Recordkeeping for Good Governance Toolkit

GUIDELINE 12:
Introduction to Digital Recordkeeping

PARBICA
Pacific Regional Branch International Council on Archives

The original version of this guideline was prepared by the Pacific Regional Branch of the International Council on Archives (PARBICA) for use by countries around the Pacific. This means that the guideline may refer to things that you are not familiar with or do not use in your country. You may find that you need to change some of the advice in this guideline to suit your own government's arrangements. To obtain an editable copy of this guideline, contact the national archives, public record office or other records authority in your country, or contact PARBICA at http://www.parbica.org.

Recordkeeping for Good Governance Toolkit

Guideline 12: Introduction to Digital Recordkeeping

CONTENTS

WHO ARE THESE GUIDELINES FOR?

Guidelines 12 through to 19 have been created to help public sector organisations in Pacific Island nations put in place appropriate and sustainable strategies for managing their digital records. They build on earlier guidelines issued in the PARBICA Recordkeeping for Good Governance Toolkit which aim to promote good recordkeeping, and are meant to be used together with those earlier guidelines.

The guidelines can be used by anyone who works with digital records and wants to learn more about managing them effectively. They may be of most use to:

- Senior managers, who will need to approve and support any digital recordkeeping strategies;
- Records managers and records management staff, who will be responsible for implementing digital recordkeeping strategies, writing policies and procedures, and training staff; and
- IT managers and staff, who should be involved in decisions about managing, storing and preserving digital records.

WHAT ARE DIGITAL RECORDS?

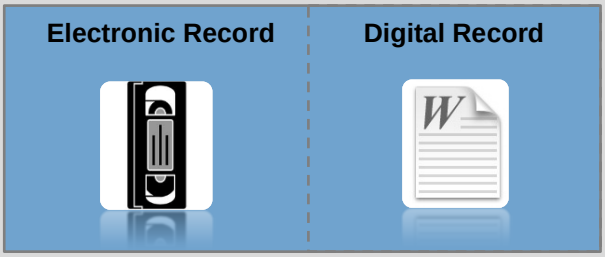
If you use a computer for your work, you create digital records. Digital records are documents, information and data stored in computer format that provide evidence of the business of an organisation. Examples of digital records include:

- Microsoft Word documents, including letters, tables and lists
- Excel spreadsheet documents such as cash flow tables and expenditure/income statements
- Emails, including attachments
- Agency websites, including software that maintains website content Other web pages including Facebook, blogs, and Twitter
- Microsoft PowerPoint presentations
- Digital images – including digital photographs captured with a digital camera or digital scans of paper documents
- Digital video
- Databases – a collection of related data that can be amended
- Instant messages (IM) – real time exchange of messages between people on a mobile phone or computer
- Information contained on personal digital assistants (PDAs)

Digital records come in different types and different formats. For instance, a digital photograph or image is a type of digital record, and for this type there could be many different formats, or ways in which the data is written. Some examples of digital image file formats include JPEG, TIFF or GIF formats. What all types and formats of digital records have in common is that they are in computer, or binary, or encoded language, and need to be translated into a language or presentation format that can be understood by people.

Digital records or electronic records?

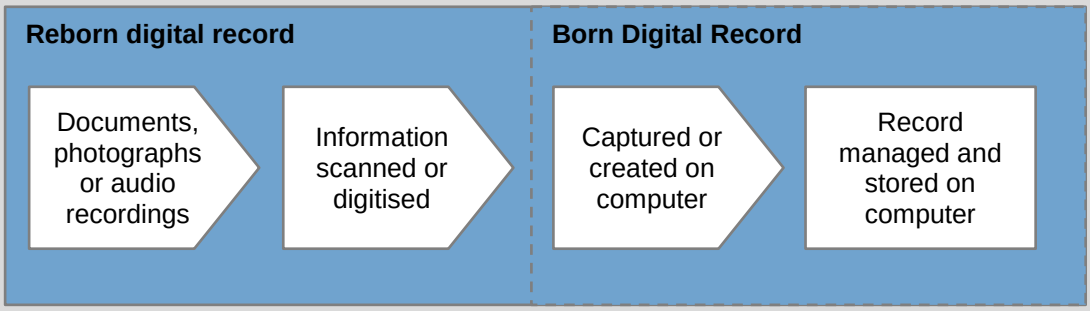
Digital records are also often called electronic or e-records, although technically the two are not the same. An analogue VHS videotape is an 'electronic' record because it requires electricity to be viewed, but it is not a digital record, as it is not composed of the computer language of zeros and ones that all digital records are. All digital records are electronic records, but not all electronic records are digital records.



