MAINTAINING AUTHENTIC ELECTRONIC INFORMATION OVER TIME (INTERPRETING THE ESSENTIAL RECORD CHARACTERISTICS DEFINED WITHIN ISO 15489 TO IDENTIFY THE CRITERIA FOR PRESERVATION)

Richard Blake *

UDC: 004.3:006

Richard Blake: Maintaining authentic electronic information over time (Interpreting the essential record characteristics defined within ISO 15489 to identify the criteria for preservation). *Technical and Field Related Problems of Traditional and Electronic Archiving. Conference Proceedings, Maribor 4/2005, No. 1, pp. 64-79*

Original in English, abstract in English, summary in German.

This paper explores the potential to use the international records management standard *ISO 15489* to define the critical preservation criteria for electronic records and proposes the use of an intellectual framework founded on the standard to categorise the records according to the essential components needed to maintain the key characteristics defined in *ISO 15489* for records. The standard provides a definition of what constitutes a record, stipulating that it must have authenticity, reliability, integrity and usability.

To categorise records in this manner it is necessary to identify the precise elements that need to be preserved to maintain these records as authentic records as defined in the standard. To enable the required analysis this paper examines the recommended characteristics and attempts to deconstruct them to provide a series of questions that need to be answered if the key features of the characteristic which have to be present in each record category are to be identified.

INTRODUCTION

CONTEXT

Many records can be destroyed within seven years of their creation as the business use has expired and there is no requirement to keep them beyond the expiry of this period. They still need to be appropriately safeguarded during their brief lifetime but it is unlikely that the need for software migration or indeed media storage migration will arise. However a diminishing but still very significant volume of records will still need to be maintained or sustained beyond this time limit and with the passage of time the threat to their integrity and therefore their authenticity grows. Some records are required to be kept for periods beyond 20 or even 80 years before they can be disposed of and always for archivists there will remain a core collection which has historic value which has to be preserved indefinitely.

For archivists trying to plan for the permanent preservation of electronic records this represents a genuine concern as unlike records held in physical form storage of electronic information may be relatively cheap but preservation, will require a far more intrusive, proactive and costly regime than that needed for paper records to ensure the records remain accessible, usable and critically, continue to

* ***Richard Blake, Head of the Records Management Advisory Service The National Archives for England, Wales and the United Kingdom.***

possess a sufficient degree of integrity to support a claim that the records remain authentic.

Put simply we are unable to secure original electronic records as these really do not exist in the digital domain all we can aspire to is to preserve valid copies. These are themselves subject to change as unless technology can create truly robust and open software formats. We will, as time passes, have to contemplate migrating the records to other formats and this will lead to a loss of information.

We need to remember this is nothing new as for example very little of what records and archives we have from classical times survives in its original form (apart from carved inscriptions and coins) and we have to interpret the history of that period from medieval transcriptions created many years afterwards and we know that the transcribers made errors, added their own interpolations or alternatively expurgated some of the original.

Uninformed digital preservation runs a high risk of inadvertently repeating the scenario we have inherited with the records from ancient times. Our aim must be to avoid the potential for corruption when developing digital preservation strategies for modern electronic records by adopting an informed approach which allows us to determine that if change or loss in inevitable the chosen method represents the best possible solution which minimises the potential for corruption and allows us to define what we need to preserve and provide an additional evidential record for posterity to explain the basis for our chosen preservation strategy.

Records produced during the course of operational business will be used in different ways for varying lengths of time. The inherent differences between various record sets means that multiple strategies will need to be developed for sustaining or preserving them. There is a need to take account of how use might change as this may affect the preservation requirement.

POTENTIAL FOR CATEGORISATION

The sustainable requirements for particular records are associated with the need to retain them for operational and other business uses. This means that there is a need to be able to categorise records in a way that reflects how the records are used and what needs to be provided to ensure this purpose can continue to be met. This will provide a broad measure of the different requirements. This paper recommends a high level approach to the development of record categories although in practice it might be necessary to develop more discrete groupings. Through developing these categories it will be possible to ensure that the records of most value to an organisation or archive are not compromised and will be fit for purpose.

