PUBLIC RECORD OFFICE VICTORIA

Public Record Office Victoria
Advice to Victorian Agencies
July 2003, Version 2.0

Advice 10

PROS 99/007 has been replaced by *PROS 19/05 Create, Capture and Control Standard*.

Public offices that have implemented and configured a system in accordance with PROS 99/007 requirements — namely VERS Version 2 VEO creation — can continue to refer to the standard and its associated specifications and advices for the life of the system.

Public Record Office Victoria will continue to:

- Accept digital record transfers in VERS Version 2 VEO format.
- Test current vendor products against the PROS 99/007 requirements up until 30 June 2021. (After this time, PROV will only test vendor VEO creation validity for VERS Version 3 VEOs against PROS 19/05 requirements).

Vendors may continue to self-certify versions of their current products against PROS 99/007 up until 30 June 2025.

Last updated: 25 March 2020

Public Record Office Victoria
Advice to Victorian Agencies
July 2003, Version 2.0

Advice 10

Advice on
VERS System Requirements for
Preserving Electronic Records
PROS 99/007 (Version 2) Specification 1

State Government Victoria

Department for Victorian Communities

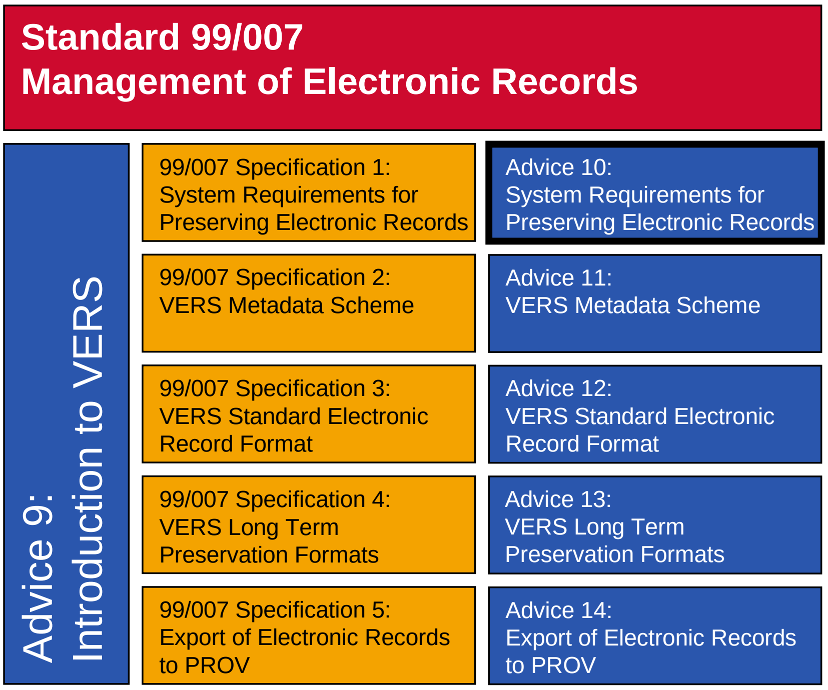
Further copies of this document can be obtained from the PROV Web site
http://www.prov.vic.gov.au/

The State of Victoria gives no warranty that the information in this version is correct or complete, error free or contains no omissions. The State of Victoria shall not be liable for any loss howsoever caused whether due to negligence or otherwise arising from the use of this Advice.

Version	Version Date	Details
2.0	31 Jul 03	Released

The Victorian Electronic Records Strategy (VERS)

This document is a guide to *PROS 99/007 Specification: System Requirements for Preserving Electronic Records*. The relationship between the VERS Standard, the Specifications that support this Standard, and the Introduction and Advices that explain VERS is shown below.



Standard 99/007
Management of Electronic Records

Advice 9:
Introduction to VERS

99/007 Specification 1:
System Requirements for
Preserving Electronic Records

Advice 10:
System Requirements for
Preserving Electronic Records

99/007 Specification 2:
VERS Metadata Scheme

Advice 11:
VERS Metadata Scheme

99/007 Specification 3:
VERS Standard Electronic
Record Format

Advice 12:
VERS Standard Electronic
Record Format

99/007 Specification 4:
VERS Long Term
Preservation Formats

Advice 13:
VERS Long Term
Preservation Formats

99/007 Specification 5:
Export of Electronic Records
to PROV

Advice 14:
Export of Electronic Records
to PROV

These documents have the following purposes:

- *Management of Electronic Records*. This document is the Standard itself and is primarily concerned with conformance. The technical requirements of the Standard are contained in five Specifications.
- *Introduction to VERS.* This document provides background information on the goals and the VERS approach to preservation. Nothing in this document imposes any requirements on agencies.
- *Specifications.* These five documents provide the technical requirements that support the Standard. Agencies *must* conform to the mandatory requirements of the specifications, *must* conform to the conditional requirements of the specifications if the appropriate conditions are satisfied, and *may* conform to the optional requirements. Some optional requirements are strongly recommended and these are noted as such.

