



Complying with the Records Management Code: Evaluation Workbook and Methodology

Module 5: Records maintenance

Module 5: Records maintenance

General

- 7.1 This module deals with the need to establish a records maintenance regime which will sustain or preserve records, along with the means to identify and retrieve them easily, for as long as they are required. The objective should be to maintain authentic, reliable and usable records, as defined in the previous chapter, that conform to BS ISO 15489 requirement for the maintenance of record integrity.
- 7.2 Additional Guidance on interpreting these characteristics is provided in the TNA publication entitled *Guidance for Categorising Records to identify Sustainable Requirements*. This is available at:
http://www.nationalarchives.gov.uk/electronicrecords/pdf/generic_reqs4.pdf
- 7.3 Given that most current information is now generated in electronic form (e.g. databases, documents generated on office systems and e-mail) and continues to be held in digital form, the maintenance regime should deal with sustaining records held electronically and well as those in physical form.
- 7.4 The relevant workbook questions which should be used to assess the level of compliance relating to these activities commence on page 7.

Context

- 7.5 Section 8.7 of the Records Management Code describes the key criteria required to establish an appropriate maintenance regime. It states that:

The movement and location of records should be controlled to ensure that a record can be easily retrieved at any time, that any outstanding issues can be dealt with, and that there is an auditable trail of record transactions.

Storage accommodation for current records should be clean and tidy, and it should prevent damage to the records. Equipment used for current records should provide storage which is safe from unauthorised access and which meets fire regulations, but which allows maximum accessibility to the information commensurate with its frequency of use. When records are no longer required for the conduct of current business, their placement in a designated records centre rather than in offices may be a more economical and efficient way to store them. Procedures for handling records should take full account of the need to preserve important information.

A contingency or business recovery plan should be in place to provide protection for records which are vital to the continued functioning of the authority.

- 7.6 The record management system referred to in module 4 should include:
- adequate storage accommodation for the records
 - a tracking system that controls the movement and location of records so that they can be easily retrieved
 - appropriate access controls
 - a business recovery plan that provides for the protection of vital records
- 7.7 The storage requirements for electronic records will be substantially different to those required for physical records although the same principles apply. The measures adopted must be appropriate for the format of the records.
- 7.8 Section 10 of the Records Management Code provides specific guidance on the management of electronic records and in respect of the records maintenance aspect it states that:
- Effective electronic recordkeeping requires:*
- *The secure maintenance of the integrity of electronic records*
 - *The accessibility and use of electronic records for as long as required (which may include their migration across systems)*
 - *The ability to cross reference electronic records to their paper counterparts in a mixed environment*
- 7.9 The Code goes on to require the maintenance of audit information, It states that:
- Audit trails should be provided for all electronic information and documents. They should be kept securely and should be available for inspection by authorised personnel. The BSI document Principles of Good Practice for Information Management (PD0010) recommends audits at predetermined intervals for particular aspects of electronic records management*
- 7.10 The international records management standard - *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 unauthorised 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.

7.11 *BS ISO 15489* provides the following clarification: “Control measures such as access monitoring, user verification, authorised destruction and security controls should be implemented to prevent unauthorised access, destruction, alteration or removal of 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”.

7.12 To sustain a presumption of authenticity it is necessary to identify the procedural controls over the records that provide a circumstantial probability of their integrity. For paper records this is often achieved entirely through the application of business rules and physical security measures (e.g. a secure room or cabinet). For electronic records, which are far more mutable, these procedural rules have to be supported, where appropriate, by functional systems, which will enforce and document the application of these rules. The controls that define integrity and thereby generate an effective record maintenance regime 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

7.13 The efficient maintenance of records will ensure that they receive adequate protection from fire, flood, theft, and other forms of catastrophic loss so the records irrespective of format are neither lost, corrupted or subjected to unauthorised alteration and can easily be located and retrieved when required.

Relevant guidance

- 7.14 Each sector may have its own sector specific rules, regulations and guidance and readers of this workbook should use such guidance when establishing a record keeping or management system. Additional guidance on this subject has been provided by The National Archives (TNA) and is available on the TNA web-site. The following publications on the maintenance of electronic records should be used:

Sustainable electronic records strategies for the maintenance and preservation of electronic records and documents

This document is appears within the list of electronic toolkits and can be accessed at:

<http://www.nationalarchives.gov.uk/electronicrecords/advice/>

- 7.15 The four volumes which comprise the Generic Requirements listed below build upon the sustainable electronic records strategies toolkit mentioned previously and provide further guidance on defining the characteristics for authentic electronic records as well as providing management and technical requirements as well as advice on how to categorise electronic records when determining an appropriate maintenance strategy:

Generic requirements to sustain electronic information over time volumes 1 to 4

These requirements are at:

<http://www.nationalarchives.gov.uk/electronicrecords/generic.htm>

- 7.16 The costs of sustaining or preserving records for long periods are potentially high even if the overall storage costs appear to be low. In particular 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 departments to identify those categories of their records, which continue to be needed for business purposes. Module 7 deals with the measures required for the effective appraisal and disposal of records. Once the profile of a category is established which clarifies the elements that are needed to preserve the records as a reliable, authentic and usable asset 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.