It is suggested that the rigour with which preservation requirements need to be applied will not be the same for all records as the length and type of business and operational use will not be the same. The differences in business and operational use will affect records in a way that will affect their need for authenticity, for example records used in court proceedings need to have a higher level of authenticity than those used for other purposes.

In developing an appropriate strategy account has to be taken of the differences of the length and type of use of different records. It would be impractical to do this at the level of individual records and unnecessary as many records have similar features. This means that it is necessary to determine how records can be

categorised at a high level in a manner where their characteristics reflect similar preservation requirements.

The nature of these categories will vary according to the nature of the creating organisation's activities and role but it is to be emphasised that a high level approach needs to be adopted to scope the sustainable requirements. Looking at every record created within an organisation and trying to establish a preservation need at that lower level is likely to be counterproductive and costly. Effective risk evaluation ultimately is critical to the success of a corporate strategy to maintain sustainable records.

The costs of sustaining or preserving records for long periods are potentially high even if the overall storage costs appear to be low. To guarantee reliable access to electronic records over time will require intervention strategies to perpetuate such access. In order to minimise costs it is therefore desirable for archivists to identify those categories of their records where it is essential for the effective conduct of the business to apply these strategies. Once the profile of a category is established which clarifies the elements that are needed to preserve the records as reliable, authentic and usable assets it will also be possible to identify the overall costs and resource implications of applying a particular maintenance strategy to a given category of records.

The benefits of adopting and implementing this approach can be summarised as follows:

- identification of the known or potential use of the records and how this may change over time.
- identification of the level of reliability required if the records are to be fit to meet the known business and operational use.
- identification of the requisite qualities that need to be maintained if the records are to demonstrate a meaningful degree of integrity.
- identification of the changing usability need to present and interpret the record in an intelligible manner.
- the ability to justify need and allocation of resources into sustaining particular record categories.
- the ability to determine when the sustainability requirements of a set of records might change and work out the implications this might have in terms of risk and resources.
- the ability to predict where resources will need to be allocated according to changes either in software or in terms of machinery of government changes to ensure records are sustained to the appropriate level of authenticity.
- identification of the risks and consequences involved if the records are not sustained. – e.g. are the benefits of sustaining greater than the benefits of not sustaining?
- identification of the resource requirements and concomitant costs needed to sustain particular record categories to a defined level of quality.

AUTHENTICITY

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

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*".

However *ISO 15489* then defines the essential characteristics of a record in section *7.2* as:

- Authenticity
- Reliability
- Integrity
- Usability

The standard is unclear as to what are the key features of authenticity although provenance is clearly very significant but this also should be apparent from the definition of reliability and integrity as it is impossible to assert that a record was created by the person or organisation as purported by the record unless there is an evidential chain provided by the reliability and integrity characteristics to support this contention.

In practice in can be argued that 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. If the other three elements are absent it is almost impossible to assert that the record is "*what it purports to be*"

The Report of the Authenticity Task Force of the InterPares 1 Project *Requirements for Assessing and Maintaining the Authenticity of Electronic Record*[1]*s* provided the concept of a presumption of authenticity

"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

[1] *http://www.interpares.org/book/interpares_book_k_app02.pdf.*

greater the degree to which an individual requirement has been satisfied, the stronger the presumption of authenticity."

In summary the Authenticity Task Force came to a pragmatic conclusion by concluding that if were are 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.

The Task Force argued that 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."

This paper agrees with these conclusions and what follows needs to be interpreted with this context. Consequently we need to examine the qualities which distinguish the other key characteristics required in *ISO 15489* that is reliability, integrity and usability if we are to identify the essential attributes that have to present and have to be preserved if records are to be considered authentic.

IDENTIFYING THE REQUIREMENT FOR RELIABILITY

Firstly we need to comprehend and clarify need for continued reliability as defined in *ISO 15489*. In other words what operational needs are served by the continued existence of a record and what elements are essential to be maintained to ensure that it can be considered to be reliable for those purposes? The need for reliability will differ according to the different types or categories of records created and held by an organisation

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

- trust
- relationship/context
- longevity

These three sub-elements are evaluated below.