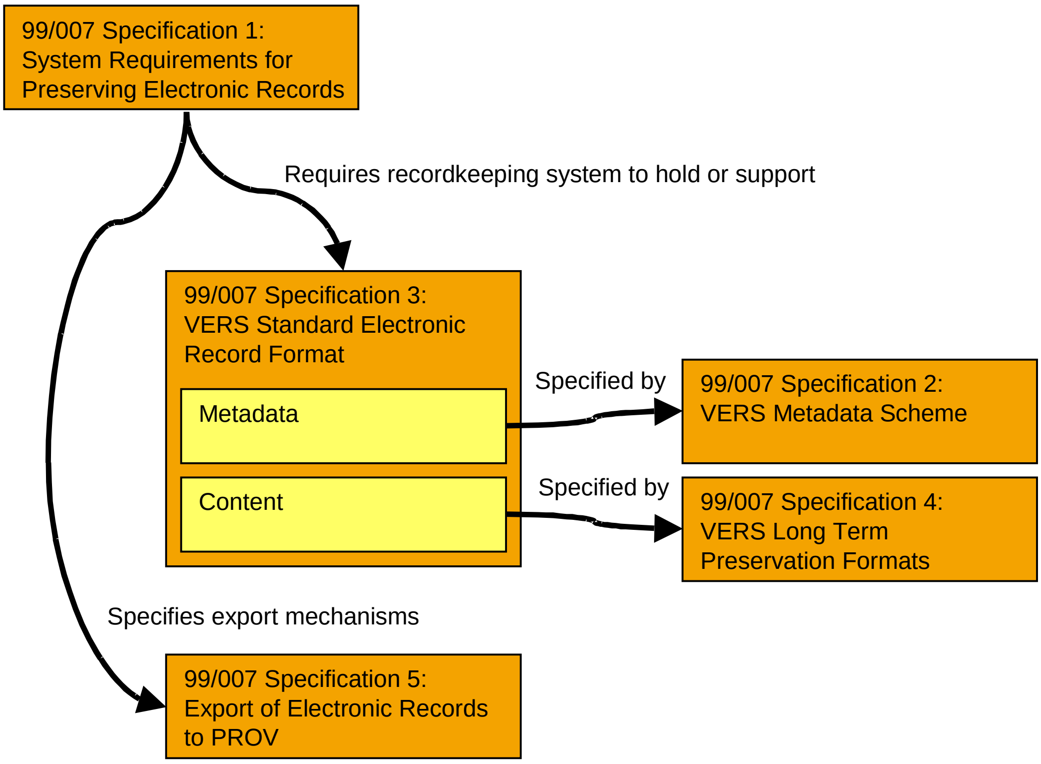
  The five Specifications are:

  - *Specification 1: System Requirements for Preserving Electronic Records.* This document specifies the overall functions that a recordkeeping system must perform to preserve electronic records for a substantial period.
  - *Specification 2: VERS Metadata Scheme.* This document specifies the metadata that a recordkeeping system must hold to conform to VERS.
  - *Specification 3: VERS Standard Electronic Record Format*. This document contains the technical definition of the VERS Encapsulated Object (VEO) format; the mandatory long-term format for records.
  - *Specification 4: VERS Long Term Preservation Formats.* This document lists the data formats that PROV accepts as suitable for representing documents for a significant period.

- *Specification 5: Export of Electronic Records to PROV.* This document lists the approved media and mechanisms by which PROV will accept an export of electronic records.

- *Advices.* These six documents provide background information, explanatory material, and examples in support of the Standard and associated Specifications. None of the information in the Advices imposes any requirement on agencies.

Relationship between Specifications. A second view of the relationship between the five Specifications is shown in the following diagram:



Specification 1 (System Requirements for Preserving Electronic Records) details the overall requirements on a recordkeeping system for preserving electronic records over a significant period. Amongst other requirements, the recordkeeping system must be capable of exporting the records in a standardised format.

The overall features of this standardised format are defined in *Specification 3 (VERS Standard Electronic Record Format)*, but some details are defined in two other Specifications. *Specification 2 (VERS Metadata Scheme)* defines the meaning and allowed values of the metadata that appears in a record. *Specification 4 (VERS Long Term Preservation Formats)* defines the formats in which the record content must be expressed.

Specification 5 (Export of Electronic Records to PROV) defines the mechanisms by which records are exported to PROV.

Relation to Version 1 of this Standard. This version of the VERS Standard completely replaces Version 1 of the Standard. Version 2 is identical in its base requirements, but makes those requirements clearer and more explicit. It also contains a number of conditional and optional extensions to Version 1.

Table of Contents

1 Introduction

Information in this guide is purely informative. Nothing in this guide imposes any requirements on a VERS compliant implementation; requirements are only imposed by the associated Specifications.

