulted when making recordkeeping plans for online resources and services.

In addition, the following international and Australian standards have relevance to managing records of online resources and services and should be consulted when planning recordkeeping strategies:

- Australian Standard AS ISO 15489:2002 *Records Management* and;
- Australian Standard AS/NZS 4360:2004 *Risk Management*.

Other resources that provide advice on the management of online resources and services are listed in **Appendix B: References**.

1.3 How to use and apply this policy and guideline

This guideline provides practical advice on how to comply with the policy statement. It does not advocate a one-strategy-fits-all approach, but outlines a range of strategies that might be appropriate for public authorities, and highlights common considerations¹.

THE IMPORTANCE OF PRESERVING ONLINE RECORDS

Online resources and activities constitute vital components of the documentary record of Queensland. If future generations of Australians are to fully understand life in Queensland and the role of government in the early 21st century, they will need to have access to preserved copies of significant government records, including records of online resources and services.

Adapted from National Archives of Australia (2001) Guidelines for Keeping Records of Web-Based Activity in the Commonwealth Government

1.3.1 Where to start?

The checklist provided in Appendix D outlines a process that public authorities could use to improve the management of records of online resources and services. QSA recommends following the checklist activities, as summarised below.

- **Conduct a risk assessment** to determine the impact of not having access to records of online resources and services.
 - Identify any situations where records haven't been available and the impact that had on the operations of your public authority.
 - A risk assessment will also help determine if online resources and services have different levels of associated recordkeeping risks or retention and disposal requirements.
- **Audit existing content**
 - Comprehensively determine what content and services are available online. This should include auditing what is available on servers or within content management systems.
 - Learn what records are currently created, and compare this to the results of the risk assessment which also detail the records that should be created.

¹ National Archives of Australia (2002) *Archiving Web Resources: Guidelines for Keeping Records of Web-based Activity in the Commonwealth Government*, page 7.

(Where to start? Cont'd)

- **Address issues of non-capture**
 - Use the framework and advice provided in section 3 of the guideline. Bear in mind that not all levels of advice will need to be implemented by all public authorities.
 - Learn from current recordkeeping practices and make sure consistent activities occur. For example, if over-the-counter customer queries are not tracked or recorded, online queries may not have to be either.
 - Make sure that current systems are capable of implementing the processes for capturing records of online resources and services. New systems, interfaces, or work processes may need to be introduced to promote records capture.
- **Establish metadata requirements**
 - Metadata requirements should be consistent with broader recordkeeping and web publishing practice. Often a single metadata element can provide recordkeeping and resource discovery information.
- **Examine publishing process**
 - Aim to include recordkeeping as a seamless activity, rather than an additional process. Make sure that all staff clearly understand and can carry out any recordkeeping activities so that unreasonable administrative demands are not made.

1.4 Guideline Overview

Section 2 Risk Assessment stresses the need for public authorities to conduct a risk assessment of their online activities to determine the nature and extent of appropriate recordkeeping strategies.

A framework for creating and maintaining records of online resources and services is described in **section 3**. This section includes a number of illustrative examples as well as checklists that can be used by authorities to ensure that they are capturing and keeping appropriate records.

Section 4 outlines the different approaches that public authorities can take when creating records of online activity. It identifies contemporary approaches to capturing records that agencies can tailor to suit their individual needs.

Section 5 supplies Queensland State Archives' contact details for any comments regarding this guideline.

Appendix A contains the glossary of terms used in this document. It supplements the Queensland State Archives' [Glossary of Archival and Recordkeeping Terms](http://www.archives.qld.gov.au) (available from <http://www.archives.qld.gov.au>).

Appendix B lists the references and further readings relating to the online environment.

Appendix C provides a summary of risk management considerations that can be used by public authorities to help determine the most appropriate recordkeeping strategies for their online activities.

Appendix D suggests a checklist to help records managers become involved in the management of online resources and services. It includes the checklists outlined in *section 3, online resources and services recordkeeping framework*.

Appendix E suggests different approaches for including records of online resources and services within recordkeeping systems.

2: Risk Assessment

It is recommended public authorities conduct a risk assessment to help determine the recordkeeping approach that will best meet their needs. Using a risk management framework will help public authorities to identify, assess and report on risks relating to their online resources and services, and to plan appropriate risk mitigation strategies, which may include improving recordkeeping activities.

Example scenario 1: A government department or agency uses its website as an official channel to warn of serious public health or personal safety risks.

Risk: If the department is unable to demonstrate what the relevant page of their website said at a particular time, it might be vulnerable to civil claims should citizens fall ill or find themselves in jeopardy. Individuals might be able to successfully argue that the warning was not made available to them in a timely manner if a public authority cannot provide evidence to prove otherwise.

Example scenario 2: A regulatory body has a provision in its founding legislation that indemnifies the directors of client organisations from personal liability should a breach of the civil law occur while following its advice.

Risk: If the regulatory body has put guidance on its website on the subject but is unable to demonstrate exactly what it said at the relevant time, it might be unable to argue that directors had not acted in good faith on its advice and consequently be unable to use its regulatory and enforcement powers to call them to account.

Adapted from The National Archives (2001) Management of electronic records on websites and intranets: an ERM toolkit.

Many public authorities will have developed their own risk management framework and approach that can be used to analyse their online activities. **Appendix C** provides a summary of risk management considerations that could be used if there is no formal agency approach. Further guidance on risk assessment can also be found in the *Information Risk Management Best Practice Guide* (available online at <http://www.qgcio.qld.gov.au/SiteCollectionDocuments/Architecture%20and%20Standards/Information%20Standards/Current/riskmanagementbpg.pdf>) and the Australian Standard AS/NZS 4360-2004 *Risk Management*.

2.1 Risk Assessment Strategies

In the online environment a key aspect of a risk assessment is determining the appropriate unit of analysis. Public authorities should decide if they are going to assess their online resources and services as a single entity, or if separate assessments will be needed for different online activities. Public authorities may choose to:

- evaluate all their online resources and services as a whole;
- evaluate clusters based on function or other relevant characteristics;
- evaluate groups of resources or services referenced by a main portal;
or
- apply any combination of the above.

Public authorities should also consider conducting a content audit of their online resources to determine exactly what information is available online. This will help public authorities to:

- determine what resources and services are available online;
- discern what records are currently being created;
- identify areas that may be failing to capture public records; and
- create recordkeeping plans to ensure that public records are adequately captured.

3: Online Resources and Services Recordkeeping Framework

Queensland State Archives has developed the following framework to provide guidance to public authorities in managing records of online resources and services. It has been developed in consultation with a reference group with representatives from a range of authorities such as State and Local Governments, Government-Owned Corporations and the tertiary sector.

The framework has four levels. Level 1 - Recordkeeping Fundamentals outlines activities that any authority with an online presence should undertake. Levels 2 to 4 provide guidance for appropriate recordkeeping activities based on the interaction that occurs between an authority and their clients online.

The framework includes a number of examples to illustrate the importance of making and keeping public records of online resources and services. Each level also includes a checklist of actions that should be carried out.

This framework has been provided as a guide only, and public authorities should adapt the advice given in this guideline to suit their needs.