TRUST

Trust is critical to reliability as without it there can be no meaningful faith in the accuracy of the retained records. The issue here is not so much the precise characteristics of an individual document as the characteristics of the records of an activity or transaction, which have to be maintained if the records are to continue to be serviceable. The questions that need to be addressed in order to substantiate trust are:

- What makes up or constitutes the record? (i.e. what is it that has been captured that is critical to the business)
- Who was the creator and how are they identified? (what are the critical elements - just the individual's identity or name or the profile allocated for example within an EDRMS at the time of the creation of the record? – the profile may be required to confirm if the officer named possessed the appropriate authority to undertake or authorise the transaction)
- Which dates have been captured in relation to the creation and modification of the records and which are significant? (i.e. what if any are the critical stages of the work process or transaction which have been captured)

RELATIONSHIP/CONTEXT

Comprehension of the meaning and value of records 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. Again it is not so much the precise characteristics of an individual document that should be considered as the characteristics of the records of an activity or transaction. Here it is the links and relationships with other records and the location of these within the business classification schema, which need to be considered. It should be noted that the development and adoption of a UK government records management metadata standard provides for the creation and management of relationships under the element pf Relation. The existence of multiple pointers within an Electronic Records Management System (ERMS) metadata database providing multiple locations is one relevant example. The questions provided below will help determine what contexts or relationships must be maintained for the records to be considered reliable.

- What is the scope of the records and what do they cover? (e.g. in the case of case records or transactions an understanding of the business process and possibly the statutory or regulatory context in which the records were created is essential to understanding them over time)
- Which records would be maintained in the same vicinity of the classification schema or file-plan, which are critical to the understanding of the activity?
- Which other significant records were produced in conjunction with the records of the activity under consideration?
- How long do these relationships continue to be meaningful?
- What cross-references or pointers exist and what is the relevance of the link between the two sets of records?

LONGEVITY

Longevity refers to the duration of the period for which the business still depends on the records to fulfil a residual business need. The requirement for reliability may differ according to the different types or categories of records created and held by an organisation. Establishment of this sub-element will assist in clarifying the requirement for maintaining the characteristic of integrity, which follows in the next section of this document.

- How long are the records used by the business centre that creates and manages the records?
- How often are the records updated while they are open?
- When are the records considered to be closed? (i.e. no longer updated)?
- How frequently, by whom and for what purposes are the records referred to once they are closed? (this helps identify the scale and nature of the continuing access requirement)
- What makes up the record and which parts are considered to be dispensable if any?
- Which dates or other information would be captured subsequently in relation to the modification of these records? (e.g. requirement to amend following a data protection subject access application)

These questions are still relevant even where it is established the records are to be selected fro permanent archival preservation.

IDENTIFYING THE REQUIREMENT FOR INTEGRITY

If we have clarified the components for reliable records we then need to identify what are the requirements for continued integrity to inform preservation strategies for sustainable records. 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. *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.

What has to be determined is what gives a record category its required level of integrity and how might this differ across the various categories of records identified.

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

- traceability
- retention periods
- applicable rules, standards and regulations
- risk

These sub-elements are examined below.

TRACEABILITY

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. The questions that follow can be used to scope the both need and the degree for auditable information

- For audit purposes, what are the minimum requirements of events to be recorded? For example,
  - changes in access provisions
  - additions to records (e. g. annotations and modifications)
  - movement history (e. g. exports or imports due to transfers of function or re-classifications within the business classification schema)
  - who has accessed the record and when
  - formats into which the record has been rendered, how this was achieved and why
  - changes in retention periods, why and when this was done
- How long would the events captured in the audit trail be needed for business purposes?
- Is there a need to maintain a record of the decisions relating to the access permissions applied to the records?
- When will a review of access provisions and permissions be required and what type of notification will be required?
- Is there a need to maintain an ongoing record of who has been permitted to have access to the records and the dates relating to the period of permitted access? (note - this is separate from a record of changes in access permissions)
- Is there a need to maintain a record of who has been permitted to modify the records? (note this is separate from a record of authorised changes or modifications)
- After the record has been disposed of how long will the metadata referencing the former record need to be viewable/ present/accessible?