This guide provides information about implementation of the requirements in *PROS 99/007 Specification 1: System Requirements for Preserving Electronic Records.*

PROS 99/007 Specification 1 contains the functions that a recordkeeping system must support if it is to preserve records for a significant period.

The Specification is mandatory for any system that holds permanent electronic records; that is, those records judged to be of permanent value to the State of Victoria. Permanent records are specified in an agency's disposal authority. It is optional but strongly recommended that systems that hold long-term temporary records for a significant period should also conform to the Specification. A significant period is one where the records have a life longer than the expected life of:

- the system holding the records, or
- the organisation holding the records.

In this Specification, a recordkeeping system is considered to be the entire system holding records. The system may include business processes, one or more software applications that manage records (which may or may not be named a 'recordkeeping system'), and any supporting computer systems (such as storage networks and servers). In consequence, the functions required in this Specification may be the responsibility of an agency, the vendor of a recordkeeping application, or the vendor of a supporting system.

The Specification covers only those functions necessary to support long-term preservation using VERS. A complete recordkeeping system must support many other functions as well. The reader is referred to the referenced standards and recommendations below for guidance on these other functions.

There are many different ways in which these functions could be implemented, depending on the applications from which records are captured and the computer technology chosen.

2 Recordkeeping Functional Specifications

Specification 1 is only concerned with those recordkeeping functions that support long-term preservation of electronic records. A recordkeeping system has to satisfy many other requirements in order to be useable. Several organisations have published general requirements for recordkeeping systems. These include:

- Model Requirements for the Management of Electronic Records (MoReq), European Commission, 2001, http://www.cornwell.co.uk/moreq (visited 26 February 2003).
- Functional requirements for Electronic Records Management Systems, Public Record Office (UK), 2002, http://www.pro.gov.uk/recordsmanagement/erecords/2002reqs/default.htm (visited 10 February 2003).

- Design Criteria Standard for Electronic Records Management Software Applications, DoD 5015.2-STD, (US) Defense Information Systems Agency, June 2002, http://jitc.fhu.disa.mil/recmgt/standards.htm (visited 10 February 2003).

The PROV does not specifically recommend any of these function specifications. Agencies should carefully consider their suitability for their purposes. In particular, it should be noted that none of these functional specifications are built around a VERS solution.

3 Specific Requirements

In this section the text in **bold** is taken verbatim from Specification 1. The plain text (not in bold) enlarges and explains the requirement. However, this explanatory material is not mandatory. In particular, although we discuss how an agency might obtain conformance to the requirement, other methods of conformance are possible.

3.1 Record authenticity (Specification 1, section 2.1)

The recordkeeping system must be capable of demonstrating that a record is authentic; that is, the system must prove that the content is what it appears to be, who created it, and when it was created.

The recordkeeping system must record the identity of the user creating the record and the time it was created. This information must not be forgeable or capable of being altered by either users or system administrators.

Authenticity is derived from the business processes associated with the creation of the record, in particular where the record is captured as part of the normal process of doing business. The recordkeeping system demonstrates authenticity by means of metadata captured when the record is registered. From a technology perspective, demonstrating authenticity is dependent upon the accuracy of the metadata being captured and whether this metadata can be shown to be unaltered.

The system must capture:

- The identity of the user that registered the record. The identity may be captured by recording the account used to register the record. The system should also include information associated with the account (such as the user's name) where this is known by the system.

  VERS does not require the recordkeeping system to prove that a specific user was operating the account when the record was created. In particular, VERS does not require any special technology (such as biometrics, digital signatures, or smartcards) to demonstrate who registered a record, though, obviously, such technology can result in a stronger proof of authenticity.
- The time the record was registered into the recordkeeping system. This time must be obtained from a source that cannot be altered by the user registering the record.

It is expected that responsibility for demonstrating conformance to these functions will lie with the vendor of the recordkeeping application.

Conformance is demonstrated by showing that the system captures the identity of the user registering the record and the time the record was registered. The time must be from a source not under the control of the user registering the record.

Ensuring that the metadata proving authenticity is unchanged after capture is an aspect of record integrity and is discussed in the next section.

3.2 Record integrity (Specification 1, section 2.2)

The recordkeeping system must be capable of proving that a record has integrity; that is, that any alterations to the record are authorised and documented.

Integrity is essentially about proof and the best way to consider this requirement is to consider how you would prove in a court of law that a record was unaltered from its creation, or that any alterations are documented.

A record can retain integrity despite being altered, provided the alteration is performed by an authorised person and the alteration is documented.

There are a number of ways of demonstrating record integrity.

One way of demonstrating integrity is by means of the VERS standard record format which is specified in *PROS 99/007 Specification 3: VERS Standard Electronic Record Format.* In this format, integrity is shown by the use of one or more digital signatures. If any modifications are carried out on the record, the integrity is shown by preserving the original record and layering the alterations around it (using the ModifiedVEO object in a Version 2 system, or an onion record in a Version 1 system). When the alteration occurred, and who performed the alteration, is recorded in the Management History.

