

Records in Evidence

First published 1998, revised 2005

© Commonwealth of Australia 2005

ISBN 0 642 22536 2

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the National Archives of Australia. Requests and inquiries concerning reproduction and rights should be directed to the Publications Manager, National Archives of Australia, PO Box 7425, Canberra Mail Centre ACT 2610, Australia.

CONTENTS

1.	'READ ME FIRST' INTRODUCTION TO RECORDS IN EVIDENCE (2005)	5
2.	EXECUTIVE SUMMARY	6
	Your systems must stand up to scrutiny	6
	Records, technology and evidence	6
3.	RECENT CASES - MCCABE V BAT (2002) AND R V ENSBEY (2004)	7
	The implications of the rulings for Commonwealth agencies	7
	Further resources	8
4.	RECORDS IN EVIDENCE (1998)	9
	Acknowledgments	9
5.	THE EVIDENCE ACT 1995 (CTH)	9
6.	THE LEGAL ENVIRONMENT	10
7.	THE RULES OF EVIDENCE	10
8.	THE DISTINCTION BETWEEN ADMISSIBILITY AND WEIGHT OF EVIDENCE	11
9.	HOW EVIDENCE OF INFORMATION IN A DOCUMENT CAN BE GIVEN	12
	Under the Commonwealth and NSW Evidence Acts	12
	In other states, Northern Territory and Norfolk Island courts	13
10.	HOW EVIDENCE OF INFORMATION IN A DOCUMENT MAY BECOME INADMISSIBLE	14
	The hearsay rule under the Commonwealth and NSW Evidence Acts	14
	The hearsay rule in other states, Northern Territory and Norfolk Island courts	15
11.	THE RULES OF EVIDENCE IN COMMONWEALTH TRIBUNALS	15
12.	COMPLIANCE WITH SUBPOENAS AND ORDERS FOR DISCOVERY	16

13.	RECORDKEEPING REQUIREMENTS	16
	Reviewing recordkeeping practices	16
	Establishing a recordkeeping and systems management regime	17
14.	FURTHER ADVICE	19

'READ ME FIRST' INTRODUCTION TO RECORDS IN EVIDENCE (2005)

The National Archives first published *Records in Evidence* in 1998 to assist Australian Government agencies to respond to the passage of the Commonwealth *Evidence Act 1995*, legislation that marked a major reform in the administration of the federal justice system. The Act replaced much of the common law and varying State and Territory statute law on evidence that had applied for almost a century in proceedings before federal courts.

Since 1997, there have been significant legal developments affecting the issue of records as evidence: the *Electronic Transactions Act 1999* and the cases of *McCabe v British American Tobacco* (2002) and *R v Ensbey* (2004) concerning records destruction.

The *Electronic Transactions Act* affirms the legal status of electronic records and formalises the increasing use of electronic communication in business transactions. To reflect this change in context, the Archives has updated the admissibility example in *Records in Evidence* to focus on electronic records. For more information about the *Electronic Transactions Act*, see [The Archives Act and the Electronic Transactions Act](#).

The BAT and Ensbey cases concern the obligation of records creators to keep records that may reasonably be expected to be used as evidence in a legal dispute. A new section on these cases follows the executive summary.

EXECUTIVE SUMMARY

This is a brief summary of the advice contained in this guideline. Since the summary may omit information that is vital to your organisation, we encourage everyone to read the full version.

Your systems must stand up to scrutiny

The Commonwealth *Evidence Act 1995* changes the requirements for the admissibility of evidence. These changes have particular implications for recordkeeping and electronic records management in Australian Government agencies.

This document presents guidance, based on current Commonwealth laws, about the legal acceptance of records, particularly electronic records. The major areas addressed are:

- rules of admissible evidence in courts and tribunals
- compliance with subpoenas and orders of discovery
- recordkeeping requirements.

Records, technology and evidence

Agencies should take special precautions when using newer technologies to enhance the reliability of their recordkeeping systems, so that records produced by such systems can be easily found and will be more likely to be legally acceptable. Establishing the authenticity and reliability of records may depend on the accuracy of the process or system used to produce the record, the source of the information in the record, and the method and time of its preparation. Problems may arise with the admissibility of records if appropriate standards and procedures are not followed in creating and maintaining them.