RETENTION PERIODS

As integrity is bound to the need to demonstrate authenticity over time it is necessary to clarify the specific business retention requirements. In doing this it will be possible to establish the overall duration of the retention period to be applied to a category of records and clarify the profile of retention taking into account that the cost of the maintenance period is related to the length of the retention period. Where it is possible to reduce the volume and complexity of the records required to be sustained without compromising business effectiveness this will help justify the business case for expenditure on sustainable strategies.

- What are the retention requirements for these types of records?
- How is the retention period determined? (i.e. is it specified by a regulatory or statutory requirement)
- Are there some records in this area where parts of the records have longer retention periods than the rest of the record? (e.g. within thee UK certain key documents relating divorce decrees are retained for 75 years whereas the bulk of the material relating to a case are deleted after 25 years)
- Are there examples where it is more appropriate for a subset or abstract of the record of a transaction, rather than the whole record, to be retained for a longer period? (e.g. summary of employment service retained for superannuation purposes)

APPLICABLE RULES, STANDARDS AND REGULATIONS

- 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. For example a query or claim for an entitlement to a benefit may only be validated by cross-checking the standards that were extant at the time the adjudication was made.
- Is there a need to maintain the requirements and standards needed when considering for how long the records should be maintained?
- Is there a need to maintain the requirements or standards relating to the maintenance conditions of the records? (i.e. certain key document types may be explicitly referenced. For example, the server on which the records were stored, maintenance operations conducted on server, architecture of the ERMS)

RISK

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. The following questions are intended to help identify the scale of the risk to the organisation if integrity is compromised. This in turn will help cost justify the selection and application of specific sustainable strategies.

- What are the potential problems if the records are not available over x, y, z number of years?
- What are the potential risks of not effectively disposing of the records at the correct time?
- What are the potential problems if access controls and permissions are not properly maintained?
- What are the potential consequences of inaccurate information?

- What are the potential risks of not knowing where related records are located?
- What areas of the business would be of particular concern in relation to risk and contingency management and which records are considered to be the vital and/or the emergency records?

Any preservation plan needs to distinguish between vital records and emergency records and to make appropriate provision for their survival. Vital records are those records whose long-term preservation must be ensured to allow the continuation of organisational functions. In the event of a disaster, an organisation may not need immediate access to vital records, but it must be confident of their safety. Emergency records are those records to which rapid access is necessary following a disaster; records without which an organisation cannot function for more than a few days. It should be understood that not all emergency records are vital. Many vital records are not emergency records.

IDENTIFYING THE REQUIREMENT FOR USABILITY

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 posit is:

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

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

These sub-elements are examined below.

LOCATING

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.

- How are the records titled?
- What cross references/pointers are also required to be maintained and how are they made visible?

- What is used to show the location of records within the business classification schema or file-plan?
- What thesaurus terms are used and are these industry standard or user defined (the latter need to be identified if they are to be maintained)?

RETRIEVAL

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

There are also very real concerns about the ability of organisations to ensure successful retrieval to encrypted or password-protected objects. In the first instance there is usually a reliance on the presence of a proprietary software to open the object and in the second instance an ability to store and recall the appropriate password upon demand – if either mechanisms are not safeguarded and managed very carefully it may prove impossible, or at least very costly, to access such material. It is for that reason within the UK we would advocate that such protections are removed from objects before capture into an ERMS environment and any ongoing access control and security issues be managed using the appropriate functionality from within the ERMS to prevent unauthorised access or retrieval.

The level of access provided for retrieval purposes has also to take account of the anticipated reasons for retrieval and the frequency of demand. It should be noted that the reasons why a record may be accessed can change over time and may involve a different set of users, with a different frequency of demand to the pattern of use established by the operational need that created the record in the first instance. The patterns of use should be regularly reviewed for that reason as these can have cost implications for the organisation. Reduced demand may suggest that off-line storage would be acceptable whereas an increase in use may suggest that continued on-line access throughout the organisation is the preferred outcome. Essentially there are four types of storage. These are:

- On-line – (e.g. on servers on magnetic disk)
- Near-line (e.g. CD juke-box or robotic tape storage)
- Far-line (e.g. an on-line index with the records held on disk or tape in off-line storage)
- Off-line (e.g. index and objects stored on media externally to the network but physical retrieval possible upon request)