If the integrity of a record is not protected using the VERS standard format it will be necessary to show that the recordkeeping system acts as a vault. Conformance can be achieved by a formal statement from the recordkeeping system vendor that:

- it is not possible to alter the contents of records except through the defined recordkeeping functions. This must explicitly consider a user with special privileges bypassing the normal access functions (e.g. a records manager, or a system administrator directly accessing the underlying computer files on the file systems).
- all modifications to records are logged in sufficient detail to identify what was modified.
- it is not possible to delete or modify all or part of the audit log dealing with modifications. (A system may allow the deletion of audit log information dealing with other aspects of the system apart from modifications.) Again, this must explicitly consider a user with special privileges bypassing the normal security controls.
- it is possible to extract the audit log entries dealing with a particular record.

Protecting integrity is difficult, as complex systems may contain software bugs or undocumented access mechanisms. An agency may require an audit of the system and its design to check the integrity of the system.

Integrity must be shown over the entire life of the record; any gap in the protection of the record will impair the record’s integrity. One way of causing an integrity failure is during the export of custody from one recordkeeping system to another system. In this case the chain of integrity will require showing that it was held securely in the first recordkeeping system, that it has been held securely in the current recordkeeping system, and that it was transferred securely from the first system to its successor. The VERS standard format can be used to secure the records while they are being transferred.

Records must be protected against undocumented modification by normal users, records managers, and system administrators.

Most systems control access by normal users, but care needs to be taken in respect of users with special privileges (such as records managers and system administrators). Conformance to this point is covered in the notes to the previous point.

It must not be possible for records to be destroyed or deleted except by authorised users. All destruction or deletion of records must be recorded.

It will be necessary to show that the recordkeeping system acts as a vault and that deletion and destruction of records can only be achieved through the recordkeeping functions provided by the system and that all deletion and destruction is logged in an audit log. Conformance can be achieved by a formal statement from the recordkeeping system vendor that:

- it is not possible to destroy or delete records except through the defined recordkeeping functions. This must explicitly consider a user with special privileges bypassing the normal access functions (e.g. a system administrator directly accessing the underlying computer files on the file systems). Particular care must be taken that system administrators or records managers cannot simply delete the underlying computer files that contain the records.
- every deletion of records is logged in sufficient detail to determine when the record was deleted and who performed the deletion.
- it is not possible to delete or modify all or part of the audit log dealing with deletions. (A system may allow the deletion of audit log information dealing with other aspects of the system apart from deletions.) Again, this must explicitly consider a user with special privileges bypassing the normal security controls.
- it is possible to extract the audit log entries dealing with a particular record.

Protecting integrity is difficult, as complex systems may contain software bugs or undocumented access mechanisms. An agency may require an audit of the system and its design to check the integrity of the system.

The system must be capable of verifying whether a record has retained its integrity.

Verification may be achieved by verifying the digital signatures, or by extracting audit information from the logs if the records are not digitally signed.

If the verification is carried out by digital signatures the validity of the root certificate must be checked. The check may be against a copy of the certificate kept in an secure portion of the archive, or by comparing various copies of the root certificate used to sign records at roughly the same time.[1]

If the verification is carried out by an examination of the audit information, there is no requirement for the system to analyse the audit log and to automatically determine of integrity. The system may simply extract the entries in the audit log that refer to modifications to the record and present these in a report for inspection by a user.

Verification must be capable of being carried out upon demand by users accessing records. However, it is not necessary to validate a record each time the record is accessed.

Conformance to this point is achieved by the recordkeeping system vendor demonstrating verification of integrity upon demand by users.

The system must be capable of auditing the integrity of a random sample of records.

[1] See Advice 12, which relates to *PROS 99/007 Specification 3: VERS Standard Electronic Record Format*, for a description of this approach to verification.

This allows the owners of a recordkeeping system to periodically audit the integrity of the record collection and may pick up systematic corruption earlier than with more ad hoc checking.

Conformance to this point is achieved by the recordkeeping system vendor demonstrating verification of integrity of a random sample of records.

Any failure to verify a record must be logged and immediately brought to the attention of the system administrator.

Failure to verify a signature may indicate an attempt to forge or alter records. This requirement can only be achieved if the system can automatically verify a record. If a failure of integrity can only be determined by a manual examination of an audit log, the system cannot automatically detect a failure and hence cannot log the event or bring it to the attention of an administrator.

Conformance to this point is achieved by the recordkeeping system vendor demonstrating logging and alarm raising after a failure to verify a record.

3.3 Document conversion (Specification1, section 2.3)

Record content must be converted to one of the standard long-term preservation formats specified in *PROS 99/007 Specification 4: VERS Long Term Preservation Formats*.

Record content may be converted upon:

- export from a recordkeeping system
- import into a recordkeeping system
- registration into a recordkeeping system.