Nothing can guarantee the acceptance of records in evidence before relevant courts. The admissibility of evidence in any court case is subject to compliance with the rules of admissibility and the interpretation placed upon them by the presiding judge. The advice contained here is necessarily general in nature and an agency should seek legal advice on its own particular circumstances.

RECENT CASES – MCCABE V BAT (2002) AND R V ENSBEY (2004)

The *McCabe vs British American Tobacco Australia Services Ltd* (BAT) case has signalled a significant change in the management of records required for evidence. In this landmark case, the Victorian Supreme Court ruled that BAT had destroyed the records that would have helped Rolah McCabe's case. It found that although legal proceedings were not current, BAT's policy of destroying records that they could foresee being used as evidence in a lawsuit – even if it had not yet started – was an illegal action directed specifically at preventing the litigant from having a fair trial.

While this finding was overturned on appeal (*British American Tobacco Services Ltd v Cowell*), it does signal a potential shift in the court's view on recordkeeping requirements, and may be taken up in other jurisdictions, including the Commonwealth. Specifically, the court ruled that records documenting actions where it would be reasonable to assume that there may be litigation, should now be kept whether or not a legal action has commenced. This replaces the previous requirement that records destruction cease only after the announcement of litigation.

The issue in the original McCabe ruling was correspondence between BAT and Clayton Utz, BAT's lawyers in Australia, advising BAT to destroy certain records. The Victorian Supreme Court ruled that ad hoc destruction of records for the purpose of hampering a case against a company, even though the action had not yet been commenced, was a criminal action.

When BAT appealed the decision, they established that the destruction of records was neither in contempt of the court nor a deliberate attempt to pervert the course of justice by convincing the court that the purpose of advice from Clayton Utz was to use records storage space more economically.

In *R v Ensbey; ex parte A-G (Qld)*, the Supreme Court of Queensland Court of Appeal found that if a person believes that a record may be needed as evidence in a possible future legal proceeding, they cannot legally destroy the record.

The implications of the rulings for Commonwealth agencies

These cases signal a change in judicial consideration of records disposal. In the past, destruction has been permitted if there were no current legal proceedings, but it has become important for agencies to consider the potential legal cases associated with the records that they generate, and whether their destruction might pervert the course of justice.

The *Archives Act 1983* ensures that Commonwealth records are not destroyed without the permission of the National Archives, in the form of a disposal authority. Disposal authorities are based on a thorough analysis of the legal delegates, business activities and stakeholder requirements **at the time of issue**. Records destruction under disposal authorities are systematic rather than ad hoc, and disposal authorities take into consideration all foreseeable uses of the records.

As long as there is no change in context, it is unlikely that records destroyed pursuant to a valid disposal authority would be considered to be destroyed with the intention of spoiling a litigant's case. Agencies are advised, however, to maintain

records in an accessible form if it is reasonable to believe they may be required for judicial proceedings. A valid disposal authority does not exempt Commonwealth agencies from this obligation. If there are any questions, agencies should seek legal advice.

Further resources

British American Tobacco Australia Services Ltd v Roxanne Joy Cowell (as representing the estate of Rolah Ann McCabe deceased) (2002 VSCA 197), published on the [Australasian Legal Information Institute website](#).

Rolah Ann McCabe v British American Tobacco Australia Services Ltd (2002 VSC 172), published on the [Australasian Legal Information Institute website](#).

R v Ensbey; ex parte A-G (Qld) (2004 QCA 335), published on the [Australasian Legal Information Institute website](#).

RECORDS IN EVIDENCE (1998)

Acknowledgments

Records in Evidence (1998) was produced by the National Archives of Australia in cooperation with the Attorney-General's Department, the Office of Government Information Technology and the Tasmanian Department of Premier and Cabinet, Information Strategy Unit.

The Archives would like to acknowledge the contributions of Greg O'Shea (National Archives of Australia), Peter Meibusch (Attorney-General's Department), and Christabel Wright (Office of Government Information Technology) and Simon Roberts (DP&C, ISU).

