the national archives

Generic requirements for sustaining electronic information over time:

1 Defining the characteristics for authentic records

TABLE OF CONTENTS

1 SUMMARY 3

2 OVERVIEW 5

2.1 SUSTAINABLE ELECTRONIC RECORDS 5

3 DEFINITIONS 7

3.1 AUTHENTICITY 7
3.2 DEFINING RELIABILITY 8
3.3 DEFINING INTEGRITY 9
3.4 DEFINING USABILITY 11

4 ATTRIBUTES OF AUTHENTICITY AND INTEGRITY 14

1 Summary

1.1.1 Sustainable records are defined as those electronic objects and their concomitant metadata which defines them as records, which require continued retention by the creating or owning organisation until such time as the records can be destroyed or, where that is warranted, passed to a specialist archive for permanent archiving.

1.1.2 This document has been published as the first volume of a set of four which are provided to give central government departments an understanding of the principles which underpin any attestation that a record or a category of electronic records are considered to be authentic in accordance with *BS ISO 15489 Information and documentation – Records management standard*. If records are to be sustained there must be confidence that the maintained records possess authenticity, reliability, integrity and usability. A summation of the attributes, which would support an attestation of authenticity and integrity and which need to be maintained as part of the electronic record is provided in this document.

1.1.3 This *document* should be read in conjunction with the other three accompanying volumes in the series on *Generic requirements for sustaining electronic information over time*. The titles of the other 3 volumes in the series are:

2. *Sustaining authentic and reliable records: management requirements*
3. *Sustaining authentic and reliable records: technical requirements*
4. *Guidance for categorising records to identify sustainable requirements*

1.1.4 Volume 2 describes the management controls required for such systems and volume 3 addresses the technical requirements needed to maintain sustainable electronic records. Volume 4 provides high-level guidance for departments seeking to categorise their records to scope the specific nature of the requirements needed to sustain these record categories as authentic records.

1.1.5 These generic requirements are not a full specification. They form a baseline, which sets out, - the minimum necessary to maintain credible electronic records which will continue to possess the attributes of authenticity and integrity over time. They also should be read as an accompaniment to the Functional Requirements for Electronic Records Management Systems 2002 revision: final version which are available at:

http://www.pro.gov.uk/recordsmanagement/erecords/2002reqs/default.htm

1.1.6 The guidance is intended primarily for those working in central government; the principles will also be relevant in local government and throughout the public sector. Throughout this document the term ‘department’ should be taken to apply to any public sector organisation, including all departments, agencies and other organisations across government. Familiarity with the concepts of records as used in central government is assumed.

1.1.7 Each government organisation wishing to make use of these requirements, as a baseline or benchmark, will always need to consider its own specific business needs and context in determining its own requirements. These generic requirements must be tailored by: adding specialist business needs which are not covered at this generic level, selecting from alternative requirements according to corporate policy and practice, assessing whether any requirements listed in these volumes are highly desirable as opposed to mandatory for their own context

1.1.8 The generic functions described in this document may also be relevant to a permanent archive but the needs of archival preservation are considered as distinct from those operations required to maintain electronic records for continuing business needs even where the overall retention period may last for some decades.

2 Overview

2.1 Sustainable electronic records

2.1.1 Sustainable records are defined as those electronic objects and their concomitant metadata which defines them as records, which require continued retention by the creating or owning organisation until such time as the records can be destroyed or, where it is warranted, passed to a specialist archive for permanent archiving. The generic functions described in this document may also be relevant to a permanent archive but the needs of archival preservation are considered as distinct from those operations required to maintain electronic records for continuing business needs even where the overall retention period may last for some decades.

2.1.2 *The Requirements for Electronic Records Management Systems: Functional Requirements* – Revision 2002 published by the National Archives (TNA) describe many of the controls that would also be required in ensuring that records captured into a managed environment are capable of being sustained as credible records over a defined period of time. The ability to capture the record so that modification, or editing, of the record is no longer possible is a key facet of authenticity and must be supported by credible metadata, audit trails and reports. However whilst it is possible to capture a copy of the record in its original software format and store it unchanged in a repository linked to a corporate classification scheme it may not be feasible or desirable to maintain that record in its original format over the medium term.