Conversion upon registration is preferred, as problems with the conversion are more likely to be detectable and correctable. Typical problems with late conversion can include:

- password-protected files which can no longer be opened
- inaccurate conversion due to ‘upgrading’ of software (which may include plugins). Inaccurate conversions include changes in appearance of the content (e.g. repagination, changes in fonts, etc.)
- failure to convert due to lack of appropriate software (which may include plugins).

For any content which cannot be converted to a standard long-term preservation format, the agency must confer with PROV to determine an appropriate archivable format. The standard long-term preservation formats are given in *PROS 99/007 Specification 4: VERS Long Term Preservation Formats.*

An agency may elect to capture record content in other formats *in addition* to the standard long-term preservation formats.

Conformance to this point is achieved by the recordkeeping system vendor demonstrating *accurate* conversion of record content for all the types of source format handled by the system.

3.4 Metadata capture (Specification 1, section 2.4)

A recordkeeping system must capture or generate the mandatory metadata specified in *PROS 99/007 Specification 2: VERS Metadata Scheme*. It must also capture the conditional metadata in Specification 2 if the relevant condition applies.

Capturing the optional metadata will improve the quality of the record or folder and it is expected that all recordkeeping systems would capture some of the optional metadata.

Conditional metadata is metadata that is mandatory in certain circumstances. Conditional elements occur in the following cases:

- A mandatory subelement of an optional element. An example is Relation Type (M44), which is conditional because it is a mandatory subelement of the optional element Relation (M42). In other words, Relation Type must be present when a Relation is present.
- Elements which are mandatory in Version 2, but do not exist or are optional in Version 1. An example of this is Lock Signature Block (M152).

Conformance to this point is achieved by the recordkeeping system vendor demonstrating that:

- the mandatory metadata can be captured and stored, or can be generated upon export
- any conditional metadata necessary can be captured and stored
- any optional metadata that the system states it can support can be captured and stored.

An agency may elect to capture additional metadata not specified in the VERS standard for storage in the record. If additional metadata is to be captured, it is recommended that the agency confer with PROV about the best approach to extending the standard record format to accommodate the additional metadata. This will assist in maximising interoperability of metadata between agencies.

An agency should conduct an analysis to ensure that the total cost of metadata capture is minimised while maximising the accuracy of information captured. As far as possible, metadata should be automatically captured from the computer system, application, or other records, and not be entered manually. However, attention should be paid to the up-front cost of software development work required to automatically capture metadata and the on-going cost of maintaining the resulting system. Obviously, the cost effectiveness will vary depending on the application, the technology used to implement the application, and the importance of the records produced.

The record capture system must be able to limit the metadata entered into a metadata element to those values specified in *PROS 99/007 Specification 2: VERS Metadata Scheme*.

This could be done using data validation techniques, pick lists and/or thesauri and the automatic capture of date and time information from the system. The cost of creating and maintaining the information used by these techniques must be analysed. Care should be taken to ensure that the system of controlling metadata is not so rigid that it prevents users from accurately describing the record.

Conformance to this point is achieved by the recordkeeping system vendor demonstrating that it is possible to limit the values captured for those elements to those specified in *PROS 99/007 Specification 2: VERS Metadata Scheme.*

3.5 Modifying information associated with records and folders (Specification1, section 2.5)

It must be possible to modify the information associated with electronic records or folders without compromising the integrity of the record or folder.

Types of modifications that may supported include:

- modifying the metadata associated with the record or folder
- adding or deleting the documents associated with a record
- modifying the metadata associated with a document
- adding or deleting encodings associated with a document
- modifying the metadata associated with a encoding.

The VERS standard electronic record format supports modification of a record. Systems that support Version 1 of this Standard can only support modifying, adding, or deleting metadata associated with the record (this is referred to as onioning). Systems that support Version 2 of this Standard additionally allow the modification of documents and encodings and the modification of folders.

Modifications of records and folders using these two VERS mechanisms does not compromise the integrity of the records or folders as the original records/folders and associated digital signatures are retained and can be verified at any time.

Conformance to this point is achieved by the recordkeeping system vendor demonstrating that it is possible to modify the metadata associated with a record. In addition, if Version 2 of this Standard is supported, the system should be capable of modifying the documents associated with a record.

3.6 Documenting the history of records and folders (Specification 1, section 2.6)

The system must be capable of recording all events that affect records and folders.

Events that *must* be capable of being recorded include:

- creation (registration) of records
- import of records into the system
- any modifications that affect the content of records (for example addition, deletion or modification of content)
- any modifications that affect the metadata of a record (for example changing the description of a record)
- changes in the classification of a folder or refiling of a record
- sentencing and disposal/destruction of folders or records
- export (transfer) of records from the system.

Events that are optional but *should* be capable of being recorded include:

- any preservation actions on a record, such as migration, conversion to another format, or refreshing

- any changes in policies that affect records or folders (e.g. changes in disposal or access control policies)
- any decisions taken about records or folders, even if they do not result in a change (e.g. the result of a disposal review even if the decision is to keep the records or folders).