In some ways, digital records are very different to paper records. They are the result of the combination of hardware (such as your computer), software (a program such as Microsoft Word) and data (the digital file). Paper records, on the other hand, are 'fixed': they always appear the same and don't need equipment to be viewed. Like paper records however, digital records need to be created, controlled, preserved and organised to make sure that they provide full and accurate evidence of business activities for as long as that evidence is required.

Born-digital or reborn-digital records?

Digital records are sometimes referred to as **'born-digital' records**, meaning that the content was originally created as a digital file. **'Reborn-digital' records** are digitised or scanned copies of information that was originally in analogue form, for example paper documents, photographs and analogue audiovisual recordings.



WHAT IS METADATA, AND WHY IS IT IMPORTANT?

For information to have meaning and value as evidence of a decision, transaction or activity – in other words, for it to be a record – it needs to include or be linked to other information that describes the content, context and structure of that record. Sometimes called 'data about data', the technical term for this information in the digital world is 'metadata': machine-processable data that is managed separately from the data that it describes. Metadata is so important because it allows people to find, use, understand, manage and preserve records over time.

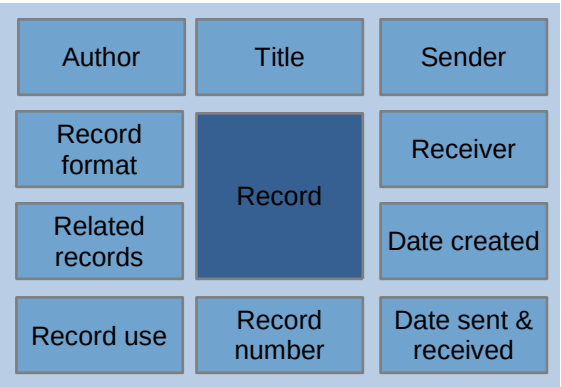
Another way to think about records and metadata is to imagine the records as cans of fruit and the metadata as labels attached to it. If the labels come off the cans of fruit and go missing, you are left with objects that you can't identify. Similarly, if you only have the labels, you have no idea how you will find the objects they describe.

Like cans of fruit without labels, records without metadata are disconnected from the context of their creation and use, and are meaningless pieces of information. Records without good metadata cannot be properly understood, managed, preserved, or found by users who need them.

In recordkeeping terms, metadata is not new. Records have always needed documentation about their content, context and structure – for example index cards, file registers, file covers, file inventories, letterheads and signature blocks. In the digital world we need more metadata than in the paper world, as digital files cannot be used or understood without accompanying technical metadata.

Common examples of metadata about the content, context and structure of records include:

- what the record is about
- who created the record
- who sent the record
- who received the record
- key action dates
- identification numbers for when the record is captured into a records system
- links to any related communication
- the file format of the digital record – is it a PDF document, a HTML web page, a JPEG image, an email, an MP3 audio file, etc?
- information about who has used the record.