THE EVIDENCE ACT 1995 (CTH)

The changes to evidence law contained in the Commonwealth *Evidence Act 1995* mark a significant turning point in the admissibility of evidence presented before Federal courts. This legislation contains significant changes to rules of evidence making it easier for records created in electronic systems to be admitted in evidence.

The National Archives has produced this document to assist agencies in assessing the implications of the legislation to ensure the admissibility and reliability of their records, particularly electronic records.

The *Evidence Act* relaxes and, in some cases, removes restrictions on evidence that can be admitted in proceedings (particularly civil proceedings), so that a greater range of relevant evidence is available to courts for fact finding purposes. The Act contains major reforms to the laws of evidence, in both civil and criminal proceedings, and the manner in which evidence is given.

In relation to documentary evidence, the reforms made by the Act include:

- a narrower hearsay rule and wider exceptions to that rule, providing for greater admissibility of hearsay evidence
- abolition of the original document rule, replacing it with simple means of giving evidence of the contents of documents, including documents held in computer and other non-paper forms
- provisions for easier proof of, and presumptions about, business and official records, and the use of mail, fax and other means of communication
- pre-trial procedures enabling litigants to test the weight of documentary evidence that might be given in proceedings

With a greater range of evidence admissible in many Australian courts, agencies must consider the quality of evidence available in a proceeding and whether that evidence is likely to persuade a court to accept the Commonwealth's version of the facts.

It is essential for public sector managers to ensure that their accountability practices and recordkeeping systems can stand up to the scrutiny of the courts, parliament, the Ombudsman and relevant auditors. Individual citizens are important

stakeholders in this process and have rights of redress through a range of institutions, and access to records and other information through the [Freedom of Information Act 1982](#) and the [Archives Act 1983](#).

With the new integrated records management systems now available for use by Commonwealth agencies, many organisations have the opportunity to re-examine their recordkeeping strategies and practices. It is particularly important that electronic systems are able to stand up to detailed scrutiny.

THE LEGAL ENVIRONMENT

Evidence introduced into legal proceedings in Australia is subject to the common law and a range of Commonwealth, state and territory legislation. Where it is necessary to use agency records in court proceedings, different laws of evidence apply depending on the court and the type of document.

If the proceeding is in a federal court (eg the Federal Court of Australia or the Family Court) or an ACT court, the evidence law which applies is set out in the Commonwealth *Evidence Act*. In other courts, except NSW, the evidence law of the relevant state or territory applies. This is largely common law, as varied by statute in the particular state or territory. The NSW Evidence Act is mirror legislation to the Commonwealth Evidence Act and consequently has the same admissibility requirements.

In addition, some provisions of the Commonwealth Evidence Act also apply in state and territory court proceedings in relation to some documents (eg a document signed or sealed in an official capacity, a government gazette or other officially printed document, a document published by the Australian Statistician, and a 'public document' or a 'Commonwealth record' within the meaning of the *Evidence Act*).

In addition, specific federal and state laws, policies, and standards may apply to particular records. For example, the *Archives Act 1983*, *Freedom of Information Act 1982* and *Privacy Act 1988*.

THE RULES OF EVIDENCE

The rules of evidence govern how a party goes about proving its case.

Courts must determine the truth about what has happened. Each party has the opportunity to persuade the court that its version of the facts is correct. The rules of evidence are intended to assist the court in its task and, in some respects, to reflect community standards (eg in relation to police questioning).

Parties seek to persuade the court of a fact by producing evidence. In doing so, a party must address three questions:

- how to adduce (ie put to the court) evidence of the fact
- whether the court will permit the evidence to be given (ie whether it is admissible)
- the weight of the evidence (ie how much importance the court will give to it in reaching its decision)

The rules of evidence are mainly concerned with the first two issues. They specify:

- how information, in the form of 'evidence', is given or presented to a court
- whether that information can be given or led in a proceeding. If it cannot, the evidence is said to be 'inadmissible'.

The new rules of evidence of most relevance to documents held by Commonwealth agencies make it easier to adduce evidence and remove restrictions on inadmissibility, especially in relation to documents. However, this does not affect the need to ensure that the evidence available is of high quality. Assessment of the quality of evidence, and therefore of the weight to be given to it, is a matter for the court in each case.