An audit trail must be maintained even if the records are protected by a digital signature, as the signature only protects the integrity of the record, while the audit log provides evidence if the record is destroyed. In systems where the records are not protected by a digital signature the audit log also provides the evidence of integrity.

The audit trail may be destroyed once the record has been disposed of (by destruction or transfer), but the fate of the record must be documented. This documentation will include the officer authorising the disposal, when the record was disposed of, and details of its fate (e.g. where the record was transferred to). This may be done at a summary level; for example, the fate of all the records in a folder may be documented in the folder history. When a recordkeeping system is decommissioned, the fate of all the records and folders held by it may be documented in a report held as a record in another recordkeeping system.

Conformance to this point is achieved by the recordkeeping system vendor demonstrating that it is possible to record the mandatory events listed above.

All accesses to records or folders must be capable of being logged.

The log will include what records or folders were retrieved, the identity of the user retrieving the records or folders, and the time of retrieval. This allows unauthorised access to records or folders to be detected.

Conformance to this point is achieved by the recordkeeping system vendor demonstrating that it is possible to log accesses.

It must not be possible for any users, records managers, or system administrators to modify the audit log without a record being made of the modification.

If an audit log can be modified without a record being kept of this modification, no trust could be placed in the audit trail. Modifications include complete or partial deletion of the audit log.

Conformance to this point is discussed in section 3.2.

3.7 Reliability (Specification 1, section 2.7)

The system must not lose records or folders once they have been registered with the recordkeeping system.

This is where it is made clear for the first time that the term ‘recordkeeping system’ encompasses more than the recordkeeping application. The complete recordkeeping system includes the computer systems on which the recordkeeping application runs (particularly the storage systems), and the policies and practices implemented by the agency (particularly concerning disaster recovery procedures). The consequence of this is that the responsibility for providing this functionality is split between the vendor of the recordkeeping application, vendors of supporting computer systems, and agencies.

Records or folders may be lost due to failure of hardware or software. Examples include:

- media failure

- failure to accurately copy a record from one location to another (e.g. when copying a record from one piece of media to another, or from one server to another)
- failure of software components
- software crashes
- disasters such as fires.

Recovery of media failure and disasters are considered in the next point. This point will cover prevention of loss due to software failure.

Note that reliability in this context is only concerned with ensuring reliable storage and handling of electronic records. It is not concerned with the reliable provision of service. While the provision of service is important, it is not an aspect of preservation.

Conformance is achieved by a formal statement from the vendor about the processes used to prevent record losses.

Typically this statement would cover the software engineering processes used to develop and maintain the application, with a particular emphasis on an analysis of events which could cause a record to be lost and the mechanisms adopted to prevent these events occurring.

Among other things, such an analysis should identify:

- all points where a record (either the content or the metadata) or a folder is copied and the original is destroyed or replaced by the copy. This includes situations where a record is modified and the original is destroyed or replaced after the modification or as part of the modification.

  It is not necessary to ensure an accurate copy operation where the copy is only used for working purposes and the original is retained. An example would be the situation where, when accessing a record, a copy is made in memory of the object on the disc; in this case the copy in memory is a working copy and will be discarded once the access is completed. However, when modifying a record, a copy is made in memory of the object on the disk. The copy is then modified, which then replaces the original on the disk. In this case, both the copy to memory and the subsequent copy to disk must be verified as accurate.
- all points where a record (either the content or the metadata) or folder is held in volatile storage where it can be lost because of a system failure. Volatile storage includes holding the record only in main memory, or holding the record in a scratch file (temporary file) that is erased or discarded when the system is sut down or restarted.
- all points where a record or folder is held in non-volatile storage, but knowledge of the record or folder is only held in volatile storage. An example of this situation is where a record is accepted by the system, but the only knowledge of the record is held in a data structure in the recordkeeping program which is lost when the program stops running.

For each point the analysis must describe how a record or folder is protected against loss at that point.

Agencies should note that several different products, produced by different vendors, may be part of the complete recordkeeping system. For example, one vendor may be responsible for the recordkeeping application itself, while another is responsible for the storage system on which the recordkeeping application runs.

Vendors are normally[2] only responsible for the portion of the system they produce; for example the vendor of a recordkeeping application would not normally be responsible for analysing an agency's storage system on which the application runs.

Records or folders must not be lost due to catastrophic failure of the system, media failure, or physical disaster (e.g. fire).

The main mechanism for handling a catastrophic failure or physical disaster is the production of copies of records and folders as part of a disaster recovery regime. At least one set of these copies must be held off-site to guard against physical disaster such as a fire. On-site copies may be produced to provide faster restoration services, but these are not a replacement for off-site storage.

One aspect that must be covered in the disaster recovery plan is periodic checking that the copies can be successfully used to restore the operational system.