2.1.3 The requirement for authenticity will mean that any software migration between formats will need to be managed and documented with care so that the reasons for the migration are explicit and the method used to validate the quality of the document following migration is clear. It should be emphasised that documentation of migration particularly needs to detail the methods used to effect the migration. These processes will also need to be supported by auditable records detailing who did what and when.

2.1.4 In order to achieve sustainable records management each institution will require an appropriate level of functionality together with the requisite tools and business rules required to support sustainable solutions. It will be necessary to sustain electronic records over time as a valued corporate asset, in a manner that retains their reliability and integrity for as long as they are required, preserving their value as a corporate record. This will include prevention of changes to the content or context to retain authenticity, and continued maintenance in an appropriate format to retain accessibility.

2.1.5 Records created and maintained in electronic form are continually at risk of inadvertent or intentional alteration, and such alteration may not be readily perceptible. The authenticity of electronic records is threatened whenever the records are transmitted across space (i.e., when sent between persons, systems or applications) or time (i.e., either when they are stored offline, or when the hardware or software used to process, communicate, or maintain them is upgraded or replaced). Authenticity can also be threatened by the act of access

as well as transmission where the access environment permits unauthorised and undocumented modifications of the record. Requirements for assessing and maintaining the authenticity of electronic records that are preserved over the long term are necessary, therefore, to support the presumption that an electronic record is, in fact, and continues to be, what it purports to be and has not been modified or corrupted in essential respects.

2.1.6 *BS ISO 15489 Information and documentation – Records management standard* requires that a record "*should correctly reflect what was communicated or decided or what action was taken. It should be able to support the needs of the business to which it relates and be used for accountability purposes."*

2.1.7 In this context this means that the content of a record should "*contain, or be persistently linked to, or associated with the metadata necessary to document a transaction "*. The key elements can be summarised as:

- the structure of a record, that is, its format and the relationships between the elements comprising the record should remain intact;
- the business context in which the record was created, received and used should be apparent in the record (including the business process of which the transaction is part, the date and time of the transaction and the participants in the transaction)
- the links between documents held separately, but combining to make up a record, should be present

2.1.8 The essential characteristics of a records are defined in section 7.2 of the *Information and documentation – Records management standard BS ISO 15489* as comprising:

- Authenticity
- Reliability
- Integrity
- Usability

2.1.9 In order to maintain a sustained object as a credible record it is necessary to define the performance criteria, which would provide credible evidence that these four elements have been addressed and supported during the period the record has existed. These elements are examined in greater detail the next section of this document. Ways of identifying the precise attributes of these characteristics are also explored in *Volume 4 Guidance for categorising records to identify sustainable requirements*

3 Definitions

3.1 Authenticity

3.1.1 BS ISO 15489 *Information and documentation – Records management standard* states in section 7.2 that:

An authentic record is one that can be proven

a) To be what it purports to be,
b) To have been created or sent by the person purported to have created or sent it, and
c) To have been created or sent at the time purported

3.1.2 It goes on to state that "*To ensure the authenticity of records, organisations should implement and document policies and procedures which control the creation, receipt, transmission, maintenance and disposition of records to ensure that record creators are authorized and identified and that records are protected against unauthorized addition, deletion, alteration, use and concealment*".

3.1.3 However BS ISO 15489 defines the essential characteristics of a records in section 7.2 as:

- Authenticity
- Reliability
- Integrity
- Usability

3.1.4 In practice authenticity can only exist if sufficient elements of the other three characteristics are present as authenticity in an electronic environment can only be established when the other characteristics are also present. As such authenticity is an implicit value derived or presumed from the presence of the explicit elements that characterise the other three characteristics. A presumption of authenticity is an inference that is drawn from known facts about the manner in which a record has been created, handled, and maintained.

3.1.5 A presumption of authenticity will be based upon the number of requirements that have been met and the degree to which each has been met. The requirements are, therefore, cumulative: the higher the number of satisfied requirements, and the greater the degree to which an individual requirement has been satisfied, the stronger the presumption of authenticity.