THE DISTINCTION BETWEEN ADMISSIBILITY AND WEIGHT OF EVIDENCE

Although evidence of information about a particular fact may be admissible, the court will not necessarily believe or act on that evidence.

If the information about a fact is the direct observation of a witness, the court may simply disbelieve the witness. This may occur for a number of reasons. For example, it may have been a long time since the events in question, the witness may give confused testimony, or may have some physical incapacity (eg poor eyesight) or have some personal inclination or motivation that causes the court to disbelieve their evidence (eg it may be shown that the witness is inclined to lie, or bears ill-will against someone connected with the proceedings).

More usually, evidence of information given in court will not be 'direct observation' evidence. Instead it will be evidence that suggests, or from which it can be inferred, that a particular fact occurred.

Example: John's email

The Commonwealth needs to prove that John, a public servant, sent a particular email at a specific time.

There is no 'direct observation' evidence of that fact, that is, no one who can testify that they saw John write the email and then press the send icon on his computer. But there may be other records that courts will consider as evidence that John sent the email at that specific time.

For example, there may be records showing that the email originated from:

- a computer which John was logged into, or
- John's email account.

Even if the evidence is admissible and is admitted, whether or not the court will accept the evidence as proof that John sent the email may depend upon other evidence before the court, including evidence that may be led by another party.

For example, the Commonwealth's evidence of a record of John's computer log on may need to be accompanied by evidence that John's password was personal to him and, in the case of a network computer system, that no one but John could log on to his personal email account.

However, the court would not necessarily infer that John was the person who sent

the email if there was other evidence before the court that, for example, personal passwords in John's work area were generally known and occasionally used by others to log on to email accounts, or if email messages logged into the agency's recordkeeping system could be manipulated after the fact.

HOW EVIDENCE OF INFORMATION IN A DOCUMENT CAN BE GIVEN

Under the Commonwealth and NSW Evidence Acts

The rules of evidence under the new Commonwealth and NSW Evidence Acts apply to a document that is a 'record of information'. The term 'document' is defined in the dictionary to the Evidence Acts to mean any record of information, and includes:

- anything on which there is writing
- anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them
- anything from which sounds, images or writings can be reproduced with or without the aid of anything else
- a map, plan, drawing or photograph.

The rules apply to an ordinary document in writing, documents written in braille or shorthand and, importantly for modern records management systems, a 'record of information' that is contained on a computer (or audio or video) tape or disk, or optical laser disks.

The Commonwealth and NSW Evidence Acts abolish (in courts where they apply) the common law 'original document rule', which requires the production of the original document in writing, and permit evidence of the contents of a document to be given in one of a number of alternate ways. These ways include tendering:

- the original document
- a copy of the document produced by a device (such as a photocopier or a word processor) that reproduces the contents of documents
- a transcript of a document recording words (such as an audio tape or shorthand notes)
- a printout of computer output or a document reproducing the contents of an optical laser disk
- a business record being an extract, summary or copy of the document.

Other ways may be used to give evidence of official documents, and documents that are unavailable to a party in the proceedings, for example, where they have been lost or destroyed.

While the 'original document rule' has been abolished, it is still necessary for parties to authenticate evidence of the contents of documents tendered in one of these ways. For example, in relation to a document in writing that is signed, it remains

necessary to lead evidence (if the point is contested) that the signature appearing on the document is the signature of the person who has purported to sign it. In the case of computer records, it is necessary to give evidence that the computer output is what it purports to be.

While several provisions of the Acts facilitate this authentication process, the Acts also set out procedures under which litigants may test the authenticity of evidence of the contents of documents led under one of the alternate ways in a proceeding. Usually, these procedures would be used by a party against whom evidence of the contents of a document is, or might be, led in a proceeding.

The procedures, which can be set in motion before the hearing of a proceeding, may result in the making of court orders against the party leading evidence of the contents of the document, including an order that:

- the original document be produced
- a party be permitted to examine, test or copy a document
- a person concerned in a recordkeeping system be called to give evidence
- in the case of a computer or similar document, that a party be permitted to examine and test the way in which the document was produced or has been kept.