In practice the business requirement will mean the first two options are preferred for their greater convenience. However, the economics of far-line and off-line storage may be very attractive if the use of the records is estimated as being residual and very infrequent

Access requirements can be characterised by the following estimates:

- Total number of retrieval requests in a given period
- Average number of documents requested
- Average total size of request in megabytes
- For databases, cost of database query (rows retrieved or examined)

- Anticipated methods of retrieval (e.g. use of keywords, full text indexes and thesauri)

Access must be capable of being defined in response to an organisation's business needs and is likely to vary according to the organisation's information requirements. Records may need to be made available to the entire organisation or to a designated part of the organisation; there may be a series of levels or views depending on user access permissions. Records maintained without a sufficient access provision can be effectively worthless as the information they contain will not be readily retrievable to the key users.

The critical elements for an effective access strategy can be summarised as follows:

- Identify who can make requests, and who can execute them
- Understand management parallels with paper records
- Beware of using past access to predict future access patterns
- Take disaster recovery into account in planning

The questions that need to be asked to ascertain the retrieval and access requirements are:

- Are the access permissions likely to change over time?
- What type of access permissions would be set?
- What prompts would be set for access permissions to be changed?
- What level of frequency of access is required?
- What is your policy on encryption and password-protected documents/objects – are these routinely removed when migrated onto a new system?

PRESENTATION

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.

Different groups of users may have different presentation requirements. In some cases a small group may need the original functionality when viewing the record. The cost of supporting such a service may not be too onerous for a small group of specialised users but excessive for the whole organisation where the opportunity of viewing a rendition would normally be a satisfactory alternative. The technology used to interface and view the record must therefore reflect the ongoing business need. The questions that need to be addressed are:

- What form do the records currently take, (e.g. spreadsheets, word processing, presentation slides, movie clips) and what format are they associated with (e.g.

MS Word, MS Excel, HTML)?

- What level of presentation is essential to enable the users to undertake the work anticipated and required by the business

INTERPRETATION

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. If, for example, a respondent has cited a specific paragraph or entry of a code of instruction by its original number as the authority for undertaking an action or receiving an entitlement and this data is not visible to the user in the business, it will not be possible to either confirm or deny the validity of the claim. This type of information is often built into the format display properties of the software in which the document was originally conceived and can only be viewed either if the original program is available or an appropriate rendition, which has captured this detail, has been created and maintained.

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 for example where functions have been transferred between government bodies resulting in bulk exports and imports of metadata and data between Electronic Document and Record Management (EDRM) platforms. In those cases a portion or subset of the earlier or original classification system will have been transferred before the records are relocated in the new business's classification system. Maintaining a copy of the original classification system can assist understanding of the full context in which the records were created and used as well in addition to how they are seen in the current classification plan.

The questions that need to be addressed are:

- What is it about the document that will require interpreting, the content, the presentation or both?
- What level of contextual information is essential to a full understanding of the records?

DEVELOPING A STRATEGY

ISO 15489 defines an authentic record as *one that can be proven*. This can only be done if the elements that constitute the other three characteristics referenced above are present. The issue for any archivist is to determine what elements have to be maintained and also to what level or degree of quality if the sustained record is to represent a viable information asset during its lifetime ...

Having identified the characteristics that need to be maintained it then becomes necessary to identify the required resource requirements and overall costs of maintaining records to that degree. Having undertaken this analysis it is then recommended that organisations apply a risk evaluation methodology to ascertain the risk to the organisation of not maintaining records to the recommended degree. The final outcome should provide a robust basis for taking corporate decisions for the development and implementation of sustainable strategies. Archivists need to identify and quantify the resource implications required to maintain an existing record collection. However there are key questions that need to be asked in order to clarify the overall resource requirement of continuing to apply a sustainable strategy to a record category.

In some instances where records are not required for permanent preservation archivists will need to compare the value of the records to the business with their concomitant requirements for reliability, integrity and usability taking account of the cost and resource implications of applying a strategy which will secure the value and the authentic properties of the records. Extended or indefinite storage of electronic records does incur significant overheads and recommendations to either dispose of, or retain, a category of records will be informed by this knowledge.