- 7.17 Other relevant advice, guidance and standards on the maintenance of physical records including business recovery planning can be accessed from the Records Management section of the TNA web-site at:

<http://www.nationalarchives.gov.uk/recordsmanagement/advice/>

Evaluation questionnaire

- 7.18 To assess whether these elements have been adequately addressed see the questions in the table on the following page, numbered 1 to 25 in this workbook. Guidance on how to analyse the responses to these questions is provided in the chapter entitled *Risk evaluation and development of mitigation strategies*.

1. *Is there a corporate strategy to ensure records in both physical and electronic form are maintained for as long as they are needed?* Yes No N/A

Reference

2. *Does the organisation have a record of the reasons why specific record sets are required to be maintained (i.e. what is the business requirement served by these records) and for how long?* Yes No N/A

Reference

3. *Have mechanisms been established to prevent unauthorised modification of electronic records whilst providing for the addition of authorised annotations where required?* Yes No N/A

Reference

4. *Does the organisation maintain an inventory of the specific formats in which the records are held (e.g. paper, video, microform) and, where electronic formats are involved, the software format and the media storage format?* Yes No N/A

Reference

5. *Are there agreed triggers to review existing software formats to ensure usability and to avoid obsolescence or degradation?* Yes No N/A

Reference

6. *Do all the records (electronic & physical) possess a unique identifier or call reference?* Yes No N/A

Reference

7. *Is there a comprehensive index or indexes to locate and retrieve records upon demand?* Yes No N/A

Reference

8. *Is there an agreed process for choosing the appropriate storage method for both physical and electronic records and to review the method over time?* Yes No N/A

Reference

9. *Where an established process exists to determine how to choose the appropriate storage method is there a validation mechanism to confirm the chosen method continues to be appropriate?* Yes No N/A

Reference

10. *Does the organisation's business continuity or disaster management programme include records maintenance?* Yes No N/A

Reference

11. *Have the resource requirements for records maintenance been identified for disaster contingency management and recovery?* Yes No N/A

Reference

12. *Has there been an assessment of the risk to the organisation where the records are incomplete or have limited auditable functionality?* Yes No N/A

Reference

13. *When storing or transporting records in electronic form have the appropriate environmental storage conditions and methods of carriage been adhered to?* Yes No N/A

(e.g. BS 4783 Storage, transportation and maintenance of media for use in data processing and information storage).

14. *Reference*

15. *When exporting or transferring electronic records to another organisation (e.g. because of a transfer of function or to preserve the records in a specialist archive) has guidance been developed to determine what metadata has to be transferred along with the record content in order to ensure the recipient acquires records which can be considered authentic, reliable, possess integrity and are usable in accordance with BS ISO 15489* Yes No N/A

(Note: the quality of the metadata available will vary according to the nature of the system upon which the records are stored. If the records are held on an ERM or EDRM system which supports the e-GMS record management metadata standard the quality measure will be the ability of the system to export selected records with such metadata. For other systems the rationale will be the ability to export and associate metadata which provides all the information required to place the records in context and enable them to be usable for the purpose required by the acquiring institution)

Reference

16. *Are there triggers to identify when migration of electronic records is needed to avoid obsolescence or degradation??* Yes No N/A

Reference

17. *Are there monitoring mechanisms or other measures to assess whether electronic records are still readable? (N/B this question should be extended to include back-up copies as part of business continuity planning)* Yes No N/A

Reference

18. *Have minimum information levels been defined within the management audit trail for each maintenance process to ensure the maintenance of reliable electronic records?* Yes No N/A

Reference

19. *Are the storage areas allocated to hold physical records adequate to accommodate anticipated accruals?* Yes No N/A

Reference

20. *Do the storage areas for physical records conform to agreed standards for the storage of records (e.g. BS 5454)* Yes No N/A

Reference

21. *Are the storage areas set aside for physical records regularly inspected?* Yes No N/A

Reference

22. *Have access controls been established to provide and record authorised access to records and prevent unauthorised access?* Yes No N/A

Reference

23. *Have procedures been implemented to allow for authorised changes in access permissions over time?* Yes No N/A

Reference

24. *Have safeguards been implemented to prevent and where feasible record unauthorised access to electronic records?* Yes No N/A

Reference

25. *Where applicable has a policy been implemented to ensure continued access to encrypted or password-protected records?* Yes No N/A

Reference