The ultimate sanction for failure to comply with such an order is that the evidence of the contents of the document is not to be admitted in the proceeding.

In other states, Northern Territory and Norfolk Island courts

In these courts, the common law with some statutory modification applies. At common law, the 'original document rule' requires that evidence of the contents of a document can only be given by tender of the original document. The rule is subject to a number of exceptions, as well as some statutory abridgment, mostly in the relevant state or territory Evidence Acts. Exceptions at common law include where:

- a party has served on another party in the proceeding a notice to produce the document, with failure to comply laying the foundation for other evidence of the document
- a stranger who has been served with a subpoena to produce the document lawfully refuses to produce it (eg on the basis of privilege)
- the document has been lost or destroyed
- production of the document is impossible (eg where it is writing on a physical object, for example, on a wall or a tombstone)
- in the case of a public document, where production would be inconvenient.

Statutory abridgment of the rule permits certain types of evidence (eg photographic reproductions, copies of entries in books of accounts or bankers books to be led as evidence of the contents of a document).

HOW EVIDENCE OF INFORMATION IN A DOCUMENT MAY BECOME INADMISSIBLE

A separate issue from how evidence of information in a document can be given, is whether the court will permit the evidence to be given (whether the evidence is admissible in the proceeding before the court).

Whether the evidence is admissible depends, initially, on whether it is relevant to a fact in issue in the proceeding. If relevant, evidence may nevertheless be inadmissible if it is excluded by a rule that provides for the exclusion of particular kinds of evidence (for example, the rule against hearsay evidence, the 'similar fact evidence' rule, and the rule against opinion evidence).

The most important exclusionary rule in relation to documents is the hearsay rule. The hearsay rule applies when evidence of what is contained in a document is being used to prove some fact asserted in it.

Example: John's email

Returning to our example of the Commonwealth trying to prove that John sent a particular email at a particular time, John offers to produce his diary to the court that contains a note that he says he wrote at the time of sending the email.

However, the hearsay rule will apply to the use of the note to prove that he sent the email at a particular time.

Unless an exception to the rule applies, evidence of the note will be inadmissible to prove that John sent the email at a specific time, because the note may have been written at a time other than the time of the email.

The scope of the hearsay rule, and the exceptions to it, differ depending on whether or not the Commonwealth or New South Wales Evidence Act applies to the proceedings.

The hearsay rule under the Commonwealth and NSW Evidence Acts

The hearsay rule under these Acts applies to any statement made by a person other than while giving evidence that is led or given to prove the existence of a fact the person intended to assert by the statement.

Under the Acts the rule applies to every statement made by a person in a document, provided evidence of the statement is led to prove the existence of such a fact. In relation to electronic records, the rule does not apply to machine produced information as such information is not a 'statement made by a person'.

When the hearsay rule applies, exceptions to the rule exist for:

- evidence admitted for a non-hearsay purpose (where the statement is relevant for a purpose other than to prove the existence of a fact that the person intended to assert, for example, where the fact that the statement was made is relevant). In such a case evidence of the statement can also be used as evidence of what is asserted by the statement

- first-hand hearsay, the scope of the exceptions depending upon whether the proceeding is civil or criminal and whether the person who made the statement is available or not to give evidence
- some categories of more remote hearsay (that is, where the evidence is not necessarily first-hand hearsay), such as some statements in business records, some tags and labels or writing attached to, or placed on, objects (including documents) in the course of business
- an admission made by a person who is or becomes a party to the proceeding.

Some procedural safeguards apply for some of these categories of hearsay evidence. For example, notice provisions where the person who made a statement admitted under one of the exceptions for first-hand hearsay is not to be called to give evidence in the proceeding, and other procedures under which a party may be required to call as a witness the person who made the statement.

The hearsay rule in other states, Northern Territory and Norfolk Island courts

The common law hearsay rule, and its exceptions at common law and under relevant statutory provisions, apply in proceedings before these courts. *Cross on Evidence* (4th Australian edition, at paragraph 1260) states that the rule against hearsay 'has never been definitively formulated judicially' at common law but 'the following will suffice ... as a succinct statement of the rule: an assertion other than one made by a person while giving oral evidence in the proceedings is inadmissible as evidence of any fact asserted.'