Record categories of low value but with high resource implications will normally be marked for early disposal. However if the resource implications for continued retention are significant and the value of the records to the business are also high, knowledge of the continuing overhead will help focus decisions to migrate the information to more accessible and less onerous technical solutions. Such decisions will ensure the continued survival of the records. Caution is advised when evaluating record categories with high resource implications as such requirements should not of themselves determine a recommendation to dispose of a collection.

The questions that need to be asked at this juncture are:

- Are these records subject to security classification and/or protective markings?
- Are these records subject to other operational access controls?
- Should the records be reviewed for sensitivity (e.g. issues of privacy and commercial confidentiality)?
- Are these records accessible via the current hardware/software platform?
- If accessed via their current platform, will the records continue to be accessible on this platform for the short term? (1 to 2 years)
- If accessed via their current platform, will the records continue to be accessible on this platform for the medium term? (3 to 5 years)
- What percentage of the records require migration in the short terms (1 to 2 years) to a different software format to retain access?
- What percentage of the records require migration in the medium terms (3 to 5 years)to a different physical format to retain access?
- Are there specific difficulties in migration due to e.g. proprietary formats, non-standard design structures?
- Should the records be sampled to verify technical decisions

In conclusion it should be emphasised that the questions proposed in this document do not represent a comprehensive or an exhaustive list nor would it be necessary to define responses to all the questions referenced in this document.

These questions are provided as guidance not as mandated requirements. Archivists should use their judgement to determine which are apposite given the business environment they work within.

ZUSAMMENFASSUNG

DIE LANGZEITERHALTUNG AUTHENTISCHER ELEKTRONISCHER DATEN (AUSLEGUNG DER GRUNDLEGENDEN CHARAKTERISTIKA VON AKTEN ZUR ERKENNUNG DER KRITERIEN IHRER ERHALTUNG, FESTGELEGT DURCH ISO 15489)

Ein schwierige Aufgabe für Archiv- und Registraturbeamte bildet die Sicherheitsgarantie für die Aufbewahrung elektronischer oder digitaler Aufzeichnungen, damit deren Echtheit nicht angezweifelt werden kann. Sie wird noch problematischer, wenn sich die Zeit verlängert, innerhalb welcher sie aufbewahrt oder gar benötigt werden.

Es wurde angenommen, dass die Eigenart jedes Dokuments dem Archivar hilft, die entsprechenden technischen Voraussetzungen zu schaffen, um dessen Authentizität zu gewährleisten. Sollten die Charakteristika nicht bewahrt werden können, verlieren die aufbewahrten Akten ihre Glaubwürdigkeit und es fehlt deren Beweiskraft. Durch das Erkennen der Hauptmerkmale besitzt der Archivar die grundlegenden Beurteilungskriterien, entsprechende Erhaltungsmaßnahmen einzuleiten. Dieses Referat untersucht die Leistungsfähigkeit der internationalen Standards für die Aktenverwaltung, ISO 15489, um entscheidende Erhaltungsmaßnahmen für elektronische Akten zu definieren. Empfohlen wird die Erstellung eines geistigen Umfeldes auf Grundlage von ISO 15489, um die Akten entsprechend ihrer Grundbestandteile, welche nötig sind, um die Charakteristika laut ISO 15489 zu erhalten, einzuordnen. Die Standards bieten eine Erläuterung dafür an, was einen Akt ausmacht, indem sie festlegen, dass er Authentizität, Vertrauenswürdigkeit, Unverletzlichkeit und Verwendbarkeit besitzen muss.

Das Referat hält fest, dass sich die Authentizität aus dem Vorhandensein der anderen drei Charakteristika, wie sie die Standards beschreiben, ergibt. Um Akten in der vorgeschlagenen Art und Weise einzuteilen, ist es notwendig, ihre genauen Einzelheiten zu identifizieren, welche bewahrt werden müssen, um sie authentisch, wie sie durch ISO 15489 *Information und Dokumentation - Standards der Aktenverwaltung* definiert sind, zu erhalten. Um die gewünschte Analyse auszuführen, werden in diesem Referat die empfohlenen Charakteristika geprüft. Es wird empfohlen, sie zu zerlegen, um eine Reihe von Fragen aufwerfen zu können, welche beantwortet werden müssen, um die Hauptmerkmale jedes Charakteristikums, das in jeder Art von Akten vorhanden ist, zu identifizieren.