3.1.6 To maintain a presumption of authenticity the records must be managed in accordance with procedures that ensure their continuing authenticity. The production of copies of the records must be done in accordance with procedures that ensure that their authenticity is not compromised by the reproduction process. The requirements are based on the notion of trust in record keeping and record preservation from the moment of a record's creation. Given some records will be subject to change or alteration if they are

migrated to different software formats the standard of trust has to be considered in terms of circumstantial probability rather than certainty.

3.1.7 Assessing a record's authenticity involves establishing its *identity* and demonstrating its *integrity*. The *identity* of a record refers to the attributes, including external attributes such as context and provenance, that uniquely characterise it and distinguish it from other records (the name of the author, its date and place of origin, its subject); while the *integrity* of a record refers to its wholeness and soundness: a record has *integrity* if it remains complete and uncorrupted in all its essential respects throughout the course of its existence. This does not mean that a record must be precisely the same as it was when first created for its integrity to exist and be demonstrated. A record can be considered to be essentially complete and uncorrupted if the message that it is meant to communicate in order to achieve its purpose is unaltered.

3.2 Defining Reliability

3.2.1 BS ISO 15489 regards a reliable record as one *whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities*. Records should be created at the time of the transaction or incident to which they relate, or soon afterwards, by individuals who have direct knowledge of the facts or by instruments routinely used within the business to conduct the transaction.

3.2.2 BS ISO 15489 further states in clarification of the characteristic reliability that:

Any system deployed to manage records should be capable of continuous and regular operation in accordance with responsible procedures.
A records system should

- *routinely capture all records within the scope of the business activities it covers,*
- *organise the records in a way that reflects the business processes of the record's creator*
- *protect the records from unauthorised alteration or disposition,*
- *routinely function as the primary source of information about actions that are documented in the records, and*
- *provide ready access to all relevant records and related metadata*

3.2.3 Reliability therefore will be apparent if there is evidence that the records were created and captured as part of a legitimate business process and assigned to a logical and appropriate location within the businesses own classification schema or file-plan where the record will then be subject to corporate management of its disposal. The identity and where possible the specific role of everyone involved in the creation and capture of the record should be clearly apparent. The operational context or business process within which a record has been generated or managed should also be visible.

3.2.4 Reliability should secure the identity of a record as described in paragraph 3.1.7 above. It can be argued that reliability is an aspect or function of the

business' immediate operational requirements. In order to implement policy and complete transactions every business needs reliable records placed within a logical context. If reliability is not built into the operational processes by the adoption of record management functionality at the time of a record's creation and capture it is unlikely that it can be asserted subsequently with any degree of confidence. The application of records management functionality should secure reliability – integrity however is a demonstration that the controls placed upon a record upon its capture into a "reliable environment" were secured and maintained for as long as the record is required.

3.2.5 Continued reliability therefore emerges from operational needs, which are served by the continued existence of a record and those elements within the record, whose continued maintenance is considered essential to maintain if the record is ton continue to be regarded as reliable. The need for reliability will however differ according to the different types or categories of records created and held by a department

3.2.6 The characteristic of reliability itself can be broken down into three sub elements. These are:

- Trust
- Relationship/context
- Longevity

3.2.7 Trust is critical to reliability as without it there can be no meaningful faith in the accuracy of the retained records. Relationship and context refer to the comprehension of the meaning and value of records, which relies upon the ability of the reader to place the records in their operational context in a manner that their relationships with other affected records are clear and transparent. Longevity refers to the duration of the period for which the business still depends on the records to fulfill a residual business need.

3.3 Defining Integrity

3.3.1 BS ISO 15489 states that "*the integrity of a record refers to its being complete and unaltered*". It is necessary that a record be protected against unauthorized alteration. Records management policies and procedures should specify what additions or annotations may be made to a record after it is created, under what circumstances additions or annotations may be authorized, and who is authorized to make them. Any authorized annotation, addition or deletion to a record should be explicitly indicated and traceable.