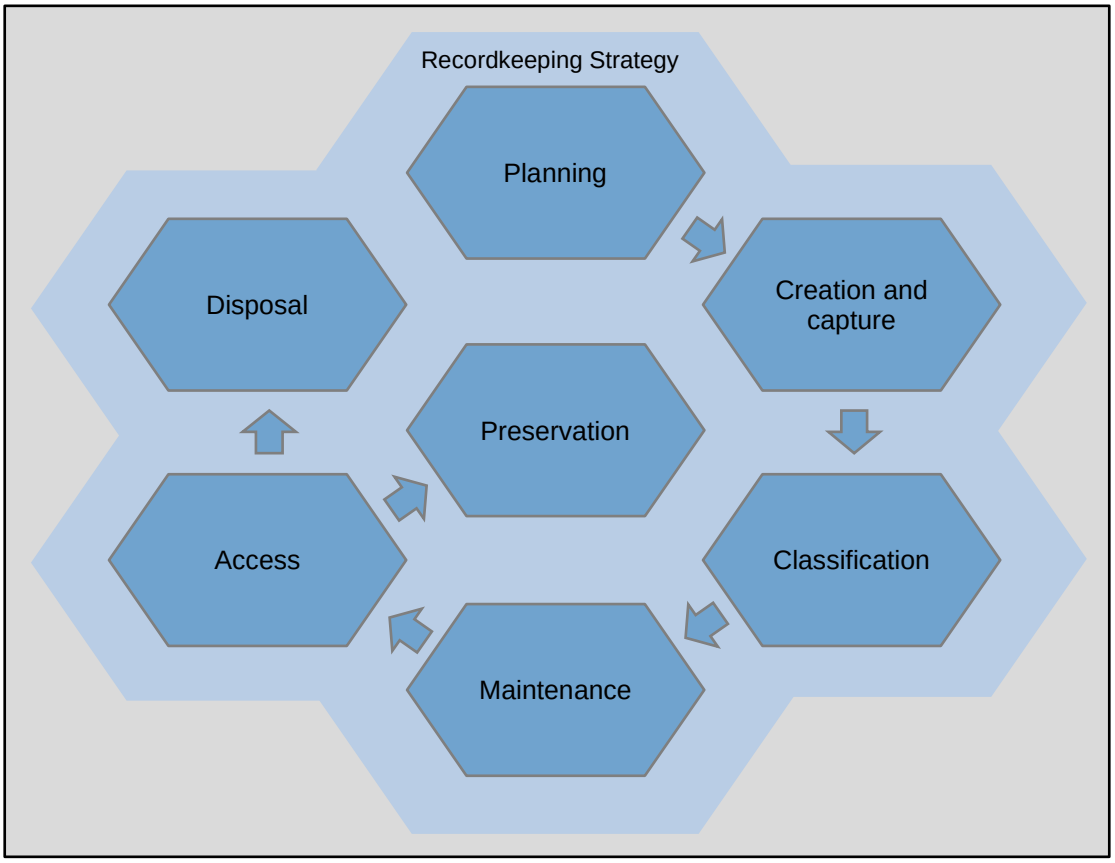
Examples of record metadata

More information about recordkeeping metadata can be found in ISO 23081 – parts 1 and 2, *Metadata for Records: Principles* and *Implementation Issues*.

WHAT IS DIGITAL RECORDKEEPING?

The term ‘digital recordkeeping’ refers to the different activities and processes involved in managing a digital record over the course of its life. The table overleaf and the diagram below show key activities making up a digital recordkeeping strategy:

- planning;
- creation and capture;
- classification;
- maintenance;
- access;
- disposal; and
- preservation.



As the recordkeeping activities are the same regardless of whether a record is paper or digital, the table overleaf includes links to earlier guidelines in the PARBICA Toolkit where appropriate, as well as to the relevant guidelines in this current Toolkit phase.

Recordkeeping activity	Why is it important?	Which Toolkit guidelines provide information on it?
Planning	The success of a digital recordkeeping strategy depends on good planning. Planning activities may include developing a policy on records management, identifying the need for a strategy and setting out possible options, and determining costs and benefits.	Guideline 1: Recordkeeping Capacity Checklist Guideline 2: Identifying Recordkeeping Requirements Guideline 3: Model Record keeping Policy Guideline 13: Digital Recordkeeping Readiness Self-assessment Checklist Guideline 14: Digital Recordkeeping – Choosing the Best Strategy Guideline 16: Systems and Software Checklists Guideline 19: Implementing a Digital Recordkeeping Strategy
Creation and capture	Records need to be captured in a way so they cannot be altered. To have value as evidence of business activity, they must also have accompanying metadata: data that provide further information about the record.	Guideline 4: Administrative Record Plan Guideline 5: Adapting and Implementing the PARBICA Administrative Record Plan Guideline 17: Managing Email
Classification	Classifying records, using a record plan or business classification scheme, makes it easier for organisations to capture, title, find and dispose of records. Classification groups records, and links them to the business context in which they were created.	Guideline 4: Administrative Record Plan Guideline 5: Adapting and Implementing the PARBICA Administrative Record Plan Guideline 6: Developing and Implementing Record Plans for Core Business Functions
Maintenance	Record maintenance includes establishing user and access controls over records to make sure they are secure and cannot be altered.	Guideline 7: Disposal Schedule for Common Administrative Functions
Access	Records should be able to be searched for, found and retrieved so they can be used by those who need them. Good metadata is vital to finding and retrieving records.	