Conformance to this point is not primarily the responsibility of a vendor. Operation of an effective disaster recovery regime is the responsibility of the agency, although a vendor or consultant may be responsible for the initial development of the regime.

Conformance is shown by the implementation of a suitable disaster recovery regime where policies and procedures are set down to ensure that records are backed up off-site. PROV may audit the agency to ensure that the disaster recovery regime is being carried out diligently and correctly.

The accuracy of any copy must be verified by ensuring that all records or folders which have not been marked for destruction have been copied, and that the contents of the records or folders have been copied accurately.

The purpose of copying records and folders is to provide a substitute for the originals should they be destroyed. Consequently, the production of a backup copy must be treated in all particulars as if the Record was being refreshed to new media. In particular, the accuracy of the copy must be checked.

Conformance can be achieved by a formal statement from the vendor responsible for the disaster recovery software that the accuracy of copies is verified.

3.8 Media refreshing (Specification 1, section 2.8)

The system must have the ability to refresh the media on which records and folders are stored.

Refreshing means copying the contents from one piece of media to another. Refreshing may involve copying the contents from one type of technology to another in order to prevent records from being left on media which can no longer be read. Alternatively, refreshing may be from one piece of media to another of the same technology; this ensures that pieces of media are replaced before they fail.

Apart from the physical process of refreshing media, refreshing involves developing procedures for the ongoing management and conversion of media, and staff training in media management.

[2] The vendor of a recordkeeping application would only be responsible for the complete system (including underlying computer systems and possibly backup and disaster recovery regimes) if the vendor was supplying a complete turnkey system, including the underlying computer systems. This situation is expected to be uncommon.

It should be realised that refreshing is a standard practice in all computing systems. For example, disk drives on servers are regularly replaced with newer units of higher capacity.

Refreshing is closely related to creating a backup of the records and folders.

The system must document the refresh (including time of refresh, the operator invoking the refresh (if any), and the identity of the media being refreshed), with the exception that it is not expected that routine refreshing by the system (e.g. by a Hierarchical Storage Management system moving files from tape to disk) would be documented.

Conformance to this point is the joint responsibility of the agency and the vendor responsible for the storage system in use.

The agency is responsible for setting up the procedures for ensuring refreshing of media.

The vendor of the storage system is responsible for the technical process of refreshing. If the storage system is the general storage infrastructure of the public agency (e.g. a storage network or file servers) the ability to refresh the media can be assumed as part of the standard infrastructure. If, however, the storage system is specific to the recordkeeping system (e.g. storage on individual CDs that are stored off-line), conformance is achieved by the recordkeeping system vendor demonstrating the refreshing of media.

The accuracy of the refresh must be verified by ensuring that all records and folders (except those which have been disposed of) have been copied, and that the contents of the records and folders have been copied accurately.

Accuracy is normally ensured by verifying the copy (i.e. checking that all records and folders have been copied and performing a bitwise comparison of the original record and the copy).

Conformance to this point is the responsibility of the vendor supplying the software performing the refresh, and is achieved by the vendor supplying a statement certifying that all refreshes are verified as accurate copies.

If records and folders are stored on removable media (e.g. CDs), the system must have the capability to manage the media, including generating media identifiers that are unique within the system.

Managing the media involves documenting the:

- creation of a piece of media
- movement of media (including off-site)
- replacement (refreshing) of a piece of media.

If media are to be transferred to another agency or to PROV, provision must be made to ensure that the media identifiers are unique or are made unique within all the offices (including PROV) involved in the transfer. Agencies should consult with PROV on the application of unique identifiers.

Conformance to this point is achieved by the vendor supplying the software demonstrating the tracking of media.

3.9 Record export (Specification 1, section 2.9)

Agencies should note that this requirement covers the technical requirements involved in physically moving records and folders from one recordkeeping system to another. Export, in this limited technical sense, is usually part of a broader process known as transfer. Transfer covers the entire process of relocating records, including negotiations between organisations about what records to transfer and when, the actual transfer itself, and quality control.

Records and folders must be capable of being exported from a recordkeeping system.

The ability to export records and folders from a recordkeeping system is one of the critical functions in the long term preservation of records. Long term preservation means preservation for longer than the life span of the recordkeeping system holding the records, or for longer than the life span of the agency holding the records. In the latter case, when the agency ceases to exist the records and folders must be transferred to another agency or an archive. This will usually involve a transfer of records and folders from one recordkeeping system to another.

Hence it must be assumed that any long term records and folders will be exported from the system that they are currently being held in.

Export may be:

- between agency systems (e.g. from one system to its replacement)
- from a system in one agency to another agency
- from an agency system to a PROV system
- from an agency system to an off-site record storage location which meets PROV storage standards.[3]

When exporting records and folders to PROV, the records must be in the VERS standard record format; this is discussed below. This specification does not require any particular export format for export between systems, except for exports to PROV.