3.1 Level 1 - Recordkeeping Fundamentals

Level 1 – Recordkeeping fundamentals contains activities that all public authorities should carry out in relation to creating and keeping records of online resources and services. These activities underpin the three other levels of the framework.

3.1.1 Include the online environment in information management plans

To be managed effectively, records of online resources and services should be included in a public authority's information management plan. *Information Standard 40: Recordkeeping* and *Information Standard 31: Retention and Disposal of Public Records* provide guidance to public authorities to ensure that they make and keep appropriate public records under the *Public Records Act 2002*.

As outlined in the policy, records a public authority may need to create and maintain about their online resources and services include

- instructions on what records will be created and how they will be created for interactive sections of websites;
- information relating to the addition, modification and removal of resources and services (including applicable policies and procedures);
- evidence of any transactions or communications carried out online;
- details of any outsourcing arrangements;
- information about visual elements used when delivering online resources and services, such as arrangements for drafting and developing presentation elements or the commissioning of logo designs;
- intellectual property agreements for content used in the online environment;
- information about any accessibility arrangements and testing;
- details of system functionality issues such as encryption methods employed or remote access arrangements;

- records documenting the use of copyrighted material in the online environment (including applicable policies and procedures); and
- information relating to the technology used to enable an authority's online presence, such as the selection or customisation of web content management systems used by a public authority.

Public authorities should regularly revisit and revise their information management plans to ensure that their recordkeeping practices continue to meet business and legislative requirements and community expectations.

Some resources may be created for use only in the online environment. They have no equivalent document that may already be captured into a recordkeeping system. Public authorities should ensure that records of exclusively online content are created and maintained with appropriate metadata within a recordkeeping system².

Ideally online records should be kept in electronic format (for example, as records in an electronic document and records management system or eDRMS). If no electronic recordkeeping system is available, public authorities could store records of online content in paper files.

Public records should be given a disposal action that determines their status (temporary or permanent), and management requirements over time, also known as sentencing. The sentencing of records is controlled by an approved retention and disposal schedule, as discussed in section 3.1.2 of this Guideline.

If records of online activity are captured in electronic formats, public authorities will need to consider strategies for their ongoing maintenance, preservation and disposal or future access.

Unlike records in paper format, electronic records require active management to ensure that they remain accessible. The three main issues to consider are

- longevity of file formats used;
- storage media lifespan and obsolescence; and
- maintaining the integrity of data over time.

Public authorities should develop records management strategies that consider these issues, to ensure that records remain accessible for their required retention periods.

3.1.2 Consider online activities in retention and disposal schedules

The *Public Records Act 2002* prohibits the disposal of public records without the permission of the State Archivist. Permission to destroy public records is given through approved retention and disposal schedules.

All Queensland public authorities are required to develop comprehensive function-based retention and disposal schedules to cover records unique to the authority. Generally, authority-specific schedules will cover all the core and non-administrative general functions of the public authority. Disposal coverage for general functions such as financial management and human

² See the Public Records Alert "*Understanding and applying recordkeeping metadata*", available from QSA's website: <http://www.archives.qld.gov.au/publications/publicrecordsbriefs/metadaintro.pdf>.

resources is authorised through the [General Retention and Disposal Schedule for Administrative Records](#) issued by Queensland State Archives.

In addition to the *General Retention and Disposal Schedule for Administrative Records*, some sector-specific schedules have been approved to cover all the functions of public authorities in a certain sector. For example, TAFEs, universities and local governments are covered by sector-specific schedules and do not need to develop individual retention and disposal schedules.

When public authorities develop a retention and disposal schedule or undertake new activities in the online environment, they should ensure that these activities are

- covered in general, public authority or sector-specific schedules; or
- plan for those activities to be included in the next version of the appropriate schedule.

For more advice on developing retention and disposal schedules, please consult QSA's [Guideline for the Development of Retention and Disposal Schedules](#) which is available from QSA's website: <http://www.archives.qld.gov.au>.

3.1.3 Capture records into a recordkeeping system or appropriate business system

Effective recordkeeping systems ensure that full and accurate records are maintained to meet business needs, accountability requirements and community expectations. Effective recordkeeping systems are a collection of people, processes, tools and technologies.

Public authorities may need to revise their current recordkeeping systems to incorporate records generated from interactions in the online environment.

This may include

- designing changes to current systems, processes and practices; and
- adapting or integrating technology solutions.

Appendix E summarises the approaches that public authorities could take to ensure that their recordkeeping systems adequately capture records of online activity.

For more information about the design of recordkeeping systems, see *Information Standard 40: Recordkeeping* and QSA's *Guideline for Recordkeeping*, as well as AS/ISO 15489 *Recordkeeping*³.

Electronic records should be managed in their original form. However, if an authority's recordkeeping system does not support the capture of electronic records, paper-based systems may be used as an interim measure while public authorities work towards implementing an eDRMS.

The DIRKS (Designing and Implementing Recordkeeping Systems) methodology provides a comprehensive overview for the design or review of recordkeeping systems. The National Archives of Australia and State

³ See Appendix B for full details of these documents.

Records New South Wales have developed manuals explaining the methodology in full⁴.

3.1.4 Capture recordkeeping metadata

Recordkeeping metadata describes the context, management, use, preservation and disposal actions of records. It is important to ensure that records of online resources and services are captured with appropriate metadata. Attaching recordkeeping metadata to records of online resources and services allows them to be located, controlled and managed appropriately.

Information Standard 34: Metadata (IS34) requires Queensland public authorities to apply metadata schemes that are interoperable with the Australian Standard 5044 “AGLS Metadata Element Set” and consistent with the requirements of the [Queensland Government AGLS Element Implementation Standard](#). *Information Standard 40: Recordkeeping* endorses the use of the National Archives of Australia (NAA) [Recordkeeping Metadata Standard for Commonwealth Agencies](#) as a recordkeeping scheme that is interoperable with IS34.

In addition to the compulsory metadata elements mandated by IS34, table 1 outlines highly-recommended optional recordkeeping metadata elements (taken from NAA’s standard) that can help manage records of online resources and services.

⁴ State Records NSW (2003) *Introducing the DIRKS Methodology*. Available online: <http://www.records.nsw.gov.au/recordkeeping/dirks/introducing-the-dirks-methodology> and National Archives of Australia (2001) *The DIRKS Manual: A Strategic Approach to Managing Business Information*. Available online: <http://www.naa.gov.au/records-management/systems/dirks/index.aspx>.

Element	Description	Example of use	AGLS Equivalent
Description	A free text description of the content and purpose of a record	Description of an image Abstracts of a publication or section of a website	Description
Relation	A link between a record and another information resource	Linking records of an online and print publication Links between version of difference policies	Relation
Format	The logical and physical form of the record	Media format (audio, image, text etc) and data format (file type), what the record is stored on and the size of the file	Format
Preservation History	All actions performed on the record after its capture into the recordkeeping system	Date and time, what was done, and what follow up actions are required	None
Location	Current location of the record	Current and home location of the record, and any storage details	None

Table 1: Mapping of optional elements from National Archives of Australia's Recordkeeping Metadata Standard for Commonwealth Agencies to AGLS elements.