The rule at common law applies equally to statements made in documents, as well as to statements made orally.

The exceptions at common law are complex and developing. While some can be grouped into defined categories (the exceptions for particular statements made by persons since deceased, statements in public documents, admissions and confessions), *Cross on Evidence* prefaces its discussion of its 'miscellaneous' category at paragraph 33790 with the remark that 'the application of the law relating to [this category] can only be explained on the footing that there are many more exceptions to the hearsay rule than is commonly supposed'.

In addition, a miscellany of statutory exceptions to the hearsay rule apply, including for statements in business records, statements in other documents, bankers books and books of accounts, and some transport documents, amongst others.

THE RULES OF EVIDENCE IN COMMONWEALTH TRIBUNALS

The admissibility rules in the Commonwealth *Evidence Act 1995*, whether evidence of information can be given in a proceeding, also apply to proceedings before 'a person or body ... that, in performing a function or exercising a power under a law of the Commonwealth, is required to apply the laws of evidence'.

The great majority of Commonwealth tribunals are not required to apply the laws of evidence. Most commonly, the statute under which the tribunal is created includes a

provision to the effect that the tribunal is not bound by the rules of evidence, but may inform itself as it thinks appropriate.

This will not necessarily mean that the rules of evidence are irrelevant to tribunal proceedings. Tribunals may, for example, have regard to what would be admissible had the proceedings been before a court, especially when the outcome of the proceeding may be subject to judicial review. In any event, a tribunal (like a court or, indeed, any person or body with decision-making functions or responsibilities) is unlikely to believe and act on records or other documents if they cannot be shown to be accurate and reliable.

COMPLIANCE WITH SUBPOENAS AND ORDERS FOR DISCOVERY

Occasionally, agencies need to comply with requirements imposed by courts to produce or disclose documents needed for legal proceedings, including proceedings in which the Commonwealth is not a party. These requirements usually arise following the issue and service of a subpoena or similar document in a proceeding, or by way of an obligation or court order.

A subpoena is a court order requiring the giving of evidence, or the production to the court of documents, or both. Discovery is the process whereby parties to court proceedings identify and disclose to each other documents that are relevant to the issues in the proceedings. Discovery only relates to disclosure of documents, and not to the giving of evidence.

In some courts, an order for discovery may be made against a person or a body who is not a party to the proceedings. Substantial obligations may be imposed upon agencies to whom a subpoena, or an order for discovery, is directed. Both processes require the agency to whom an order is directed to make a full and thorough search for relevant documents, including documents held in an electronic form.

Depending upon the circumstances, failure to comply with relevant requirements (eg to produce all documents falling within a stated description) may result in the agency being found in contempt of court.

RECORDKEEPING REQUIREMENTS

Changes to evidence legislation and the need to comply with subpoenas and discovery orders has significant implications for the management of agency records and the development and maintenance of recordkeeping systems, particularly where those systems are in electronic form. Therefore, efficient and prudent recordkeeping and information systems will ensure that records required for legal proceedings, often within tight deadlines, can be readily identified and located.

Reviewing recordkeeping practices

As government agencies make increasing use of newer technologies for recordkeeping and information management – such as electronic document management, digital imaging, electronic messaging, workflow management, electronic commerce and other electronic information systems – recordkeeping practices should be reviewed so that agencies continue to produce and capture records that are authentic, reliable and accurate for legal, audit and other purposes.

When using newer technologies agencies should take special precautions to ensure that records produced by their recordkeeping systems will be legally acceptable. Establishing the authenticity and reliability of records may depend on the accuracy of the process or system used to produce the record, the source of the information in the record, and the method and time of its preparation. Problems may arise with admissibility if appropriate procedures are not followed in creating and maintaining records.

The primary purpose for keeping records is to support the business of the agency. Records are also used to account for agency actions to government and the community. Decisions about the creation, maintenance and use of records and their management systems must be made in the context of laws and regulations under which the agency operates. They must also conform with established recordkeeping, data processing, auditing and related professional practices and standards, and with applicable administrative rules and policies. This process needs to include an assessment of the costs and benefits associated with current recordkeeping and information systems, and any refinements which may be required to improve them.