Conformance to this point is achieved by the recordkeeping system vendor demonstrating that it is possible to export records and folders from the recordkeeping system. Since the system is required to be capable of exporting records and folders in the VERS format (see below), export conformance will be satisfied by demonstrating export of records and folders in the VERS format.

An export of records or folders from a recordkeeping system is not complete until the receiving system has acknowledged that the record or folder was exported without error and the receiving system has accepted responsibility for the record or folder.

An export of records or folders is not complete until the receiving system has accepted responsibility for their ongoing custody. A simple indication that the receiving system has received the records or folders is not sufficient; the export might be subsequently aborted due to errors in the records or folders. A receiving system may decline the export for any reason, including errors in the records.

Until the receiving system accepts responsibility for a record or folder, the sending (exporting) system cannot complete the export and retains responsibility for the record or folder. It may be necessary for records or folders to be exported several times before responsibility for the records or folders is accepted by the receiving system.

Conformance to this point is achieved by the recordkeeping system vendor demonstrating that the export of a record or folder is not complete until an acceptance of responsibility is received from the receiving system. It will also be necessary to demonstrate that the

[3] See PROS 97/004 *Transfer and Storage of Public Records*. Available at the PROV Web site (http://www.prov.vic.gov.au/)

recordkeeping system allows the re-export of a record or folder (e.g. where the original export failed for some reason and the records or folders need to be exported a second time).

Importing or exporting of records or folders from a recordkeeping system must be documented.

Transferring records or folders is one method of disposing of records. Consequently, an export must be fully documented; this is discussed further in section 3.6.

Conformance to this point is achieved by the recordkeeping system vendor demonstrating that the recordkeeping system documents the export between systems, including the identity of the operator and the new location of the records.

The system must be capable of exporting the records and folders

- **in the standardised format given in *PROS 99/007 Specification 3*: *VERS Standard Electronic Record Format.***
- **containing at least the mandatory metadata given in *PROS 99/007 Specification 2*: *VERS Metadata Scheme.***
- **with the content in an approved long term formats given in *PROS 99/007 Specification 4*: *VERS Long Term Preservation Formats* or a format otherwise approved by PROV.**
- **on one of the approved export media formats and using the mechanisms given in *PROS 99/007 Specification 5: Export of Electronic Record to PROV*.**

It is optional, but highly desirable, that the recordkeeping system be capable of importing records and folders from VERS compliant systems.

- **in the standardised format given in *PROS 99/007 Specification 3: VERS Standard Electronic Record Format*. A recordkeeping system may only be capable of importing onion records (Version 1) or both onion records and Modified VEOs (Version 2).**
- **containing the metadata given in *PROS 99/007 Specification 2: VERS Metadata Scheme*.**
- **with the content in an approved long term format given in *PROS 99/007 Specification 4*: *VERS Long Term Preservation Formats*.**
- **on one of the approved export media formats and using the mechanisms given in *PROS 99/007 Specification 5*: *Export of Electronic Records to PROV* or a format otherwise approved by PROV.**

Conformance to this point is achieved by the recordkeeping system vendor demonstrating that the recordkeeping system can export, and import (if necessary), the records and folders according to the specifications.

Appendix A. Changes between Version 1 and Version 2 of this specification

The major changes between Version 1 and Version 2 of Specification 1 are:

- *Focus on the preservation requirements*. Version 1 of this Specification included many requirements that were general functions of a recordkeeping system. There are many documents covering these general functions, and these documents are more complete than the requirements given in Version 1. Consequently, in Version 2 the focus of the Specification has been narrowed to those requirements that support long term preservation of electronic records.
- *Explicit models of implementation*. In Version 1 there were two implicit models of implementation: one where the recordkeeping system used VEOs as the internal data structure, and a second where VEOs were only produced upon export. In Version 2 these models are made explicit and the implications of these models are discussed.
- *Specification of conformance requirements*. Some of the specifications in Version 1 were difficult or impossible to test. In Version 2 information has been added about how to achieve conformance to requirements and who would normally be responsible for achieving conformance.

A.1. Requirements that have been removed in Version 2

This section lists the requirements that have been removed from Version 2 of the Standard. Refer to Version 1 of the specification for the full text of the requirement. The relevant page numbers of Version 1 are given to facilitate reference.

A.1.1. Record Capture System Requirements

- Unique Files/Record Identifiers (p. 3)
- Record Linking (p. 4)
- Automatic Record Creation (p. 4)
- Record Creation Functionality (p. 4)

A.1.2. Archive System Requirements

- Evidentiary Integrity (p. 5)
- Access Control (p. 6)
- Disposal (p. 6)
- Destruction of Records/Files (p. 6)
- Refresh (p. 7)

A.1.3. Record Discovery System Requirements

- Supporting Documentation (Finding Aids, Thesauri) (p. 8)
- Access Control (p. 8)
- Access Logging (p. 8)
- User Interface (p. 9)

- Searching (p. 9)
- Verification (p. 9)