3.1.5 Checklist – Level 1 Recordkeeping Activities

Records of online activities have been identified in authority or sector-specific retention and disposal schedules	<input type="checkbox"/>
Recordkeeping systems have been designed and implemented to incorporate records arising from the online environment	<input type="checkbox"/>
A public authority's information and records management plan considers records of online resources and services, and also includes strategies for managing and preserving paper and electronic records over time.	<input type="checkbox"/>
Recordkeeping metadata is captured and kept with records of online activity.	<input type="checkbox"/>

3.2 Level 2 – Provision of Resources

Most public authorities use the online environment to publish resources such as an overview of their business, or to provide copies of policies, procedures and contact information. This use of the online environment is characterised as level 2 – Provision of Resources.

Online resources at level 2 are normally static HTML webpages. Under *Information Standard 26: Internet (IS26)*, all Queensland Government agencies should have a level 1 website accessible from the qld.gov.au domain that provides information to the public. Some public authorities will not require a more advanced online presence.

For example, when a new department or public authority is established, its first presence in the online environment may be a simple website compliant with the CUE (Consistency in User Experience) standard, with content required by IS26, such as

- the services available from the authority;
- identification of the clients of the authority;
- the structure of the authority;
- links to publications produced by the authority; and
- a link to the Queensland Government Internet Gateway at <http://www.qld.gov.au>, privacy and security statements, copyright and disclaimer notices.

Example: A public inquiry into a human tragedy uses its website to publicise its proceedings

The site is used not just to raise awareness, but also to air public safety issues, provide the general public with transcripts of the public hearings and invite comment. It is also intended to prompt witnesses of the event to come forward.

This is an example of a *Level 1- Provision of Resources* website. Records should be created to document what was available online, when content was added to the site and any comments or information provided by the public via the website.

Adapted from The National Archives (UK) (2001) Management of electronic records on websites and intranets: an ERM toolkit.

3.2.1 Capture and maintain administrative records

Administrative records are created to document and support the operational activities of a public authority, such as those tasks involved in the routine administration of an online presence. Administrative records are distinct from functional records, which are created in the course of the public authority's core business⁵. Many administrative activities will be common to most Queensland public authorities.

One method of creating and maintaining administrative records can be to maintain a log of what, where and when resources were made available online. Such a log could be a partially automated, or it may be a spreadsheet

⁵ See QSA's *Glossary of Archival and Recordkeeping Terms* for more detail on administrative and functional records.

form completed when changes to online resources are made. Fields that the log could capture include

- date and time of the change(s);
- the person making the change(s);
- a brief description of the change(s);
- the person who requested the change(s);
- the target URL for the change(s);
- the source or documents relating to the change(s);
- the person responsible for authorising the change(s); and
- if relevant, the file number relating to the activity.

In addition to the log of online activity, public authorities could also consider capturing records of correspondence and communication where changes to online resources are requested, authorised or confirmed. For example, a public authority could capture all the relevant emails and attachments that are sent to the officer responsible for making the changes, and all the confirmation emails that officer returns once the work has been carried out.

3.2.2 Consider regular snapshots of websites

Snapshots capture a copy of the visual presentation of a website at a particular point in time. In some instances public authorities may find it useful to create a snapshot of their website to augment other records of online activity. For example, snapshots can be used to supplement and provide context to an activity log.

Snapshots are particularly useful for capturing the look, feel and full functionality of a website. However because snapshots only capture records of online activity at particular points in time and do not capture full records of client interaction with a website, they should not be used as a public authority's only recordkeeping strategy.

If public authorities are planning to capture snapshots, there are a number of issues to consider. These include:

- the regularity of snapshots. Bi-annual snapshots are common, but they may need to be more or less frequent depending on the agency's risk assessment, frequency of change and the planned role for snapshots.
- the extent of resource and service capture. To maintain a fully functioning website, public authorities should capture all related scripts, programs, plug-ins and typical browser software.
- how hyperlinked resources will be managed. Because hyperlinks are volatile it may be necessary to add information about hyperlink destinations to ensure that the integrity of the resource is maintained if the hyperlinked document changes location or is removed.
- the development of an ongoing plan for the maintenance of snapshots. Public authorities should ensure that appropriate strategies are in place to migrate file formats, regularly refresh or migrate media formats, and manage recordkeeping metadata after the snapshot has been captured into a recordkeeping system.
- how retention and disposal of the snapshot will be managed. Most snapshots will contain records with different minimum retention periods.

Disposal of snapshots will be based on the record with the longest retention period, meaning some snapshots may have to be kept for many years past their minimum retention period.

3.2.2.1 Legal Deposit Requirements

Online publications (without analogue equivalents that have already been deposited) are subject to legal deposit provisions under the Commonwealth *Copyright Act 1968* s201 and Part 8 of the *Libraries Act 1988 (Qld)*.

When an online resource or service is identified to be a publication, Queensland publishers should fulfil their legal deposit obligations by notifying the State Library of Queensland (SLQ) of their website, and authorising its capture using the “Suggestions for Preservation” online form, available from the SLQ website

(http://www.slq.qld.gov.au/find/sites/pandora/suggest_a_site/). Websites that meet the selection guidelines will be selected for inclusion in the PANDORA web archive (<http://www.slq.qld.gov.au/find/sites/pandora/>).

The SLQ’s collection policy is focused on research value, rather than evidentiary value. That is, the SLQ’s collection of websites may not be frequent enough to provide a trail of evidence relating to, or all versions of a resource.

3.2.3 Checklist: Level 2 Recordkeeping Activities

Level 1 activities have been carried out (see checklist 3.1.5)	<input type="checkbox"/>
Procedures have been implemented to capture records of what, where and when resources were made available online (logs or other methods)	<input type="checkbox"/>
Where necessary, snapshots of websites are routinely created and captured into a recordkeeping system.	<input type="checkbox"/>

3.3 Level 3 – Basic Provision of Services

In addition to providing online resources as characterised by Level 2, some public authorities will also use the online environment to deliver basic services to their clients. This level is characterised by non-authenticated online interaction between clients and the agency's online resources and services.

Public authorities at this level may:

- dynamically generate content to be delivered to users;
- enable searching of online resources; or
- provide public access to agency databases.

For example, dynamic websites are often used to present regularly changing information (such as news headlines) or to display resources in reaction to user inputs.

Recordkeeping for Level 3 activities may involve creating and maintaining records of dynamic generation processes, search processes and of all the resources and services that are available through the dynamic generation and search processes and tools.

3.3.1 Keep records of dynamic generation processes

Often public authorities will choose to dynamically select content to be displayed online. The resources and services that are displayed may be selected using variables such as:

- the date or time;
- cookies⁶;
- web session states; and
- current database contents.

To ensure that a complete history of their online activity is created, public authorities should consider capturing and maintaining records detailing how dynamically generated resources and services are selected. Recordkeeping activities may include:

- creating, updating and maintaining a log of the available resources and services, and the triggers for their delivery; or
- capturing and maintaining a record of the HTML file(s) that are delivered to a client, and the elements that triggered its creation.

In some circumstances, it may also be advantageous to capture records of the IP addresses that resources or services were provided.

3.3.2 Keep records of search processes and tools

An online search facility provides clients with fast and direct access to resources and services. There are many different searching tools that can be implemented in the online environment. If a public authority provides search facilities to help clients access resources and services, they need to create and maintain a record of:

⁶ Refer to Glossary of Terms at Appendix A

- the tool(s) selected;
- the dates of use; and
- details about how the search facility selects and ranks results.

For most public authorities, capturing how the search function works will be a sufficient record for their business.

In limited situations public authorities may also want to capture the search queries that are used to access online resources and services, or the queries and the resources that were returned to the client. Appropriate recordkeeping activities may include:

- creating a record of search queries and the results, and ensuring links between the two are maintained; or
- capturing a record of each unique HTML file that is delivered in response to a query.

3.3.3 Decide if records of all content or only accessed content are necessary

It is important that public authorities create and maintain full records of the resources and services that are made available online. In the case of dynamically generated or accessed content, determining the best approach requires that public authorities consider if it is necessary to capture all the online resources and services that are available online, or if only records of the accessed resources and services are important. An authority's risk assessment and legislative, accountability and business requirements should be used to inform a decision on what records need to be created, kept and maintained.

If creating and maintaining a record of all available resources and services delivered online is required, public authorities should ensure that they

- create records of all online content that is not available in any other format (see Level 1 *Include the online environment in information management plans*);
- if resources or services are already captured in a recordkeeping system, add a note identifying the date and process that made the document available online, and when it was removed; and
- capture a record of each unique HTML file (including resource or service information and relevant parameters) that is delivered online.

If only records of accessed resources and services are required, public authorities could consider

- capturing a record of each unique HTML file (including resource or service information and relevant parameters) that is delivered to a client; or
- maintaining logs of when resources and services were accessed.

3.3.4 Checklist: Level 3 Recordkeeping Activities

Level 1 activities have been carried out (see checklist 3.1.5)	<input type="checkbox"/>
Any relevant Level 2 activities have been carried out (see checklist 3.2.3)	<input type="checkbox"/>
Records of how content is dynamically selected and displayed have been captured	<input type="checkbox"/>
The details of any search facilities provided to assist access to online resources and services have been recorded	<input type="checkbox"/>
If necessary, search queries and results have been captured as records	<input type="checkbox"/>
Records of resources and services available or accessed have been created and captured within a recordkeeping system	<input type="checkbox"/>
If necessary, records of who has accessed online resources and services have been created and captured, with due regard to Queensland's Information Privacy Act 2009	<input type="checkbox"/>

3.4 Level 4 - Transactional Resources and Services

Some public authorities will provide access to online resources and services that are restricted to registered or identified clients. Often such resources and services will have privacy and security requirements. This type of interaction is characterised by Level 4: Transactional Resources and Services.

For example, public authorities at this level may

- provide e-commerce or other financial services online;
- allow clients to update their personal details or lodge forms containing personal details; and
- exchange information about clients with other agencies (such as changes of address).

Interaction at this level requires the authorisation and authentication of client identities, and is accompanied with a number of security and privacy considerations. Public authorities should ensure that records about the privacy, security, authorisation and authentication processes are created, along with any transactional service records, and records of online information exchanges.

Example: A local council allows rates and other levies to be paid online.

A local council allows ratepayers to carry out a range of activities online, such as paying rates and applying for and purchasing permits. These services are enabled by a proprietary system that has been purpose built for the council which integrates directly with their recordkeeping system.

3.4.1 Create and maintain records of privacy, security, authorisation and authentication processes

Public authorities should create and maintain records of the privacy, security, authorisation and authentication processes relating to online transactional resources and services.

3.4.1.1 Privacy and Security

Agency clients are entitled to expect that personal details provided online:

- will remain private;
- will not be accessible to others without their permission;
- will not be used for another purpose other than originally intended; and
- that they will have the ability to determine the extent of disclosure of their personal details;

Many records of online transactions will contain personal details about clients. Public authorities must comply with *Information Privacy Act 2009*. Capturing and maintaining records in a recordkeeping system that conforms to the principles of *Information Standard 40: Recordkeeping* will help public authorities to meet legislative and other privacy requirements while ensuring that the records are secure, inviolate and protected.

Public authorities should also create and keep records that:

- give an authority permission to distribute or otherwise make available personal details that have been provided online; and
- document the processes that ensure client privacy is maintained.

Ensuring the privacy of online transactions requires that the related systems and processes are secure. Secure online resources and transactions should be free from as many risks as possible (both for the agency and their clients), and inviolate; that is, complete and undamaged. Public authorities should document their processes that ensure the security of online resources and services and capture appropriate records into a recordkeeping system.

3.4.1.2 Authentication and authorisation

A key characteristic of Level 4 interaction between public authorities and their clients is that it requires authentication and authorisation of a user's identity.

Authentication refers to the verification of a user's identity. Common authentication processes include something the user is (e.g. a DNA sample or finger print), something they have (such as an identity card or car registration plates), something they know (such as a PIN number) or any combination of the three (credit card plus signature). An authenticated user will have authorisations to access certain services or resources.

Authorisation processes determine if a user (or program or device) has the right to access a defined set of resources and services. For example, a public authority that maintains an online employment service may authorise businesses to submit and make changes to employment listings, but only allow job seekers to search the current employment opportunities.

Public authorities should ensure that they maintain records about the authentication and authorisation processes relating to online resources and services. For example, this may require that public authorities:

- create and maintain records of authentication processes and requirements;
- create and maintain records of different authorisation for resources and services;
- create and maintain records of authorisation processes; and
- maintain lists of authorised users, including the dates of their authorisations and any relevant renewals.

3.4.2 Ensure that records of transactions are created and maintained

Online transactions may not result in the production of a physical item that can be captured as a record. To create full and accurate records of a public authority's business, it is vital that records of online transactions are created and maintained for as long as they required.

Many online transactions will be integrated into business systems such as agency finance applications or databases. If public authorities are processing transactions online, it is important that they ensure records of such transactions are created.

Public authorities could create records of transactions by:

- ensuring that transactional records are created and maintained in a system with sufficient recordkeeping functionality; or
- capturing records of transactions into a recordkeeping system and maintaining them for as long as they are required.

Example: Systems Often Neglect Recordkeeping Requirements

Organisations are increasingly doing business online, in accordance with government-wide initiatives. Many of the systems that are being developed include interfaces that allow clients to conduct business with government electronically. Often recordkeeping is a neglected component of these systems. Systems are designed to allow easy access to government services and to meet client needs, but sometimes neglect to include functionality that will support recordkeeping requirements.

For example the ability to dispose of certain records while retaining other records for a longer period of time may be neglected in system designs.

As a result the systems may transact business, but they do not document or keep adequate records of this business.

Adapted from State Records NSW Strategies for documenting government business: Introducing the DIRKS methodology: Recordkeeping systems, available online:
<http://www.records.nsw.gov.au/recordkeeping/dirks/introducing-the-dirks-methodology/introducing-the-dirks-methodology/?searchterm=dirks>

3.4.3 Keep audit logs

An audit log (or trail) maintains information about who has accessed (or attempted to access) a system, and the actions performed within a certain period of time. They may have several functions, such as providing statistics about the number of people accessing, or verifying the security of a system.

Public authorities that conduct transactions online may need to create and maintain audit logs detailing the interactions between users and their resources and services. Recordkeeping and Information and Communication Technology staff should work together to establish audit logs that meet recordkeeping requirements. Audit logs often capture information such as:

- date and time of the transaction;
- user profile, including IP address;
- all actions performed online, including any searches or queries; and
- any objects returned to the user.