3.3.2 BS ISO 15489 clarifies this with the following statement:

Control measures such as access monitoring, user verification, authorised destruction and security controls should be implemented to prevent unauthorised access, destruction, alteration or removal or records. These controls may reside within a records system or be external to the specific system. For electronic records the organisation may need to provide that any system malfunction, upgrade or regular maintenance does not affect the records

3.3.3 To sustain a presumption of authenticity it is necessary to identify the procedural controls over electronic records that provide a circumstantial probability of their integrity. The controls that define integrity include:

- establishing access privileges over the creation,
- modification,
- annotation,
- relocation, and
- destruction of records;
- instituting procedures to prevent, discover, and correct loss or corruption of records;
- implementing measures to guarantee the continuing identity and integrity of records against media deterioration and across technological change;
- where multiple copies of records exist, formally identifying the authoritative record; and
- clearly identifying and maintaining, along with the records, all the documentation necessary to understand their statutory, administrative and technical context

3.3.4 If reliability emerges from the original operational purpose that caused the record to be created integrity should reflect the long-term business needs that are served by the continued existence of a record. BS ISO 15489 differentiates reliability from integrity which suggests there is a distinction to be drawn between the immediate operational need, which requires records to be reliable to ensure effective transactions, and the longer term business need, where those same records must display integrity through possessing a quality of auditability ensuring that they can be considered to be authentic over time. If integrity is absent authenticity is very difficult to adduce let alone assert.

3.3.5 The characteristic of integrity itself can be broken down into four sub elements. These are:

- Traceability
- Retention periods
- Applicable rules, standards and regulations
- Risk

3.3.6 In order to confirm the record is unchanged or that only authorised and appropriate changes have been made, the status of the records and the presence or absence of change has to be auditable or traceable

3.3.7 As integrity is bound to the need to demonstrate authenticity over time it is necessary to clarify the specific business retention requirements.

3.3.8 In certain instances it may be necessary or desirable to retain records related to a broad record category where the records were themselves generated in response to codes of instruction or standards in force at that time. In order to confirm if the record of a transaction was valid in these circumstances it may be necessary to reference the rules that applied at that juncture.

3.3.9 The issue of record integrity is closely linked to effective business continuity planning in that in order to clarify the cost of maintaining record integrity it is necessary to evaluate the risk to the organisation if the records have been retained as incomplete or with limited auditable functionality.

3.4 Defining Usability

3.4.1 BS ISO 15489 defines a usable record as *one that can be located, retrieved, presented and interpreted.* It should be capable of subsequent presentation as directly connected to the business activity or transaction that produced it. The contextual linkages of records should carry the information needed for an understanding of the transactions that created and used them. It should be possible to identify a record within the context of broader business activities and functions. The links between records that document a sequence of activities should be maintained.

3.4.2 The aspects that will define usability will vary according to the business need. Initially the operational process, which created or captured a record will define how it is to be used and stored. However as the operational purpose that created that record evaporates other needs for this information may come to the fore. It may be necessary to provide access to the information in different forms linked or related to other material created subsequently. The issue for any business is that whatever drives the business need for the information and in whatever form this may take it should be immediately accessible to authorised users and the context in which the record was created and held should be apparent if that information is also required.

3.4.3 Usability comprises at least four key elements:

- The form or forms which the organisation may wish to view or publish this information
- The ability to produce new renditions in other formats as additional instances of the record whilst maintaining links to the original record
- the access permissions which allow access to the record or to redacted instances of the record (e.g. where it is necessary to publish or release a limited subset of the information but where some details such as names or addresses are retained)
- The ability of the user to know where this information was obtained and where it can still be located and retrieved if a requirement for authentication is established

At no point should usability infringe upon the integrity of the record

3.4.4 The requirement for usability may appear superficially the easiest to scope and comprehend particularly where the records either consist of images or text. Providing the appropriate viewer or browser is available the end users should have no difficulty accessing the record. The issue can then appear to revolve around the availability and presence of the appropriate viewing software. However, the issue is more complex than the previous analysis might suggest as usability is also about ease of locating, quick retrieval and the quality of the presentation. The first question to ask is:

- What makes a record usable and how might this differ according to different types of records?

3.4.5 Four sub-elements then need to be considered in evaluating the requirement for the usability of records over time. These are

- Locating
- Retrieval
- Presentation
- Interpretation

3.4.6 Locating refers to the means used to reliably identify without undue difficulty the record or records needed to satisfy the user's query. The location within the business classification schema or file-plan is one aspect but also the issue of accurate titling, meaningful nomenclature and the use of aliases or alternative titling fall into this area.