Disposal	Disposal refers to what happens to a record at the end of its active life, which could either be destruction, or retention of the record as an archive – a record of permanent value.	Guideline 7: Disposal Schedule for Common Administrative Functions Guideline 8: Implementing the Disposal Schedule for Common Administrative Functions Guideline 9: Adapting the Disposal Schedule for Common Administrative Functions
Preservation	Active preservation aims to make sure records can be used for as long as they are needed. It begins before a record is created and continues throughout the life of the record. Preservation includes storage, record authenticity and reliability, and computer technology going out of date.	Guideline 18: Digital Preservation

DIGITAL RECORDKEEPING CHOICES

Any organisation that has computers needs to make some key choices when it comes to digital recordkeeping, such as whether to:

1. preserve and manage ‘born-digital’ records in digital form, or print those records to paper, keeping the paper copy as the official record and disposing of the born-digital original;
2. continue to manage paper records, or to scan or digitally reformat those records and treat the ‘reborn-digital’ copies as the official records of the organisation; or
3. maintain hybrid records systems that are a mixture of paper and digital records.

Guideline 14: Choosing the Best Strategy, provides detailed guidance for organisations faced with these choices. The most appropriate option for an organisation will depend on its level of digital recordkeeping readiness. Guideline 13: Digital Recordkeeping Readiness Self-assessment Checklist for Organisations, will help your organisation to determine its readiness.

DIGITAL RECORDKEEPING BENEFITS AND RISKS

Unlike paper records, digital records require ongoing active management, or if not, they become unusable over time.

Managing digital records properly can bring many benefits to an organisation, ranging from more consistent and efficient business processes to improved public confidence and trust. If work is being carried out using automated systems then it makes sense for the records of that work to be made and kept in digital form. However, it is not easy to manage digital records. There are serious risks and challenges that can impact upon digital recordkeeping, and these should be considered carefully when choosing a recordkeeping strategy. *If your organisation is going to do digital recordkeeping it has to be confident that it can do it well, because bad digital recordkeeping will almost certainly be disastrous.* If you are not confident that you can implement good digital recordkeeping it is better to stick with paper-based recordkeeping systems until you feel that your organisation is ready. Organisations looking to implement an effective strategy to manage their digital records well will find there are many different options. For more information on choosing an appropriate strategy, see Guidelines 13 and 14.

Benefits of *good* digital recordkeeping

If your organisation has a good program for digital recordkeeping in place the following benefits may be achieved:

- Records can be accessed anywhere, at any time by any authorised person who has access to the organisation's computer network (unlike paper, which can only be used by one person at a single location).
- Records can be more easily found and retrieved by the people that need them.
- You don't need to create multiple copies of records, as with paper records.
- Organisations may be more accountable and compliant with legislation and policy.
- Records are more secure due to access controls. Because they are more secure, they are more authentic and reliable.
- Cost savings, due to less duplication and double-handling of records.
- Future cost savings – for example, evidence can be quickly provided if it is needed in court, instead of having to spend time and money finding information.
- A better reputation for your organisation, with improved public confidence in its activities.
- Having an effective recordkeeping system where people can find the information they need improves morale and job satisfaction, and builds a more positive and productive internal culture.

- If an organisation already uses computers to do its work, it is more efficient for the records of that business to be kept in computerised form.
- Establishing control over information that is spread over a wide area, for example multiple offices across the country or in different islands.