Audit logs should be captured as records when they provide appropriate evidence of a public authority's actions. This may be done by

- ensuring that audit logs are maintained in a system with sufficient recordkeeping functionality; or
- capturing audit logs into a recordkeeping system and maintaining them for as long as they are required.

If audit logs are to be used as part of records of online resources and service, authorities need to ensure that they are kept for their appropriate retention period, rather than being regularly purged or overwritten.

3.4.4 Create and maintain records of information exchanges

Some public authorities may exchange information provided online by clients, with their prior consent and knowledge. If public authorities are planning to

interchange information gathered in the online environment, they should comply with *Information Privacy Act 2009* and capture records of:

- how client consent was gathered;
- the date, time and process of information exchange;
- authorisations for the exchange; and
- the transaction itself.

3.4.5 Checklist: Level 4 Recordkeeping Activities

Level 1 activities have been carried out (see checklist 3.1.5)	<input type="checkbox"/>
Any relevant Level 2 activities have been carried out (see checklist 3.2.3)	<input type="checkbox"/>
Any relevant Level 3 activities have been carried out (see checklist 3.3.4)	<input type="checkbox"/>
Records of how the agency will maintain online privacy and security have been made	<input type="checkbox"/>
Authentication and authorisation processes have been recorded	<input type="checkbox"/>
Records of client authorisation permissions have been maintained	<input type="checkbox"/>
Records of online transactions are being created and maintained, either in a recordkeeping system or a business system with appropriate recordkeeping functionality.	<input type="checkbox"/>
Audit logs have been created and maintained when necessary	<input type="checkbox"/>
Records of any information exchanges have been created and maintained	<input type="checkbox"/>

4: Approaches for Managing Records of Online Resources and Services

This section outlines some of the options available for creating and keeping records of online activity. It should be used in conjunction with the recordkeeping framework described in section 3 to ensure the creation of full and accurate records. It is important to note that the strategies are not mutually exclusive; often a combination of approaches will be the most appropriate strategy for ensuring full and accurate records are created and retained.

The three main strategies recommended for managing records of online resources and services are:

- maintaining an online archive;
- using object-driven approaches, such as snapshots and change logs; and
- using event driven approaches, such as activity logs.

The approaches discussed in this section have been drawn from contemporary recordkeeping policies and are technology neutral. They describe only an outcome, not how or what tools should be employed for the task.

Public authorities should choose and, if appropriate, combine approaches to fit their circumstances and requirements. The selection of an appropriate strategy will depend on:

- the types and complexity of resources and services delivered online;
- the results of a public authority's risk assessment; and
- the recordkeeping requirements of the agency.

Example: Different Strategic Options

Some departments use scripting languages to dynamically maintain up-to-date publication lists on their websites. Script files retrieve either the information content itself or a list of active links to the information, which is generated from an unstructured database. Because the database is updated when publications are either discontinued or added, the results from launching the list may vary as the information is not held independently but is generated by running a database query in real time.

One approach might be to preserve snapshots of such lists each time an update is made. Another would be to ensure that the database had a comprehensive audit log function. Either or both of these might be required in high risk environments. An alternative would be to rely on the metadata and the capture of the individual electronic objects.

Adapted from The National Archives (2001) Management of electronic records on websites and intranets: an ERM toolkit

4.1 Online Archive Approach

From an ICT perspective, an online archive is a dedicated server that replicates all past and present resources and services made available online. The major advantage of an online archive is that it allows the reconstruction and navigation of online activity for any point in time. However, an online

archive is not a recordkeeping system itself, and needs to be linked to a recordkeeping system where sufficient metadata is also stored and maintained, and records are protected. Online archives also do not capture records of electronic transactions.

Online archives are effective in providing access to and preserve maximum functionality of online activity. However, maintaining an online archive may also require large amounts of storage and technical support, with subsequent cost implications. Maintaining an online archive also requires careful planning that considers recordkeeping and system requirements, and to succeed requires collaboration between recordkeeping staff, IT staff and staff that administer online activity.

4.2 Object-driven Approaches

Object-driven approaches to recordkeeping concentrate on managing the objects that are delivered online. Objects may be HTML webpages, or they may be elements of resources such as the header, footer, logos or images. Object-driven approaches are often recommended for keeping records of static resources that are collections of HTML documents, and that do not rely on complex interactivity with users. These approaches are often used to manage online interaction at Level 1 within public authorities. Object-driven recordkeeping strategies include managing objects separately, taking snapshots or combining snapshots and change logs.

4.2.1 Managing objects separately

One approach to keeping records of online resources and services is to manage all the objects separately. A register of the resources displayed online, such as documents, graphics and forms, along with associated metadata is maintained and linked to the URL where they have been available. One advantage of this strategy is that online resources can be managed individually, instead of as a more complicated set of objects displayed online.

The major disadvantage of managing online resources separately is that there is no easy way to reconstruct the set of resources made available at a given point in time. Although individual objects can be viewed, presenting the collection of online resources can be problematic.

4.2.2 Snapshots

Snapshots are copies of online resources and services taken at regular intervals. Intervals may be time-based (for example, creating a snapshot on the first day of every month) or they may be related to events (such as the addition of a new resource online). Appropriate intervals need to be determined based on the needs of each agency. Each snapshot should be captured into and managed within a recordkeeping system for as long as necessary, along with sufficient metadata. Snapshots are particularly appropriate when the entire collection of resources and services need to be captured as a record.

Ensuring that each snapshot is a full and accurate record of resources and services at a particular point in time requires capturing all of the content, layout and functionality of the website. Therefore, snapshots need to collect:

- the text or documents displayed;
- any scripts that run on the page; and
- any programs, browser software and plug-ins that are used.

Some functionality may have to be modified to ensure the snapshot is authentic. For example, webpage counters that measure the numbers of visitors to a page may need to be disabled so that they do not continue to increment when a record is accessed.

Snapshots are useful for static resources that do not change frequently. Snapshots do not allow re-creation of online resources and services throughout their existence, as they are only captured at set times or in response to certain events. Often snapshots are combined with change logs.

4.2.3 Snapshots and change logs

Change logs track the alterations made to resources and services over time, creating a list of online activities. Change logs are often used to provide a record of online activity between snapshots, and hence combining snapshots and change logs is a popular strategy. Change logs should capture changes to online resources and services including the text or documents displayed, scripts, plug-ins and forms. In some cases, combining snapshots and change logs will result in the creation of appropriate records for online activity at Level 3 of the recordkeeping framework.

When change logs are created, they need to be captured into a recordkeeping system and maintained for as long as necessary. Metadata should be captured to enable long-term accessibility and understanding of the change log.

4.3 Event-driven Approaches

Event-driven approaches capture records of interaction that occurs between a user and online resources and services. For example, an event-driven approach may create a new record in response to a user query or an online payment. Event-driven approaches are best suited to collecting records of dynamically generated resources or services, such as those typically at Levels 2 or 3 of the recordkeeping framework. A recommended event-driven recordkeeping strategy for online resources and services is to keep activity logs.

4.3.1 Activity logs

Activity logs capture online transactions in response to particular events. The logs can be used to capture evidence of resource or service use, and for tracking queries or transactions enabled online. Activity logs should capture information such as:

- the date and time of the event;
- information about the user (IP address or domain name, web browser used, user name or identification);

- the resources and services accessed and actions performed (such as queries and searches); and
- the resources returned to the user (including any scripts that are executed).

An activity log for a transactional service should also record additional information about the authentication of identities involved in an event, payment(s) made and data security.

Some websites automatically create visitor logs for each page within a site. However, these logs are generally for administration purposes rather than to meet recordkeeping needs. When activity logs are used to keep records of online activity, procedures and processes need to be established to ensure that the logs meet recordkeeping requirements and are captured into a recordkeeping system. Metadata must be recorded with the activity logs to ensure long-term accessibility and understanding of the records.

4.4 Use of content management systems

Content Management Systems (CMS) are popular software tools that may be used to structure and manage organisational information, including online content. However, CMS are often focused on controlling publications and their associated processes rather than maintaining full and accurate records over time. If a CMS is used to maintain records, care must be taken to ensure that:

- the system has adequate recordkeeping functionality; or
- the CMS is suitably integrated with a recordkeeping system; or
- other recordkeeping strategies are employed.

5: Feedback and Contact Details

Queensland State Archives welcomes feedback on this guideline and its contents. Comments and queries about this matter may be addressed to:

Manager, Policy and Research

Queensland State Archives

Phone: (07) 3131 7788

Fax: (07) 3131 7764

Email: info@archives.qld.gov.au

Address: 435 Compton Road Runcorn Qld 4113

Mailing Address: PO Box 1397 Sunnybank Hills Qld 4109

Website: <http://www.archives.qld.gov.au>

Appendix A: Glossary

This glossary should be used in conjunction with Queensland State Archives' [Glossary of Archival Recordkeeping Terms](#) that explains commonly used recordkeeping terms within the Queensland public sector. QSA's glossary is available online from QSA's website: <http://www.archives.qld.gov.au>.

Term	Definition
Cookie	A packet of information sent by a server to a web browser, and then sent back by the browser each time it accesses that server. Cookies are mostly used for authentication, tracking, and maintaining user-specific information (preferences, shopping bag, etc.).
Domain name	A name that identifies one or more IP addresses. Domain names are used in URLs to identify particular Web pages.
HTML	HyperText Markup Language. The set of markup symbols or codes inserted in a file intended for display on an Internet Browser.
IP Address	An IP address is a unique number used by machines (usually computers) to refer to each other when sending information.
Plug-ins	A hardware or software module that adds a specific feature or service to a larger system, by simply plugging in to an existing system.
Online Resource	Resources accessible via a device connected to the Internet or a private network. Information provided via the online environment – for example, publications available as online documents.
Scripts	A list of executable commands to perform actions such as dynamically generating content, creating menus and processing forms. Client-side scripts are executed by a web browser (the client). Server-side scripts run on a Web server.
Online Service	Services that are accessible via a device connected to the Internet or a private network. Tailored information or transactions available online, such as allowing clients to search databases; dynamically generating content or allowing e-commerce transactions online.
URL	The global address of documents and other resources on the World Wide Web. An abbreviation of Uniform Resource Locator.
Web browser	A software application used to locate and display Web pages, such as Microsoft's Internet Explorer. Most browsers can display graphics as well as text. Most modern browsers can also present multimedia information, including sound and video.
Web page	A document on the World Wide Web, normally consisting of an HTML file and any related files for scripts and graphics, and often hyperlinked to other documents on the Web. It can be viewed by anyone with access to a web browser.
Website	A collection of electronic files, usually under common administrative control, linked together and made accessible to the public via the World Wide Web.

Appendix B: References

Legislation

Commonwealth Copyright Act 1968. Available online:

http://www.austlii.edu.au/au/legis/cth/consol_act/ca1968133/ . Accessed 06 April 2005.

Libraries Act 1988 (Qld.). Available online:

<http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/L/LibrarArchA88.pdf>. Accessed 06 April 2005.

Public Records Act 2002 (Qld.). Available online:

<http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/P/PublicRecA02.pdf>. Accessed 06 April 2005.

Recordkeeping Policies

Archives New Zealand (2004) *A guide to developing recordkeeping strategies for websites*.

Available online: <http://www.archives.govt.nz/continuum/dls/pdfs/G20-RecordkeepingForWebsites.pdf>. Accessed 06 April 2005.

Government of Western Australia (2002) *Guidelines for the Management of Web Information*.

Available online: <http://www.egov.dpc.wa.gov.au/index.cfm?fuseaction=projects.wsmanagement>. Accessed 06 April 2005.

Minnesota Historical Society (2004) *Electronic Records Management Guidelines, File Naming*.

Available online: <http://www.mnhs.org/preserve/records/electronicrecords/erfnaming.html>. Accessed 06 April 2005.

National Archives and Records Administration (2004) *NARA Guidance on Managing Web Records*. Available online:

http://www.archives.gov/records_management/policy_and_guidance/managing_web_records_index.html. Accessed 06 April 2005.

National Archives of Australia (2001) *Archiving Web Resources: A Policy for Keeping Records of Web-based Activity in the Commonwealth Government*. Available online:

http://www.naa.gov.au/Images/archweb_policy_tcm2-902.pdf. Accessed 06 April 2005.

National Archives of Australia (2001) *Archiving Web Resources: Guidelines for Keeping Records of Web-based Activity in the Commonwealth Government*. Available online:

http://www.naa.gov.au/images/archweb_guide_tcm2-903.pdf. Accessed 06 April 2005.

Public Record Office UK (2001) *Management of electronic records on websites and intranets: An ERM toolkit*. Available online: http://www.nationalarchives.gov.uk/documents/website_toolkit.pdf. Accessed 22 June 2005.

Public Record Office UK (1999) *Guidelines for management, appraisal and preservation of electronic records. Volume 2, Chapter 2: Creating and capturing records*. Available online:

<http://collections.europarchive.org/tna/20080108103210/http://www.nationalarchives.gov.uk/documents/procedures.pdf>. Accessed 06 April 2005.

State Records South Australia (2004) *Managing Web Resources as Official Records: Policy and Guidelines*, draft V0.4 January 2005.

Standards and Toolkits

AS ISO 15489.1 (2002) *Records management - General*. Available from Standards Australia, <http://www.standards.com.au>

AS ISO 15489.2 (2002) *Records management - Guidelines*. Available from Standards Australia, <http://www.standards.com.au>

AS/NZS 4360:2004: *Risk Management*. Available from Standards Australia. <http://www.standards.com.au>

Information Standard 18: Information Security. Available online: <http://www.qgcio.qld.gov.au/qgcio/architectureandstandards/informationstandards/current/Pages/Information%20Security.aspx>. Accessed 06 April 2005.

Information Standard 26: Internet. Available online: <http://www.qgcio.qld.gov.au/qgcio/architectureandstandards/informationstandards/current/Pages/Internet.aspx>. Accessed 06 April 2005.

Information Standard 31: Retention and disposal of Public Records. Available online: <http://www.qgcio.qld.gov.au/qgcio/architectureandstandards/informationstandards/current/Pages/Retention%20and%20Disposal%20of%20Public%20Records.aspx>. Accessed 06 June 2005.

Information Standard 34: Metadata. Available online: <http://www.qgcio.qld.gov.au/qgcio/architectureandstandards/informationstandards/current/Pages/Metadata.aspx>. Accessed 06 April 2005.

Information Standard 40: Recordkeeping. Available online: <http://www.qgcio.qld.gov.au/qgcio/architectureandstandards/informationstandards/current/Pages/Recordkeeping.aspx>. Accessed 06 April 2005.

Information Risk Management Best Practice Guidelines. Available online: <http://www.qgcio.qld.gov.au/SiteCollectionDocuments/Architecture%20and%20Standards/Information%20Standards/Current/riskmanagementbpg.pdf>. Accessed 22 July 2005

National Archives of Australia *Recordkeeping Metadata Standard for Commonwealth Agencies*. Available online: http://www.naa.gov.au/images/rkms_pt1_2_tcm2-1036.pdf. Accessed 06 April 2005.

National Archives of Australia, *DIRKS Manual – Glossary*. Available online: http://www.naa.gov.au/Images/dirks_glossary_tcm2-954.pdf. Accessed 06 April 2005.

Public Record Office UK (2001) *Management of electronic records on websites and intranets: An ERM toolkit*. Available online: http://www.nationalarchives.gov.uk/documents/website_toolkit.pdf. Accessed 22 June 2005.

Queensland Government Web Centre, *Consistent User Experience Standard*. Available online: <http://www.qld.gov.au/web/cue/standard/>. Accessed 06 April 2005.

Other Information

Queensland State Archives (2004) *Glossary of Archival and Recordkeeping Terms*. Available online: <http://www.archives.qld.gov.au/downloads/GlossaryOfArchivalRKTerms.pdf>. Accessed 06 April 2005.

Appendix C: Risk Management Considerations

This appendix contains a summary of risk management considerations that public authorities could use in lieu of or as a supplement for a public authority-defined risk management framework. A risk management assessment will help public authorities to identify and select an appropriate recordkeeping strategy for managing records of online resources and services.

Properly analysing business activity risks is an integral part of good management. The Australian Standard AS/NZS 4360:2004 *Risk Management* provides a generic guide for managing risks in the activities or operations of an organisation. Public authorities should consult AS/NZS 4360:2004, internal risk management frameworks and the advice in this guideline when considering the management of online resources and services.

Public authorities can also consult the *Information Risk Management Best Practice Guide* for advice regarding ensuring the integrity, availability and confidentiality of information assets and the information environment. It is available online from the Queensland Government Chief Information Office: <http://www.ggcio.qld.gov.au/SiteCollectionDocuments/Architecture%20and%20Standards/Information%20Standards/Current/riskmanagementbpg.pdf>.

For example, a risk assessment can help to determine the recordkeeping risks arising from capturing only parts of a website, in contrast to treating the entire website as a public record. A risk assessment will also help determine if online resources and services have different levels of associated recordkeeping risks or retention and disposal requirements.

Determining risks

Several archival policies identify a range of factors that can be used to determine the level of recordkeeping risks that relate to online resources and services.

These include:

- the records management threats;
- the consequences of records being unavailable;
- the sensitivity and purpose of online resources and services operations;
- the public visibility of online resources and services;
- the complexity of online resources and services; and
- the frequency and regularity of content change.

Each of the risk factors is outlined in more detail below.

Records management threats

Records management threats may arise from challenges to the authenticity, reliability and integrity of records, or the loss and unauthorised destruction of records. These threats generally come from technical and system risks, such as not ensuring that records are stored in an appropriate recordkeeping system, not storing sufficient recordkeeping metadata or poor migration of records from one format to another.

Other threats that may occur can include undocumented citizen-government interaction that occurs online; an inability to recreate dynamically generated content; and the failure to discover records of online resources and services in response to litigation.

Consequences

The severity of consequences suffered by a public authority or citizens if records of online resources and services are not available is a risk factor that must be considered when planning and evaluating recordkeeping activities.

Consequences may range from constrained decision making and planning capabilities and limited access to information supporting agency actions or decisions, to dissemination of misinformation, litigation and liability, and unfavourable media attention.

Public visibility

The public visibility of a public authority is determined by its business and the extent of its dealings with the public. When a public authority's business has a high profile or level of public scrutiny, or they provide a large range of services to the public, they normally have a higher level of visibility and associated risks. Public authorities with higher public profiles may be at heightened risk of being held accountable for their website content than those with lower profiles.

Public authorities could categorise their current level of visibility as high, medium and low, and use this assessment when determining the level of risk associated with its online activities and choosing a recordkeeping strategy. The risk assessment should be periodically reviewed as new activities are commenced or the agency's environment changes⁷.

Purpose and sensitivity

The purpose and sensitivity of a public authority's online presence should be considered when determining the level of risk a public authority faces. Three common purposes for using the online environment include publishing information, to communicate and collaborate, and to provide access to goods and services.⁸

For example, a website that is primarily used as a source of publications that are also available in paper form would have different recordkeeping risks from a transaction-based e-commerce service that has no analogue equivalent.

The factor of sensitivity is also closely related to the purpose of a public authority's online activity. Sensitivity is linked to the importance that a public

⁷ National Archives of Australia (2001) *Archiving Web Resources: A Guideline for Keeping Records of Web-based Activity in the Commonwealth Government*, page 20

⁸ National Archives of Australia (2001) *Archiving Web Resources: A Guideline for Keeping Records of Web-based Activity in the Commonwealth Government*, page 21

authority places on its online operations and role of such resources and services in the agency's business⁹.

Increased sensitivity leads to higher recordkeeping risks. A website that is used only to publish information will be less sensitive than one that is used to provide online access to goods and services.

Complexity

Higher complexity generally correlates to increased recordkeeping risks. The complexity of a public authority's online presence will depend on its characteristics (discussed in the previous section), underlying technology, sensitivity and purpose, and whether it is document or application centred. Generally, resources that are dynamic and services that are application centred have higher levels of complexity and associated recordkeeping risks.

Content Change

Like complexity, high rates of unplanned change can increase recordkeeping risks of online resources and services. Some terms that can be used to describe the timing of changes to resources and services include:

- frequent – three months or less between changes;
- infrequent – more than three months between changes;
- regular – changes are made on a planned basis; and
- irregular – changes are not planned, but are made on an 'as required' basis.

When these terms are combined, four rates of change emerge, as in the table below; regular and frequent; regular and infrequent; irregular and frequent; and irregular and infrequent.

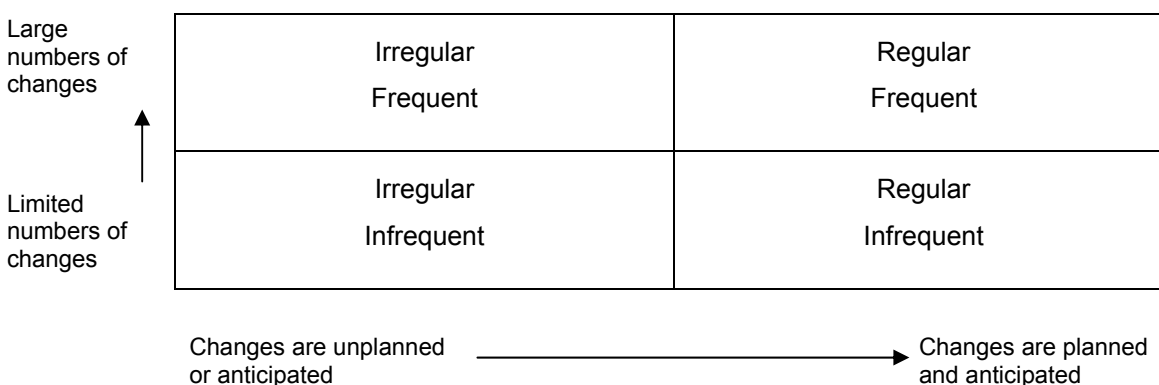


Figure 1: Risks relating to content change. Adapted from National Archives of Australia (2001) *Guidelines for Keeping Records of Web-Based Activity in the Commonwealth Government*.

Online resources and services that are irregularly but frequently changed often pose the greatest recordkeeping risks, because the many changes that occur are difficult to track¹⁰.

⁹ US National Archives & Records Administration (2005) *NARA Guidance on Managing Web Records*.

Mitigating risks

A number of actions can help a public authority mitigate the risk factors that have been identified here. These actions can include:

- documenting the systems used to create and maintain records;
- ensuring that records are created and maintained in a secure environment, with protection from unauthorised alteration or destruction;
- implementing and documenting standard operating procedures for the creation, use and management of online resource and service records;
- using and following the standard operating procedures; and
- providing staff training in the standard operating procedures.

¹⁰ Adapted from National Archives of Australia (2001) *Guidelines for Keeping Records of Web-Based Activity in the Commonwealth Government*, pages 21-23.

Appendix D: Online Recordkeeping Action Checklist

This checklist has been adapted from *Management of electronic records on websites and intranets: an ERM toolkit*, published by The National Archives, UK (2001). It was developed to assist Records Managers ensure that appropriate public records are created in the online environment. The checklist assumes that records managers have only just become involved in the management of online resources and services, but may also be used by those currently handling records of online activity to identify their progress and future actions.

Action	Responsibility	Other issues/references	Review interval	Done
Conduct a risk assessment of online presence				
Issues to consider: <ul style="list-style-type: none"> • online visibility; • business transactions conducted directly online; and • the interests of all stakeholders in the resources and services available online. 	IT staff responsible for online resources and services Records and information managers Content producers Possibly business managers	Appropriate capture of dynamic resources May need internal legal advice on the status of disclaimers (may be ineffective) Extent of audit trails and recordkeeping functionality in business applications	Low risk: At least annually Medium risk: At least bi-annually High risk: At least monthly	<input type="checkbox"/>
Audit existing content				
Audit online resources and services as you would other records and information. Identify an owner for all online content. Ensure that the State Library of Queensland is informed of publications that are only available online.	Records and information managers	Map out online activities to identify areas where records should be created, but aren't being	As per agency records management plan and requirements	<input type="checkbox"/>

Action	Responsibility	Other issues/references	Review interval	
Address issues of non-capture of records				
<p>Design new records capture procedures where they have been shown to be missing, using input from the content audit.</p> <p>Ensure that recordkeeping responsibilities for online resources and services are clearly assigned and documented.</p>	Records and information managers	<p>See section 3, Online resources and services recordkeeping framework</p> <p>Challenges in capturing dynamic and business system records</p>	As use of the online environment increases and results of risk assessments	<input type="checkbox"/>
Establish metadata requirements				
<p>Within the agency,</p> <ul style="list-style-type: none"> • decide what metadata standards will be followed; • introduce standards for new content; and • apply new standards to legacy content, if appropriate. 	Records and information managers	Consult AS ISO 23081 (Information and documentation – Records management processes – Metadata for records), Queensland Government’s Information Standards and QSA’s publications for advice.	Review as per risk assessment timeline and when new publications are made available	<input type="checkbox"/>
Examine publishing process				
<p>Ensure that the publishing process encourages the creation and maintenance of appropriate records.</p> <p>Also consider sustainability issues relating to file formats and technology in use</p>	<p>Records and information managers</p> <p>IT staff responsible for online resources and services</p> <p>Possibly content producers</p>	Particularly important if web content is to be sustained across several platform migrations for business or historical reasons	Review as per risk assessment timeline or technology issues arise	<input type="checkbox"/>
Repeat process as required				

Appendix E: Recordkeeping System Approaches

Public authorities have a number of options when deciding how to make and keep records of online activity. They may choose to apply their current recordkeeping practices to online resources and services without making any changes to their activities.

Alternatively, authorities may decide to tailor their recordkeeping approaches to address the requirements of online resources and services, or may decide to establish new recordkeeping procedures and systems to capture and maintain records of online activity.

Each approach has associated benefits and risks, which are summarised in the table below.

Approach	Benefits	Limitations	Example
Incorporate records of online activity into existing recordkeeping practices without making any changes	<p>Minimal changes to current recordkeeping processes are required.</p> <p>Links between online and offline materials can be maintained.</p> <p>Low costs are likely to be incurred.</p>	<p>Many current systems are not capable of capturing records of online activity, especially if records are to be captured in electronic formats.</p> <p>May be difficulties in capturing the context, structure, content and metadata of records using existing processes.</p> <p>Will still require an audit of online content and practices to determine what records will be captured.</p>	<p>When an agency adds or removes a resource from its website, a paper copy is printed out and the date, time and approvals noted. The paper copy is then added to an existing file.</p> <p>Obviously the resulting record may lack context and functionality of the online resource.</p> <p>However, this approach requires few changes to current practices and can be easily incorporated into recordkeeping and web publishing processes.</p>

Approach	Benefits	Limitations	Example
<p>Modify current practices to incorporate the needs of online activities, or develop new recordkeeping systems to manage both existing records and those arising from online activity.</p>	<p>Limited changes to current recordkeeping practices are required.</p> <p>Links between online and offline materials can be maintained.</p> <p>Changes can be identified from a content and process audit.</p>	<p>Tailoring or developing new practices will incur costs.</p> <p>Will result in procedural changes that need to be communicated and managed.</p> <p>Deficiencies in the current practices may be carried across to records of online activity.</p>	<p>An agency decides to capture records of their online activity in electronic format.</p> <p>An existing recordkeeping system, which includes currently-unused functionality for managing electronic records, is expanded to allow management of electronic records;</p> <p>OR</p> <p>A new recordkeeping system is procured to allow an agency to manage all of its public records.</p> <p>New processes to adequately capture online resources are introduced to web publishing processes.</p>
<p>Develop new recordkeeping activities for online activity and link to existing systems</p>	<p>Requirements of the online environment directly addressed.</p>	<p>Major changes to recordkeeping practices may be required.</p> <p>May attract high establishment costs.</p> <p>Could lead to the siloing of online and offline records within authorities.</p> <p>Increased complexity in coordinating multiple recordkeeping systems.</p>	<p>A new recordkeeping system is procured to allow an agency to manage records created or arising from the online environment.</p> <p>The system does not include capabilities to manage existing paper files, or paper files continue to be managed using existing systems.</p> <p>Links between the paper and electronic recordkeeping systems are required to ensure the context of records is maintained.</p>