Daraus folgt, dass ein Akt, welcher nicht diese Charakteristika aufweist, nicht authentisch und daher für unsere Zwecke unzuverlässig und unbrauchbar ist. Die Erklärung dessen, was einen authentischen Akt ausmacht, wird nicht für jede Bestandseinheit gleich sein, da jeder Teil verschiedenen Anforderungen dient und andere Kriterien, wie Vertrauenswürdigkeit, Unverletzlichkeit und Verwendbarkeit, aufweist. Letztere sind quasi die Voraussetzungen, da Authentizität ohne sie, also allein, nicht bestehen kann. Das unterschiedliche Niveau der entscheidenden Charakteristika der einzelnen Aktenbestände, die manchmal auch als authentische

Kopien angesehen werden können, kann dazu verwendet werden, spezielle Erhaltungsmaßnahmen zu entwickeln. Als Teil der Bemühungen, diese Anforderungen der Bewahrung digitaler Bestände zugrunde zu legen, haben die Staatsarchive Großbritanniens ein Konzept erstellt, das wir unter der Bezeichnung *erhaltenswürdige Akten* einordnen.

Diese *erhaltenswürdigen Akten* werden als jene elektronischen Objekte samt begleitender Metadaten definiert, welche sie als Akten ausweisen, für welche eine dauernde Erhaltung von Seiten der aktenbildenden Stelle oder der Eigentümer bis zu jenem Zeitpunkt gewährleistet werden muss, ehe sie zerstört oder auf Anordnung einem speziellen Archiv zur dauerhaften Aufbewahrung übergeben werden. Übernimmt das Archiv solche Akten, muss die Garantie gegeben sein, dass diese Authentizität, Vertrauenswürdigkeit, Unverletzlichkeit und Verwendbarkeit besitzen.

Schlussendlich soll betont werden, dass die in diesem Referat erhobenen Fragen keineswegs eine umfassende oder erschöpfende Liste darstellen. Es war daher auch nicht notwendig, auf alle gestellten Fragen zu einzugehen. Sie sollen eher als Anleitung denn als angeordnete Voraussetzungen dienen. Archivare mögen sich auf ihre Urteilskraft stützen, um zu erkennen, welche auf die Umgebung ihres eigenen Arbeitsplatzes passen.

Richard Blake *is the Head of the Records Management Advisory Service (RMAS) which is a service which was established by the National Archives for England, Wales and the United Kingdom in May 2003 to support public authorities beyond UK central government to local government, health, police and emergency services to support their development of effective record and information management systems. This service brought together the existing Archival Inspection Service with the Electronic Records Management Development Unit to extend the services already provided to central government to also provide advice and guidance to other public authorities wishing to implement ERM systems and subsequently transfer records to the archives. He is responsible for developing and managing the programme for this service. Prior to the establishment of the National Archives on 2 April 2003 he worked for the Public Record Office for 31 years specialising in records and information management and preservation storage. Since 1995 as an electronic record management specialist he has focused on developing guidance on implementing electronic record management and up to March 2002 was also responsible for the contract management of the PRO's database archive service (NDAD) provided by the University of London. He has contributed to the development of the Functional Requirements for Electronic Records Management published in 2002 and has participated in the Electronic Record Management (ERM) software compliance-testing programme. In this context he is also the author of a number of PRO publications on planning for Electronic Document and Record Management (EDRM) and was one of the contributing authors of the earlier Guidelines for the management, appraisal and preservation of electronic records. Other activities have focused on developing a 'sustainability' strand of ERM work -the needs of public bodies to maintain authentic and reliable electronic records as defined by ISO 15489 over the medium term - and led the project to develop detailed generic requirements for sustainability of electronic information. More recently he has been charged with the development of an audit methodology to evaluate the performance of records management systems and services - the first product of which will be published in the form of a consultation draft in April 2005.*