Risks and challenges of digital recordkeeping

Although digital recordkeeping may bring benefits to your organisation, you should be aware of the following risks and challenges:

- The sheer amount of information created and generated, and the speed at which digital information is created and sent. It may be difficult for staff to know what digital information should be captured as an official record. Staff may also struggle to find the time to make and keep adequate records if they are overworked and lack training.
- Technological obsolescence, or computer software and hardware going out of date, can make records unusable. One strategy for dealing with this is to migrate digital records across new systems and software over time. See Guideline 18: Digital Preservation, for more information on managing this risk.
- Preserving digital records so that they remain authentic and reliable evidence of business activity. Unlike paper records which can be moved, copied and used without changes, a digital record can be changed easily or even deleted, losing its integrity and reliability as evidence.
- Loss of security and privacy. Any computer or digital archive that is connected to a network can be hacked into. Organisations using computers to manage sensitive or private information need to make sure that records in their care are protected from misuse, loss or damage.
- Digital storage devices and media can be fragile and easily damaged.
- Poor choice of software applications or systems.
- The long-term costs of managing digital recordkeeping. Any new system implementation will have ongoing, as well as upfront, costs. Often the ongoing or hidden costs can be significant – for every dollar an organisation may spend on a new system, they may need to spend up to 10 dollars on change management. See Guideline 19: Implementing a Digital Recordkeeping Strategy for more information on managing this risk.
- Relying on third parties such as internet service providers or outsourced data storage providers can reduce the control an organisation has over its assets. In the Pacific Islands vendor support may be from a distant foreign country and may disappear overnight.

- Lack of access to resources such as IT support and software vendor assistance. This can be addressed by negotiating and managing a good contract with service suppliers and through good staff training. Many organisations in the Pacific will lack the IT resources to deal with issues locally.
- Users can be resistant to new ways of doing things. It is very important to manage change. See Guideline 19: Implementing a Digital Recordkeeping Strategy for more information on managing this risk.

15 DIGITAL RECORDKEEPING MYTHS

Myth	Reality
1. Everything on a computer is 'safe'	Digital information can easily be lost and needs to be properly managed in a recordkeeping system to be safe.
2. Information generated on my computer is not a record	Information created on your computer or any digital communication device in the course of your work is a record. Digital information can be a vital source of evidence about how an organisation performs its work, makes decisions and interacts with clients. Email can be a record. An SMS or text message can be a record. Any information that records a business decision or transaction is a record.
3. Digital storage is cheap	While the unit cost of digital storage is getting cheaper, the amount of digital information organisations are creating and keeping is rapidly expanding. As a result the total storage bill is likely to increase, even though the per-unit costs may be going down. Storage is just one of the costs associated with keeping digital records – digital records also need to be actively managed by trained staff, and these management costs are not cheap.
4. Computers will create a paperless office	The opposite is usually true – as organisations get more computers they tend to buy more paper for printing.
5. All information generated or received on my PC at work is my personal property	Information generated or received on a work computer or during work time is usually the property of your employer.
6. Scanning provides a cheaper and more reliable way of storing information	This is sometimes true and sometimes false. See Guideline 15 for more information on the advantages and disadvantages of scanning and recordkeeping issues relating to scanning projects.
7. 'Archiving' (in the IT sense) is the same as digital recordkeeping	Software programs increasingly use the word 'archiving' (such as the pop-up box in email software programs that asks if you would like to 'auto-archive'). This refers to data storage only, not the recordkeeping activities needed to make sure records can be properly controlled, found and retrieved.

8. Databases such as spreadsheets are reliable forms of evidence	To be reliable and authentic, a record must be unchangeable. Spreadsheets by their nature are easily altered.
9. Outsourcing will solve all my problems	Outsourcing can create problems if roles and responsibilities are not in contracts and if those contracts are not properly managed. Remember, you can outsource the work, but you cannot outsource the responsibility.
10. Google will help me find everything I need, therefore I don't need to manage my digital information	Google is a web search engine, not a records management tool. It is not a substitute for good records management.
11. Our shared drive is good enough for managing our records	Shared drives often end up being everyone's – and no-one's – responsibility. There are ways to manage your shared drive more effectively, but they usually lack the controls and functions of a recordkeeping system. See Guideline 14 for advice on keeping records in shared drives.
12. When I delete an email it has been destroyed	All that gets destroyed usually is the link to the record – the original record can usually still be retrieved.
13. Digital records cannot be used as evidence	This depends on the laws and rules of evidence in your jurisdiction. Increasingly, as in Australia and New Zealand, jurisdictions are moving to accept digital records as admissible evidence in courts.
14. I will be able to access my digital records in 10 years' time	Unlike a folder of paper documents, a digital record cannot be placed on a shelf and someone will be able to read it in ten years' time.
15. Recordkeeping is not my responsibility	All staff who create, send and receive digital information have recordkeeping responsibilities.