Establishing a recordkeeping and systems management regime

Meeting evidentiary requirements in a complex, changing technological environment is a challenging undertaking that requires cooperation and coordination within agencies. To ensure that records are authentic, accurate and reliable, an agency must maintain a comprehensive, credible information and recordkeeping regime. This requires formal organisational arrangements and clarification of the responsibilities of records management. These should be stated in policies and guidelines relating to records management and recordkeeping systems. Agencies must ensure the appropriate numbers, quality and proficiency of staff responsible for stewardship of an agency's information assets, including records. With the growth of decentralised computing and distributed electronic information systems, each user must assume responsibility for producing and maintaining authentic, accurate and reliable records within organisational recordkeeping systems supported by rules, procedures and training to ensure an understanding of individual requirements.

In summary, corporate managers, records managers, information managers, administrative support staff, and information technology professionals all need to be involved in the recordkeeping process to ensure that records are produced by electronic information systems and that they are authentic, accurate and reliable.

For the establishment of an appropriate recordkeeping regime, agencies need to:

- undertake a strategic analysis of corporate information and recordkeeping requirements
- produce written policies and procedures to define normal operations for development, maintenance, and use of electronic information and recordkeeping systems
- provide training and support to help ensure that policies and procedures are understood and implemented by staff

- ensure recordkeeping requirements are built into electronic information systems and to enable the capture of appropriate records
- ensure that records in electronic recordkeeping systems are only disposed of in accordance with authorisation provided by the National Archives of Australia.

In addition to undertaking steps to ensure appropriate recordkeeping regimes are established, agencies also need to ensure that an appropriate systems management regime is in place to support the business of the organisation and the authenticity of records. Agencies need to:

- develop adequate system controls to ensure the quality and reliability of the records created and maintained by electronic systems
- develop and implement system audit trails to detect who had access to the system, whether staff followed certain procedures, or whether fraud or unauthorised acts occurred or might be suspected in the system
- conduct routine tests of system performance (Automated information systems rely on system edits and routine testing to verify the accuracy and validity of data. System edits define the parameters of online system processing. Tests of system performance, conducted on a routine basis, provide necessary oversight to verify the integrity of a system.)
- routinely test and document the reliability of hardware and software using a plan developed with the advice of the manufacturer, retaining all documentation related to hardware and software procurement, installation, and maintenance, and maintaining operation logs and running schedules to document the reliability of system operation and performance
- provide adequate security by developing routines that limit access and update privileges to the appropriate people and prevent unauthorised modification of data
- establish controls for accuracy and timeliness of input and output through systematic procedures for data entry
- reach agreement on issues relating to data exchange including provisions for the structure and format of data into transactions sets, the standards for communication, and security procedures
- create and maintain comprehensive system documentation on all aspects of system design, implementation, maintenance, and oversight
- retain documentation describing how a system operated and describing the purpose, structure and origins of data for at least as long as any records produced by a system are retained.
- Agencies using digital imaging technology should implement the following measures as part of the normal operation of the imaging system:
 - mechanisms for verifying that the system accurately reproduces originals based on recognised industry standards and procedures
 - use of standard compression and decompression algorithms

- thorough description of any image enhancement techniques in the system's documentation
- stringent security provisions to prevent alteration of digital images
- use of Write-Once-Read-Many (WORM) optical media for imaging applications.

FURTHER ADVICE

The technical nature of digital recordkeeping environments requires standards to ensure inter-operability, best practice and the creation of full and accurate records, including sufficient evidential context of business activities. The National Archives of Australia endorses the use of the Australian Records Management Standard (AS ISO 15489) as the model for best practice recordkeeping. The Records Management Standard can be used as a stand alone document or in conjunction with the ISO 9000 suite relating to Quality Systems. The Records Management Standard is available for purchase through your local Standards Australia office.

The National Archives of Australia website includes a number of publications about recordkeeping, particularly in the Australian Government environment. [Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records](#), May 2004 and [General Disposal Authority for Source Records that have been Copied, Converted or Migrated](#), February 2003 are of particular relevance to the matters discussed in Records in Evidence.