Recordkeeping for Good Governance Toolkit

PARBICA
Pacific Regional Branch
Branche Régionale pour le Pacifique

GUIDELINE 23:
Identifying Vital Records for Government Departments

Acknowledgements

The disaster management guidelines of the PARBICA Recordkeeping for Good Governance Toolkit were kindly supported by the Programme Commission of the International Council on Archives.

Project Managers: Fiona Gunn and Helen Walker, National Archives of Australia

Authors: Brandon Oswald, Island Culture Archival Support

Lillie Le Dorré / Talei Masters, Archives New Zealand

Fiona Gunn, National Archives of Australia

Thanks to the following people who provided advice on the guidelines, peer-reviewed the guidelines and provided editing support:

- Opeta Alefaio, National Archives of Fiji
- Eric Boamah
- Greg Doolan
- Margaret Inifiri, National Archives Solomon Islands
- Tukul Kaiku
- Emilie Leumas and Gregor Trinkaus-Randall, ICA Expert Group on Emergency Management and Disaster Preparedness
- Linda Macfarlane and Monique Nielsen, National Archives of Australia
- Tess Perez, Yap State Archives
- Noa Petueli Tapumanaia, Tuvalu National Library and Archives
- Ros Russell
- Amela Silipa, National Archives and Records Authority Samoa
- Margaret Terry and Augustine Tevimule, Vanuatu National Library and Archives.

Special thanks to the PARBICA Bureau.

Contents

Introduction

The Pacific Regional Branch of the International Council on Archives (PARBICA) has developed this guideline on ***Identifying Vital Records for Government Departments*** as part of the Recordkeeping for Good Governance Toolkit. It was drafted in consultation with the Pacific Island Reference Group made up of representatives from the following countries:

- Australia
- Federated States of Micronesia
- Fiji
- New Zealand
- Papua New Guinea
- Samoa
- Solomon Islands
- Tuvalu
- Vanuatu.

Who is this guideline for?

This guideline can be used by anyone seeking to understand which business records a government department must have access to in order to carry out its day-to-day business or which must be kept by law. Once information about these records has been captured, it can be used in situations where business may be disrupted, such as a disaster, or as evidence for accountability and good governance.

It can be useful to have a team of people working together to identify vital records such as:

- senior managers in the department
- operational staff from each area of the business, who have a good understanding of how the organisation works
- records management staff from within the organisation
- staff from the government archives or national library
- staff from the government audit office or who have other audit experience.

The work of identifying which records are vital will usually be done by someone who works inside the government, although it may be possible to hire an expert consultant to guide the work or a temporary staff member who can concentrate on the project.

What are vital records?

Vital records are those business records that a government department must have access to in order to do the essential day-to-day business of the office. These records are irreplaceable and would require significant resources and commitment to recreate if lost or damaged. Vital records protect the assets and interests of a department, its clients and stakeholders, and are usually associated with a department's infrastructure, legal and financial matters.

Vital records will only be a small proportion of a department's total records, often around 5% of the total records created by the department. Vital records could be paper files, computer files, maps, plans, financial records, etc. The majority will be 'active' records – that is, current and in regular use. Steps must be taken to protect these vital records from damage so that they remain accessible.

In any department, there will be **vital**, **important** and **useful** records. Understanding the differences between these is important to determining which records are vital to your department's operation.

Important records are those business records that:

- have *some* value to the department, such as helping to restore operations during or after an emergency
- would inconvenience the department if lost or damaged but their loss would not halt operations
- can be replaced at a moderate cost.

Examples of important records include accreditation documents, annual/monthly/quarterly reports, billing source documents and current calendars or appointment books.

Useful records are those business records that:

- are handy but not critical in an emergency
- would inconvenience the department if lost or damaged but their loss would not halt operations
- can be replaced at a moderate cost.

Examples of useful records include subject files or existing but non-current agreements.

Vital records are not those records cared for as archives – see ***Guideline 24: Assessing Significant Records in Archival Holdings*** for information on identifying and protecting significant heritage records.

As the business of each department is different, this means that the list of vital records for each department will also be different. Vital records may be considered vital only in the short term or may retain their status indefinitely. Some examples of vital records include:

- contracts or agreements that prove ownership of property, equipment, vehicles, products, etc.
- operational records such as current accounting and tax records, current personnel or payroll records, account histories, and shipping records
- current client files
- current standard operating procedures (SOPs)
- produced reports and summaries
- software source codes (including both licensed programs and systems, and custom developed applications).

Examples of core functions and records vital to those functions can be found in **Appendix A**.