OVERVIEW OF TOOLKIT DIGITAL RECORDKEEPING GUIDELINES

The PARBICA guidelines on digital recordkeeping aim to help organisations in the Pacific region to put in place appropriate and sustainable solutions for managing their digital records. This will help guarantee that digital records of government activities and decisions are properly managed to ensure their integrity, authenticity, usability, accessibility and survival for as long as they are needed.

The guidelines are:

Guideline 12: Introduction to Digital Recordkeeping
Provides an overview of digital records and recordkeeping, addressing key concepts, benefits, risks and myths. Includes glossaries of key terms.

Guideline 13: Digital Recordkeeping Readiness Self-Assessment Checklist for Organisations
Allows organisations to assess their resources, policies, procedures, tools, technologies, training and organisational culture to help them determine their level of readiness to pursue a digital recordkeeping strategy.

Guideline 14: Digital Recordkeeping – Choosing the Best Strategy
Addresses seven different options for managing digital records, looking at the advantages and disadvantages of each. The options are: printing to paper and filing; using shared drives; using collaboration software; scanning paper records for access and preservation purposes; developing hybrid systems; using an electronic document and records management system (EDRMS); and using an existing business system.

Guideline 15: Scanning Paper Records to Digital Records
Practical advice for organisations considering a scanning project looks at the various processes involved in a scanning project from planning to file storage, risks and issues such as outsourcing, and includes information on technical standards and the different equipment available.

Guideline 16: Systems and Software Checklists
The three parts of Guideline 16 are designed to be used by different sections of an organisation.

16A is a checklist that allows a records manager to see at a glance how well their existing business systems meet core recordkeeping requirements.
16B allows assessment against high-level recordkeeping principles (ICA-Req statement of principles), and is designed to help gain senior management approval for a business case or project.
16C allows assessment of the systems against detailed functional recordkeeping requirements, and is designed to be completed by an IT manager. As well as allowing organisations to test how well their existing

business systems support good recordkeeping, the tools can also be used to build a design of preferred recordkeeping functionality for future systems, or as a benchmark if a systems audit is required.

Guideline 17: Managing email
Practical advice on email management, including why emails should be captured, when to capture, how to store, and tips for managing email.

Guideline 18: Digital preservation
Looks at issues such as preserving authenticity and access, and dealing with computer technology going out of date. Explains open and proprietary formats, and provides examples of low-budget digital preservation solutions. Also examines the digital reformatting of analogue audiovisual recordings.

Guideline 19: Implementing a digital recordkeeping strategy
The processes needed to support and enable successful implementation of a digital recordkeeping strategy. Includes project planning through to rollout of a strategy.

RECORDS MANAGEMENT GLOSSARY – for IT Managers

Appraisal – the process of evaluating business activities to determine which records need to be captured and how long they need to be kept to meet business needs and community expectations.

Archives – records that are to be kept permanently because of their continuing legal, administrative, financial or historical value.

Authenticity – a record that is authentic can be proven to

- be what it says it is;
- have been created or sent by the person supposed to have created or sent it; and
- have been created or sent at the time stated.

Born digital – materials that originate in digital form and do not have an analogue equivalent.

Business email – an email that contains information created or received by the organisation in the course of work.

Capture – the process of lodging a document or digital object into a records management system and assigning metadata to describe the record and place it in context, to allow the appropriate management of the record over time.

Classification – the process of identifying and arranging business activities and the resulting records into categories according to logically structured conventions, methods and procedural rules.

Context – describes the ‘who, what, when, where and why’ of records creation and management. Records require context to be meaningful and have value as evidence.

Disposal – the range of processes documented in a disposal authority which determine whether a record is to be kept, destroyed or transferred.

Document – document is any piece of written information in any form, produced or received by an organisation or person. All records start as documents, but not all documents will ultimately become records.

Integrity – the quality of a record being whole and unaltered through loss, tampering or corruption.

Metadata – data describing the context, content and structure of records which enables their discovery, use, management and preservation through time.

Original order – the sequence or grouping in which archival records were originally accumulated or kept by their creator. Maintaining the original order preserves the context of creation and the records' authenticity.

Provenance – the relationships between records and the organisations or individuals that created, accumulated and/or maintained those records.

Reborn digital – digitised or digitally reformatted copies of information that was originally in analogue form, for example paper documents, analogue audiovisual recordings.

Record – information created, received and maintained as evidence and information by an organisation or person according to legal obligations or in the transaction of business.

Recordkeeping – creating and maintaining complete, accurate and reliable evidence of business transactions in the form of recorded information. Includes the:

- creation of records in the course of work and the means to ensure the creation of adequate records;
- design, establishment and operation of recordkeeping systems; and
- management of records used in business and as archives.

Records disposal authority – lists categories of records and the retention period, disposal sentence and custody arrangements for each category.

Retention – the function of preserving and maintaining records for continuing use. Records may be retained in the system of origin, or transferred to a separate repository such as an offline system, records centre or archival institution.

INFORMATION TECHNOLOGY GLOSSARY – for Records Managers

Automation – the use or introduction of automatic equipment in a manufacturing or other process or facility.

Business system – an automated system that creates or manages data about an organisation's activities.

Conversion – the process of changing a record from one format to another, or from one type of computer system or software to another.

Digital record – a record that has been created in digital form that requires a combination of computer hardware and software to be read and understood.

Digital preservation – series of managed activities undertaken to ensure continued access to digital materials for as long as necessary.

Digital signature – information which, using cryptographic techniques, provides guarantees of the authenticity and/or reliability and/or authorship of a digital file.

Electronic Document and Records Management System (EDRMS) – a system used to manage the creation, use, management and disposal of both paper and electronic documents and records. An EDRMS can:

- support the creation, revision and management of digital documents;
- improve an organisation's workflow; and
- provide evidence of business activities.

These systems maintain appropriate metadata or contextual information, and links between records to support their value as evidence. They are sometimes referred to as Records Management Applications or RMAs.

Email – an electronic mail message sent or received using an email system. See also business email.

Functional requirements – the tasks a computer application must perform to carry out a process satisfactorily, or the conditions or performance standards that a computer system should meet in order to support the business of the organisation.

Interoperability – the ability of one computer application, system or metadata scheme to communicate, work or interface with another.

Legacy system – a previous generation or version of an information technology system and its contents. Can include paper-based systems.

Migration – changing the format of digital information so that it can be viewed and used with different, usually newer or longer-term, hardware and software, while maintaining the authenticity, integrity, reliability and usability of the information.

Network server – a computer system that serves as a central repository of data and software programs shared by users who can access those resources through a computer network.

Open format – a data format that is not considered proprietary and is free of commercial ownership or patents. Typically the technical specifications for the format are also publicly available, allowing users to change and develop the format to suit their needs.

Open source software – computer software that is distributed free of charge under a licensing arrangement and which allows the computer code to be shared, viewed and modified by other users and organisations. Open source software development is often performed by a distributed community of software developers via the internet.

Personal email – an email that relates to a private or personal matter and has no relevance to the business of an organisation.

Platform – the type of computer or operating system on which a software application runs. Some common platforms are PC (Windows), Macintosh and Unix.

Proprietary format – computer software applications and/or file formats that are developed, owned and controlled by a private commercial entity, where the software code or specification is not readily available and usually cannot be used without paying a licence fee.

ACKNOWLEDGEMENTS

The PARBICA Bureau would like to acknowledge the assistance of the following people who participated in the Reference Group that was responsible for guiding the development of Guidelines 12 to 19:

Amela Silipa	Samoa
Vaveao Toa	Samoa
Jacob Hevelawa	Papua New Guinea
Tukul Kaiku	Papua New Guinea
Jeannine Daniel	Cook Islands
Salote Vuki	Tonga
Salesia Ikaniwai	Fiji
Torika Cakacaka	Fiji
Naomi Ngirakamerang	Palau
Mark Crookston	New Zealand
Anna Gulbransen	New Zealand
Helen Onopko	Australia
Adrian Cunningham	Australia
Elizabeth Nannelli	Australia
Emma Buckley	Australia
Henry Ivature	Pacific Islands Forum Secretariat

The Recordkeeping for Good Governance Toolkit is produced by the Pacific Regional Branch of the International Council on Archives with assistance from the National Archives of Australia and AusAID.