3.4.7 Effective retrieval is dependent upon identification of the anticipated pattern of access demand and the application and continued management of appropriate access permissions across time.

3.4.8 Effective presentation ensures the user can retrieve and view the records with the appropriate level of functionality required to undertake a meaningful interpretation. In some instance this may require the original program to be available so that the data can be manipulated or edited using the same functionality to create a new document or version, which can then be saved and added to the corporate record without changing or deleting the original. In other cases it may be sufficient to view the image in a more static environment either by using viewer technology or be generating a rendition, which is a faithful image of the original.

3.4.9 Interpretation at its simplest can be addressed by an ability to view text or images using a simple browser without the enhancements offered by the original software, for example one can view document created in MS Word using a text file viewer such as WordPad although the formatting is lost in this view. In other circumstances seeing the content without the display and formatting built into the original document makes interpretation difficult if not impossible.

3.4.10 In other instances interpretation also needs to be supported by linked contextual information, for example the ability to view the metadata of the record in both its original and existing context. This may require users having sight of both the current business classification system in which the records

reside and the original classification system where that differs from the current version. This situation can arise where functions have been transferred between government bodies resulting in bulk exports and imports of metadata and data between EDRM platforms.

4 Attributes of authenticity and integrity

4.1.1 In common usage, the concept of authenticity is defined as "the quality of being authentic, or entitled to acceptance."1 The term authentic means "worthy of acceptance or belief as conforming to or based on fact" and is synonymous with the terms genuine and bona fide. *Genuine* "implies actual character not counterfeited, imitated, or adulterated [and] connotes definite origin from a source." *Bona fide* "implies good faith and sincerity of intention." From these definitions it follows that an authentic record is what it purports to be and is free from alteration or corruption.

4.1.2 A presumption of authenticity is an inference that is drawn from known facts about the manner in which a record has been created, handled, and maintained. Volume 2 and 3 of these requirements describe the management and the technical requirements needed to support a presumption of authenticity. Volume 4 of these requirements *Guidance for categorising records to identify sustainable requirements* also describes the elements that form the key characteristics of a record and provides a list of the key questions departments will need to address when formulating their strategies to sustain record categories over time.

4.1.3 As stated previously in paragraph 3.1.7 assessing a record's authenticity involves establishing its *identity* and demonstrating its *integrity*. The *identity* of a record refers to the attributes, including external attributes such as context and provenance, that uniquely characterise it and distinguish it from other records (the name of the author, its date and place of origin, its subject); while the *integrity* of a record refers to its wholeness and soundness: a record has *integrity* if it remains complete and uncorrupted in all its essential respects throughout the course of its existence.

4.1.4 This does not mean that a record must be precisely the same as it was when first created for its integrity to exist and be demonstrated. A record can be considered to be essentially complete and uncorrupted if the message that it is meant to communicate in order to achieve its purpose is unaltered.

4.1.5 When records are captured into a controlled domain required for long-term storage, it is necessary for the maintaining authority to establish whether, and to what extent, the records have been maintained using technologies and administrative procedures that either ensure their authenticity or at least minimise risks of change from the time the records were first set aside to the point at which they are subsequently accessed. The requirements described below deal with the maintenance of authenticity. After the attributes for supporting authenticity of the electronic records have been established, their authenticity needs to be maintained over the long term across different hardware and software platforms and in some cases changes of custodian. Authenticity has also to be maintained where records are selected for permanent preservation and transferred into the custody of a specialized archive.

[1] Oxford English Dictionary

4.1.6 To do so, that part of the organisation charged with the responsibility of maintaining and preserving reliable and authentic records must manage the electronic records in accordance with procedures that ensure their continuing authenticity. They must produce copies of those records in accordance with procedures that ensure that their authenticity is not compromised by the reproduction process. The requirements are based on the notion of trust in record keeping and record preservation from the moment of a record's creation. Given some records will be subject to change or alteration if they are migrated to different software formats the standard of trust has to be considered in terms of circumstantial probability rather than certainty.