Why identify vital records?

Identifying vital records is an important part of ensuring that the department can continue its business in any event and meet any legal recordkeeping requirements. This makes identifying vital records a key part of planning for disasters, but it is useful information even if you do not have a complete Disaster Preparedness Plan.

Disruptive events may cause confusion and uncertainty; if the department knows what activities to focus on, it can resume vital business quickly. If the vital records have been identified and steps have been taken to protect them, the department will be able to limit damage to them, access them faster, and resume business.

How to identify vital records

Identifying the records vital to a department should be part of a broader analysis of the department's recordkeeping requirements. There are four key steps to identifying vital records:

1. identifying and collecting information on core functions
2. recognising vital records
3. documenting information on the identified vital records
4. prioritising vital records.

In many ways, identifying vital business records is similar to undertaking an appraisal in that it is a systematic way of deciding the value of records. ***Guideline 10: Starting an Appraisal Programme*** can be used in conjunction with this guideline.

1. Identifying and collecting information on core functions

The first step in identifying vital records is to understand which functions your department needs to keep performing to maintain critical operations during and after an event, and in order to meet your legal obligations. Functions are the goals or purposes of an organisation. An organisation undertakes activities in order to perform its functions.

Your records management team may already have done work that can help you identify vital records based on functions. For example, you might have a Record Plan that documents your activities in each core function effectively and identifies records consistently (see ***Guidelines 4-6*** on developing Record Plans). Record Plans use an understanding of an organisation's functions and activities to provide headings for file titles. If you have listed your department's activities, then you can decide which records are vital. You can also use your record plan to find out which records are required to perform those functions.

You may also have a Disposal Schedule for your records (see ***Guidelines 7-9*** on developing Disposal Schedules). A Disposal Schedule is produced by appraising all records across the department and is usually arranged by functions and activities. A Disposal Schedule usually maps to the Record Plan. If you have a Disposal Schedule, you can work through the classes to determine which records are required for critical operations and legal obligations.

If you do not have a Disposal Schedule, you might have a basic information audit, inventory, or survey. Your records management team may have already carried out a survey across the department in the past. This would contain all records being created, why they are created, what they are used for, where they are stored and how many there are. If you have an inventory, you can make sure it is current and identify which of the listed records are vital.

If your department has none of these sources, you will need to rely solely on gathering information from senior managers and the staff who carry out operational activities.

2. Recognising vital records

Once your list of functions, activities and record classes has been compiled, you will be able to identify the records essential to your operations. Gather your group of managers, staff, records managers, archives staff and any other useful personnel. Discuss and agree on the following:

- Which functions must your department continue to perform to maintain critical operations?
- Which functions must your department continue to perform to meet legal obligations?

Then discuss and agree on the following:

- Which records contain information that is vital to continuing the critical functions of your department?
- Which other records are required for your department to continue working under extraordinary circumstances?
- Which records are needed to confirm your department's legal and financial status?
- Which records are essential to protecting the rights of staff and customers?
- Which records are essential to protecting or recovering critical systems, facilities or equipment?
- Which records are unique or would be extremely expensive to replace?
- Which records would lead to severe negative consequences if unavailable?

Consider the following factors in your discussions:

- Does the information exist elsewhere - in the records of other departments or organisations, for example, and what is the likelihood of them losing access to that information at the same time?
- Can the records be replaced or reconstructed from other sources? How long would this take, how much would this cost, and what would the impact be on continuing critical activities?
- Will the information be required in its original form to be valid for use in activities?

When undertaking this step, remember:

- to assess all of the department's records, regardless of location and format
- not all important records may be considered 'vital' to the agency's recovery of core business functions – refer to the list of examples provided earlier in this guideline
- that vital records should be easily accessible, up-to-date and identified as critical to the recovery of business operations.

3. Documenting information about vital records

This step has two main objectives: to document the process taken to identify your department's vital records, and to document the records themselves.

Document the process you followed to agree on which functions and records were vital. This should include a record of which staff members were involved and in what capacity.

A Vital Records Register is a simple way to capture information relevant to your identified vital records. The register should include:

- a brief description of the record type
- an explanation of the business functions and activities the records support
- the location of the records, e.g., onsite, offsite, of original, of duplicate, server, data centre, backups, mirror sites
- the date for review, update or disposal
- the format of the record
- any accessibility requirements, e.g., position, authorisation, software or equipment.

An example Vital Records Register is at **Appendix B**. Ensure that the register is approved and signed by the most senior manager. This is important as a record of organisational commitment to protecting your vital records.

4. Prioritising vital records

Even within the subset of records identified as vital, it is advisable to rank them according to priority. This will help with prioritising disaster planning, response and recovery activities.

Your Vital Records Register can group records as Priority A, B, or C. This can help you determine the best risk mitigation strategies and storage options for each group of records. For example:

- Priority A – likely to be required at your disaster response site, usually your normal office place of business.
- Priority B – need to be accessible at your disaster recovery site, usually where you will attempt to resume operations if you cannot access your normal place of business.
- Priority C – could be stored at offsite locations that are unlikely to be damaged in the same event as your normal place of business.

Managing vital records

Managing vital records is part of the process to ensure that those records identified as vital to the continuing operation of the department are available in the event of a disaster.

Risk assessment

The purpose of a risk assessment is to safeguard vital records by determining and evaluating the exposure of vital records to specific risks. Risk assessment provides the basis for protection planning and other records management decisions.

Work through your Vital Records Register, carrying out a risk assessment for each type of record. Begin by identifying the threats and vulnerabilities to which your vital records are exposed. Risks to vital records can be broken down into three broad categories:

- destruction
- loss
- corruption.

A risk assessment can be based on intuitive, relatively informal qualitative approaches or more formal, quantitative methods. A qualitative approach will see you consider the actual or potential risks to the records, describing the impact of that risk being realised, assessing the severity of that impact and the likelihood of the risk being realised.

In assessing risk, you should consider:

- your department's building and office space where records are stored
  - identify physical threats to the building or location
  - where are the high risk areas, such as basements near water pipes, heaters, potential fire hazards
  - what security measures are in place?
- storage methods for business records
  - location, e.g., basement, attic, offsite, etc.
  - format, e.g., physical, digital
  - accessibility, e.g., how quickly can the records be retrieved?
  - contingency plans, in case of loss of personnel, locked encryption data, loss of power, etc.

- the costs associated with vital records
  - reproduction, recovery and business value lost
  - protection and supplies.

A basic risk assessment matrix is included at **Appendix C.**

Once the actual and potential risks have been identified, consider and document the specific actions that the department will take to reduce the likelihood of the risk or the severity of the impact. Examples of risk this mitigation could be:

- special storage measures for vital records, e.g., fireproof filing cabinet
- duplicating vital records and storing copies offsite
- dispersing records across more than one site
- protecting records by moving them to less hazardous storage areas
- reducing risk by repairing unsafe facilities or hazardous equipment
- developing formal agreements with emergency services and other departments
- assigning specific emergency response responsibilities to personnel.

Assessing risk is part of your disaster preparedness work - see ***Guideline 20: Developing a Disaster Preparedness Plan*** for further information on assessing risk.

Disaster planning and response

Use the Vital Records Register in your disaster planning activities. For example, you might share a storage area plan with the fire service and give them periodic tours of the facility. This will enable them to know where the vital records are stored in order to concentrate firefighting activity and avoid damaging critical areas with water.

Knowing where your vital records are located will help to ensure you have the correct equipment nearby to protect them fast - for example, enough tarpaulins to cover those shelf units. You will also know where to concentrate your salvage efforts during disaster response.

If you know what equipment is essential for accessing information in your vital records, such as microfilm reader or computer software, you could try to ensure that this is available offsite in advance of an emergency.

Storage of vital records

It is good recordkeeping practice to store all records, not just vital records, as securely as possible. Extra steps can be taken to protect vital records so they are safe in case of an emergency. This can include:

- onsite, using a fire- and flood-proof safe or storage area, data backups
- offsite in a storage facility or data centre with the same disaster prevention measures as your main site. Offsite storage should also have the equipment required for accessing records and working communications technology
- across a variety of secure secondary locations.

Storage should be suitable for the record format and identified risks. Establish procedures for regular back up of digital vital records. Ensure that vital records are easily identifiable and distinguished from other records. To make sure your plans will work, run test procedures on how to access vital records in an emergency.

Reviewing information about vital records

It is essential that your department's Vital Records Register is reviewed periodically to ensure the records listed, and the information about them, remains current. This is particularly important should the department's functions or activities change significantly. Such changes might require modification of the Vital Records Register.

Review your Vital Records Register every time you review your Disaster Preparedness Plan. Ensure that a review date is recorded on the latest version of the register and record which staff position is responsible for leading the review.

Your department's functions and activities may change over time and the records may change in status over time. They should only remain on the register if they are vital, otherwise you will waste valuable effort and cost in protecting them unnecessarily.

References

Stanborough, C 2005, *Yap State Archives Disaster Preparedness and Response: A Manual for Records.*

Saffady, W 2005, 'Risk analysis and control: Vital to records protection', *The Information Journal, 39*:5, pp 62-68.

United Nations Archives and Records Management Section, *Records and Information Guidance 3: How do I know which records are vital?*

University of Wisconsin 2017, *University employee guide to: Creating a university vital records plan, r*etrieved 25 September 2017, https://www.library.wisc.edu/archives/wp-content/uploads/sites/23/2016/01/2017Vital-Records-GuidanceMay.pdf.

Appendix A - Examples of core functions and records vital to those functions

Civil Registration

- BMD registers contain the original data, from which replacement certificates can be issued.

Passport Service

- citizenship registers contain the original data, from which replacement passports can be issued.

National Archives

- accession registers contain the information on which records the institution holds, which department transferred it and what its original identifying number was.

Healthcare

- x-rays
- patient registers

Procurement

- contracts

Legal

- patents
- copyright registers
- leases
- deeds

Property

- leases
- deeds
- building blueprints/plans

Appendix B - Example of a Vital Records Register

ID	Type	Area responsible	location	Business Owner	Controlling System (digital records)	Format	Why vital?	Risks	Protection measures	Recover if backups are suitable*	Disposal Schedule / class
1	General ledger	Finance Department	Level 2 West		Financial system	Digital	Records expenditure and revenue. Loss would cause difficulty in meeting audit responsibilities.	Data corruption Fire Fraud Hackers Viruses	Completed back-ups daily Store Back ups off-site	No	DA2200 12.01.01
2	Records registry	Records Department	Level 2 East		TRIM / RecFind / Objective / ECM etc	Digital	Control system which allows access to organisation's records and contains information showing integrity, authenticity and reliability of records. Required as State archives.	Data Corruption Fire Fraud Viruses Hackers	Completed daily back-ups Store Back ups off-site File Creation Forms Virus checkers	Yes	
3	Title deeds	Legal Services Department	Level 2 West		TRIM / RecFind / Objective / ECM etc	Digital / Paper	Shows ownership of Council owned properties. Loss would make ownership difficult to prove.	Loss of deeds	Photocopy and store offsite Store in fire proof safe	Yes	
4	Rates books	Customer Service Department	Level 1, 1990-present Level 2 East, 1870-1990		TRIM / RecFind / Objective / ECM etc Financial system	Books	Supports rights of rate payers and Council regarding rates collected. Loss would cause difficulty in proving who has paid and may cause financial hardship. Required as State archives.	Fire Fraud Virus Hackers	Microfilm books and store offsite Back up database nightly and store offsite	Yes	

Appendix C – Basic risk assessment matrix

Measures of likelihood		
Level	**Descriptor**	**Detailed description**
A	Almost certain	Is expected to occur more than once during the life of the records
B	Likely	Will probably occur during the life of the records
C	Possible	Might occur at some time during the life of the records
D	Unlikely	Could occur at some time during the life of the records
E	Rare	May occur only in exceptional circumstances during the life of the records

Measures of consequence				
Level	**Descriptor**	**Damage or destruction**	**Security**	**Access**
1	Insignificant	Minor repairable damage to records	Unauthorised access to records is possible, but would be detected and dealt with.	Access is slightly more difficult than before
2	Minor	Minor repairable damage to vital records or records of archival value	Unauthorised access to records.	Access is delayed by up to a day
3	Moderate	Some damage to vital records or records of archival value. Extensive damage to other records.	Records are stolen and/or misused.	Access is significantly delayed
4	Major	Extensive damage to vital records or records of archival value. Complete loss of other records.	Sensitive records are stolen and/or misused.	Access is very difficult or may cost considerable amounts
5	Catastrophic	Complete loss of vital records or records of archival value, without any possibility of recovery.	Highly sensitive records are stolen and/or misused	Access is impossible

Once likelihood and consequence have been determined, the matrix below can be used to derive a risk rating from Low to Extreme. Extreme and high risks should be prioritised for treatment.

Risk Analysis Matrix					
Likelihood	**Insignificant 1**	**Minor 2**	**Moderate 3**	**Major 4**	**Catastrophic 5**
A (Almost certain)	High	High	Extreme	Extreme	Extreme
B (Likely)	Moderate	High	High	Extreme	Extreme
C (Moderate)	Low	Moderate	High	Extreme	Extreme
D (Unlikely)	Low	Low	Moderate	High	Extreme
E (Rare)	Low	Low	Moderate	High	High