4.1.7 The organisations own policies and procedures have to reinforce the characteristics of a trusted record management system. A trusted record management system includes the rules that control the creation, maintenance, and use of the creator's records, which support a presumption of the authenticity of the records within the system. The requirements have to identify the core information about an electronic record that must be persistently linked to it over time and across hardware and software platforms in order to establish and perpetuate its identity. Such information includes, among other things, the names of the creator, addressee, and custodian the indication of the action or matter to which the record relates, the manifestation of the record's context within the classification system (what is referred to as the "archival bond"), and the indication of any annotations and attachments. These elements are clarified in the *Requirements for Electronic Records Management Systems Metadata Standard* published by the National Archives (TNA) and can be accessed at:

http://www.pro.gov.uk/recordsmanagement/eros/invest/2002metadatafinal.pdf

4.1.8 The metadata standard indicates, for the first time, some metadata at the component level (i.e. a level below that of the individual record and consisting of the single physical object (i.e. the smallest level of granularity the operating system can handle - MS-DOS or UNIX file level). This is the first phase of extending PRO guidance on metadata into the areas of sustainability and preservation of business records within departments. This Standard is extensible to allow for these developments to follow. Element 16 in the standard – Preservation- is not yet fully defined at this stage to flag up an area that is to be developed within the next 12 months. It is expected that the definition of requirements and accompanying metadata for sustaining records in departments, as well as work on permanent preservation in the National Archives (TNA), will lead to additions to this area of the metadata framework.

4.1.9 This metadata with additional information about changes the electronic records of the creator have undergone since they were first created will comprise the Preservation element in the metadata standard.

4.1.10 To sustain a presumption of authenticity it is necessary to identify the procedural controls over electronic records that provide a circumstantial probability of their integrity. Such controls include: establishing access privileges over the creation, modification, annotation, relocation, and destruction of records; instituting procedures to prevent, discover, and correct

loss or corruption of records; implementing measures to guarantee the continuing identity and integrity of records against media deterioration and across technological change; where multiple copies of records exist, formally identifying the authoritative record; and clearly identifying and maintaining, along with the records, all the documentation necessary to understand their statutory, administrative and technical context.

4.1.11 The requirements assume the existence of a role of a trusted custodian. The management requirements are published in volume 2 of these generic requirements: *Sustaining authentic and reliable records: management requirements.* These describe the procedures necessary to enable custodians to attest to the authenticity of electronic records after they have been transferred to their custody. Increasingly this will commence when a document is captured into an electronic record management system (ERMS). This role will require the custodian to actively intervene as part of the long-term maintenance process (e.g. software migration). Such interventions may require the application of approved and documented alterations to ensure the record remains usable whilst at the same time ensuring that the authenticity of the record is not affected. To be considered a trusted custodian, an organisation must demonstrate that it provides no opportunity for unauthorised alterations to the records, or to allow others to alter them in such a manner that the alteration compromises the authenticity of the record; and that it is capable of implementing procedures that ensure that any loss or change to records over time is avoided or at least minimised.

4.1.12 These controls required by a custodian can be summarised as:

- maintaining unbroken custody of the records,
- implementing and monitoring security and control procedures; and
- ensuring that the content of records and any required elements of documentary form and annotations remain unchanged after any reproduction or transformation process.

4.1.13 The maintaining organisation must also be able to demonstrate that the activity of reproduction has been thoroughly documented; and that the description of a given body of electronic records includes information about any substantial changes the records have undergone over time. Documentation and description are essential means of accounting for the integrity of the maintenance process in general and the reproduction process in particular and are necessary, therefore, to the proper fulfillment of the role of a trusted custodian.

4.1.14 This means that the authority and legitimacy of the claims made for the authenticity of electronic records derive entirely from the integrity and internal coherence of the procedures adopted to manage them. It follows that an organisation needs, not only to design and implement procedures that provide a strong probability of record trustworthiness but also to provide an honest and adequate account of the choices and decisions taken, during the stewardship of the custodial organisation.

4.1.15 For further information on what controls and mechanisms a custodial organisation will need to adopt please refer to volumes 2 and 3 of the Generic Requirements listed below: