The National Archives
Records Management Guides

5. Active Records Management: Record Keeping and Record Maintenance

The National Archives Records Management Guides

Active Records Management: Record Keeping and Record Maintenance

Introduction

This Records Management Guide has been produced by The National Archives as part of a series of brief explanatory guides which have been developed to help public authorities achieve compliance with the Code of Practice, issued by the Lord Chancellor, under Section 46 of the Freedom of Information Act 2000 which provides guidance on good practice in records management to all authorities subject to either the Freedom of Information Act, or the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923. For the convenience of the reader this Code is hereafter referred to as the Records Management Code.

The main aim of keeping and maintaining active records is to ensure that records can be retrieved and accessed for as long as required but in an environment that ensures their preservation and integrity. This guide covers:

- How to maintain the active recordkeeping system once it has been set up
- How to carry out a survey of the organisation's records
- Implementing and reviewing procedures for filing
- How records will be retrieved, accessed, tracked and returned
- Planning and managing storage of records in all media to ensure proper security and protection from damage and deterioration
- Identification and protection of vital records to ensure their continued accessibility
- Periodic review of the system

Inventories and surveys

As with any resource that requires management, you need to know the quantity and nature of the records that the records management system encompasses. The best way to find out the scope of the records in the organisation is by carrying out a comprehensive record survey (sometimes called an audit). This initial survey is the cornerstone of your records management system. The Records Management Code states:

"Installing and maintaining an effective records management programme depends on knowledge of what records are held, in what form they are made accessible, and their relationship to organisational functions. An information survey or record audit will meet this requirement, help to promote control over

the records, and provide valuable data for developing records appraisal and disposal procedures."

Purpose and outcome of the survey

The survey is the basis for physical and intellectual management decisions about the organisation's records. It should provide you with all the information you need to manage the organisation's records effectively, whatever their format, including efficient and effective storage and retrieval, improved records filing systems, disposal schedules and vital records protection.

In particular the purpose of the survey is:

- To produce an inventory of the organisation's records
- To provide data on the quantity, medium and format of records
- To identify and evaluate current records storage arrangements
- To provide information on the functions and activities that give rise to or are supported by the records
- To gather data on who uses records and the information flows between different functional areas or business units
- To gather information to enable assessment of the value and longevity of the records and preparation of disposal schedules
- To identify records vital to the continued functioning of the organisation
- To identify sensitive or confidential records
- To provide information on legal and regulatory considerations
- To identify the master record and related copies
- To identify issues and risks related to version control

The survey also:

- Allows the records management team to meet and talk to a wide range of colleagues who have been identified as key stakeholders in the records management programme and to hear their concerns
- Provides an opportunity to raise organisational awareness of records management
- Informs records management planning and facilitates the development of policy, strategies and procedures to support the implementation of an effective recordkeeping regime
- Helps in planning controlled transfer of archival records to a designated archives service (in the case of public records this will be The National Archives or another archives office appointed as a place of deposit for public records)

- Supports the specification and development of and/or migration to systems which contain and/or manage records

The outcome of the survey will be information required to develop tools, procedures and products that will underpin the organisation's records management programme, including:

- Disposal schedules
- New or improved filing systems
- More effective identification and retrieval of records when needed
- A vital records protection strategy and related disaster recovery programme
- Secure handling of records identified as sensitive or confidential
- Early destruction of records assessed as of no continuing business or historical value
- Removal of inactive records to non-current (and more cost-effective storage) thereby consolidating and/or freeing up office filing space
- Inadequate or redundant records systems identified

How to carry out the survey

The records survey needs to be carefully planned to ensure it covers all areas of the organisation required, that all the necessary information is collected and full advantage can be taken of the opportunity to publicise the benefits of good records management. This initial stage includes clear definition of the objectives of the survey, as this will influence later stages.

Before launching the survey proper, some desk research will inform the survey and ensure that the time is used effectively and all aspects of records management are covered. In particular it is useful to look at:

- Existing file plans and lists
- Existing retention schedules
- Records management policies and procedures
- In-house and outsourced storage area costs and locations
- Details of any microfilming or scanning operations
- Inventories of application systems maintained by the IT department
- The IT infrastructure, platform, servers, intra-, extra- and inter-net arrangements etc.

It is essential to secure senior management support for the survey. Ideally the senior manager responsible for records management will endorse initial communications announcing the survey, its purpose, benefits and outcomes, to staff.

The survey should be announced to staff in plenty of time to schedule and complete the work that involves them. How this is done will depend on the organisation's corporate culture, e.g.:

- Initial and follow-up email or memos to all staff
- Initial and follow-up email or memos to managers
- Initial and follow-up email or memos to staff particularly engaged with or representing their team on records management issues
- Briefing meetings for different categories of staff or functional areas

There are two ways of carrying out a survey: by interview or by questionnaire. The best way is to interview staff representing all business areas because this ensures that the data is gathered in a consistent way, with no room for misunderstanding or omission. An alternative is to send out a questionnaire for completion by staff. This can be more cost-effective especially if help is available to anyone finding it difficult to complete. However there are risks associated with this approach, such as non-return and omission of data: a more comprehensive survey will be achieved by face-to-face interviews and physical observation.

Regardless of whether the interview or questionnaire method is used, it is important to identify the appropriate staff to provide the necessary information on their team's records. The organisational chart is invaluable in identifying work units and assessing the number of individual surveys to be done. Scheduling interviews can be time-consuming so it is advisable to allow plenty of time for scheduling and to build in flexibility for re-scheduling as necessary.

Development of the survey form is a crucial step in planning the survey. The content of the form is covered in the next but one section but you also need to consider how you will hold the data. A relational database will enable production of searchable and sort-able tools such as a full records inventory, retention schedules, vital records inventories, file plans etc. In smaller organisations a spreadsheet may be sufficient.

There are a few issues concerning electronic records which have an impact on the survey and which must be taken into consideration. You need to think through the level at which data about records will be captured. Often it is not so easy to identify an electronic record series, particularly in a non-managed environment, as records in the series may be saved and maintained in many different locations. It is also important not to confuse an application system with a record series or collection because although a database may be one and same, many record series are not. You will also need to gather information not only on the record series but the system, which holds it. If there are concerns about the record-ness of electronic information, which is particularly likely in non-managed systems rather than where EDRM systems are in use, the survey data should include the possibility of substantiating compliance with recordkeeping standards.

Finally you will need to present the survey findings. How you do this will depend on the organisation but one obvious way is a report on the state of recordkeeping in the organisation with recommendations and implementation plans. This could be supported by a database with inventory of records, retention schedules, file plans etc. You should present your findings to staff and managers as appropriate, either in writing or in an oral briefing supported by a written summary.

What to include in the survey

A comprehensive records survey needs to include all records created or processed in the organisation, it may also cover information other than records, especially where these have an important relationship with other records or affect records management issues (for example reports from other organisations which form the basis of decisions or policy). The survey must include all records:

- Regardless of the medium or format
- Regardless of the record's status (for example both registered and non-registered files, electronic records in EDRM systems and in non-managed systems such as Microsoft Office folders)
- Regardless of whether they are current or non-current unless the non-current records are no longer in the custody of your organisation

Survey data

It is advisable to design a form to collect the survey data. The form will provide a set of questions to ask which will ensure consistency in the data gathered and result in structured information to use as a basis for analysis and for the development of disposal schedules, files plans and other survey outcome tools. What data is gathered and in what order will depend on the main focus of the survey, which should have been decided at the planning stage.

The section on further guidance and information at the end of this guide contains a number of references to works, which contain sample forms and discuss survey data in detail. Here is a list of the data elements, which should be considered for inclusion in the survey:

- Record creator(s) and organisational origin
- Unique identifier or call reference for each record series, group or collection
- Title and/or description of record series, group or collection
- Function or activity supported by records

- Record medium and format
- Master or copy
- Date range of records
- Whether the records are current or non-current
- Location of records
- Quantity and growth rate of records
- Length of time record series, group or collection should be kept for legal or business reasons
- Reasons for retaining each record series, group or collection (legal, business, regulatory or other)
- If the records are archival and should be kept permanently
- If the records are confidential, sensitive or subject to security classification
- If the records are vital records in the event of an emergency, their cycle of currency and any protection strategies in place
- Any indexes, lists, databases or other finding aids which assist in locating and retrieving records
- Frequency of use of records
- Other business areas with access needs to records
- Tracking systems for records
- Details of record containers
- Planned changes or upgrades, e.g. migration to new systems

Review of survey and systems

As organisations develop and change, the priorities and functions change which results in different recordkeeping requirements. It is therefore good practice not only to keep the record inventory up to date but also to periodically review it or even repeat the survey. This ensures that the records management programme remains comprehensive and consistent. Periodic surveys of records also demonstrate a commitment to best practice.

Filing and on-going maintenance

Unless it is properly maintained the filing system will quickly become ineffective. The National Archives Guide, *Active Records Management: Record Creation*, covers how to design, implement and document filing systems. Once the system is established all staff should be trained in how to add new records, including capturing the necessary metadata. The structure of the filing system will need to be maintained over time too: staff should know the procedures for adding new file categories or taking out sections that are no longer required. Training should be based on the filing system documentation, which includes procedures for referencing, titling, indexing, security marking (if appropriate) as well as the file plan itself. The training should also be integrated into induction for new staff. Training and clear procedures will contribute to the reliability and authenticity of the records and the recordkeeping system and will ensure that the system can be understood and operated efficiently.

Retrieval and tracking

Records are created and captured in order to be used, therefore recordkeeping systems must include effective mechanisms for retrieving records and tracking their whereabouts and use. Effective procedures must be in place to ensure swift retrieval, an audit trail of use and, for paper records, their accurate return.

A good records retrieval operation contains the following elements:

- Effective finding aids to identify the record and provide location details and access restrictions particular to it (e.g. indexes, databases, file plans)
- Authorisations for access (for named staff or according to their role or business unit)
- Security clearance system (if appropriate)
- For paper records, a production register to record details of records accessed, their location, member of staff responsible and return of records

Depending on the nature of your organisation’s business, authorisation to access records may be more or less important. Where most records are available to the public, it is clearly nonsensical to operate an authorisation system to give staff access to records. However, where records are sensitive because of data protection, commercial confidentiality or security issues, the records will need to be tagged in some way and staff will need to be authorised before gaining access. It is also important to bear in mind that electronic formats are more susceptible to undetected change and amendment than paper records – and a record that has been changed is technically a new and different record. Therefore, unless adequate version control facilities are part of the system, generally speaking, access to electronic records should be provided on a read-only basis. However, with databases and other electronic records where one or more people enter and even change data over time, there must be clear procedures, regular quality control and an audit trail to ensure that updating and amending can be carried out but that it is authorised and transparent.

Effective record tracking ensures not only that records can always be located when required but also that records remain in a controlled and secure environment thus adding to their reliability and authenticity. Access to electronic records can be automatically tracked, but paper records require a robust system and procedures. Tracking systems should record:

- The record's reference or unique identifier
- Title or description of the record
- The individual, position or business unit accessing the record
- Date of record movements (including return to storage)

Tracking systems and procedures should also provide for the transfer of records between individuals when the record is not first returned (and tracked) back to the storage system. The National Archives Standard, *Tracking Records*, provides sample tracking forms and other mechanisms for controlled retrieval and access of records.

It is also good practice to keep an accurate record of when personal data is transferred or copied to another body, for example for data sharing purposes, and any conditions of use that are to be applied.

It is important not only to track records accessed but also to record levels of use, retrieval patterns and other statistics related to access. This information can be used to re-assess disposal and retention decisions, justify storage requirements and provide essential data about performance and resource requirements of the records management programme. Data to record with respect to record use include:

- Records used
- Individual or business area using the records
- Length of time and frequency of records accessed

It is a good idea to develop a single system to track records, record access statistics and monitor use so that location and use reports can be automatically generated.

Storage

Records storage facilities, together with handling and processing procedures, have a major impact on the authenticity and reliability of records as well as their preservation and protection. With paper records this is demonstrated through documented procedures and practices; with electronic records automated access controls and audit trails can be used. The aim is to provide records with a secure environment, which prevents unauthorised access, deters theft and vandalism and enhances the records' longevity. Where personal data is involved this will ensure compliance with the 7th data protection principle. It should also be noted that records, which need to be kept for longer, will require higher standards of handling and storage.

Records which are no longer frequently required for current business needs can be moved to storage which is more cost-effective, albeit less accessible. The need for access must be weighed up against business requirements and resources.

Whatever the solution adopted for record storage, good housekeeping and management is very important. Premises should be kept clean and tidy and they should be regularly inspected because early detection of maintenance issues will ensure threats to records are kept to a minimum and have minimal impact.

Electronic records must be subject to a back-up regime. This is usually the responsibility of IT support staff and involves taking a series of copies of records on the organisation's network (together with the software and programmes required to read the records). The backups must be kept off site at a location, which can be easily reached in an emergency. The series of backups will enable the whole system and the records on it to be reconstituted together with any additional records or edits to existing records in-between the full backup. The organisation should have a disaster recovery plan which includes retrieving electronic records in the event of a systems failure.

Environmental conditions

Whilst the record media should be selected to ensure the records' usability, reliability, authenticity and preservation for as long as required, record storage areas should be maintained at the appropriate temperature and humidity to prevent the records from physically deteriorating. Depending on their physical and chemical properties, records require different environments. For example paper, microform and electronic records all have slightly different temperature and humidity requirements. The National Archives Standard, *Storage of Semi-Current Records*, contains recommendations and references to appropriate British standards. In essence all records need to be kept cool and at a low relative humidity but there is also a need to maintain stability in the environment as fluctuations cause stress to the media, which is also damaging. Higher temperatures and greater humidity not only damage the media but also promote the growth of moulds, which corrupt and distort records. Electronic and audio-visual media is particularly susceptible to magnetic fields and may need additional protection, for more detail see the section on further guidance and information.

Flood and fire protection

Record storage areas should meet applicable fire regulations. Walls and doors should resist fire for two hours, there should be automatic fire and smoke detectors and staff should be trained in the use of fire extinguishers, which should be positioned in and near records storage areas. Fire officers and the local fire brigade should be consulted and informed of the need to protect records from both the effects of fire and of water and chemicals used to extinguish fire.

Water represents a risk to records as it can damage them and also a rise in humidity, particularly if coupled with a rise in temperature, will encourage mould growth on all media. Since basements and attics are especially prone to leaks and floods, records should not be stored in these areas. If there is no possibility of storing records where no water pipes run through, the pipes should be lagged. Flood detectors and alarms should be installed and storage areas should be regularly checked for leaks and for increased humidity levels.

Boxes and filing cabinets provide a measure of protection to records from flood and fire. Similarly shelving lifts records off the floor (and prevents them from standing in water in the event of a flood) and where the top shelf provides protection by acting as a "roof".

Security

Whether records are kept in filing cabinets in offices, in filing rooms adjacent to offices or in off-site accommodation appropriate access controls should be in place. This includes, if necessary:

- Sturdy construction of buildings
- Barred/secure windows
- Secure doors
- Guards or intruder alarms
- Controlled-access key system

Access to buildings containing record systems should only be given to staff. This practice provides evidence that the records have been kept securely and without any possibility of loss, tampering or damage: it can be assumed that records can for the most part be available to all staff in the team or department as record storage must facilitate access in accordance with the rate of use. There must also be a system in place to allow changes to access authorities as these will change over time.

Records that are sensitive should be subject to special storage arrangements, which include the use of locked filing cabinets, safes, locked filing rooms, secure servers and limited electronic access through password protection.

Migration and media replacement

Electronic records need to be subject to a preservation strategy that will ensure their continued viability through system change and upgrade. Electronic records in obsolete formats cannot be readily accessed and are at risk of becoming wholly inaccessible. They must therefore be migrated, which is a process that can call into question the authenticity and reliability of the record. The solution is to follow standards such as the BSI *Code of practice for legal admissibility and evidential weight of information stored electronically* which has guidance for documenting processes, which ensure continued viability of electronic records. Following these guidelines and documenting processes which convert or migrate records from one system to another will ensure that electronic records remain accessible, authentic, reliable and useable through system change. The documentation of such processes must be maintained as evidence throughout the life of the records.

Similarly, where digitisation and microfilming programmes are in place to maximise space or achieve other efficiencies in records management, appropriate documentation of conversion must be created and maintained.

Electronic records

The principles behind storage management for paper records hold true for records in all media. However with electronic records the lack of physicality due to centralised server storage can make it hard to ensure and/or demonstrate security. Therefore access permissions need to be set up and, if necessary, encryption and password protection should be invoked. However encrypted and password protected records can remain inaccessible without the keys or passwords for long after the need for that level of security has ceased so there should be procedures and guidance for reducing security after time has elapsed.

Audit trails must be activated and maintained to provide evidence not only of records accessed and by whom, but also of any changes to records or deletions. Electronic records are susceptible to corruption and data loss during refreshment and migration so they require procedures and practices that check and monitor their content and accessibility.

As a general rule, procedures for monitoring, accessing and handling electronic records should be issued, followed and documented to ensure those records are controlled and managed at all times.

Space management

With all records, regardless of their medium or format, storage space needs to be large enough to meet anticipated needs. Assuming that records will either be destroyed or transferred to a designated archives service, it is possible to calculate a finite amount of space to house your records. Estimates of storage needs should be based on the survey data elements covering quantities and growth rates.

Vital records and emergency plans

Vital records are those records which, in the event of an emergency or disaster, are most necessary to continue or reconstruct business and meet identified important organisational obligations: they are vital in ensuring the organisation can continue to function. Vital records should be subject to a vital records programme, which is a regime to identify them, protect them and make sure they can be readily accessed if needed.

A vital records programme will require some allocation of resources. Since records are unique, they cannot be replaced if they are stolen or destroyed – vital records protection and preparation of a recovery plan is, in effect, insurance for records.

Vital records management consists of:

- Identifying and listing vital records
- Establishing senior management agreement on vital functions and vital records
- Identifying potential threats and risks to recordkeeping and vital records
- Devising a strategy or system to protect vital records and ensure that the vital records inventory is kept current
- Developing and testing a vital record recovery plan for use in the event of a disaster
- Putting in place appropriate and adequate preventative measures to ensure that as far as possible disasters are avoided

Identifying vital records

Vital records can be identified as part of the record survey. Identification of vital records depends on a good understanding of the functions of your organisation, which will allow you to recognise the records, which support those functions. Remember that although staff may see certain records as vital to them in so far as they support their work, their functions may not be of a high priority in the event of an emergency. In identifying vital records, remember:

- Most vital records are still active
- Although copying vital records is the best strategy for protecting them, in some cases the original record will be vital for legal reasons
- Only 2-4% of an organisation’s records are likely to be vital: it is important to keep the records designated as vital to an absolute minimum to run an effective vital records programme

The following types of records are likely to be vital:

- Records of territorial boundaries and demarcations
- Multilateral treaties
- Memoranda of understanding
- Staff medical and personnel files
- Records which document legal and financial status
- Records which document the rights and obligations of citizens
- Records which document organisational assets
- Financial records which ensure solvency and accounting/finance functions (money owing, account status and statements, account access authorities, current staff payroll and benefit details, records allowing access to emergency funding)
- Records which authorise and support the organisation's main responsibilities and activities (policy documents, contracts, ownership records, delegations and authorisations, directives/instructions)
- Key administrative records (operating procedures, licences, permits, timetables, insurance policies)
- Records relating to buildings, doors, safes, sprinklers, alarm systems; personnel lists; building plans; security clearance records

Some records, such as staff contact lists and the emergency recovery plan itself, whilst not so important to the organisation's business recovery, will be crucial in the immediate aftermath of a disaster. These are known as emergency records and should be identified and be subject to contingency plans which ensure they can be readily accessed when required.

Organisational context

Vital records management, including confirmation of the inventory, must have senior management endorsement, as the organisation's successful continuity in the event of a disaster will depend upon having the relevant records to support vital operations and functions. The vital records programme must be integrated into the organisation's business continuity strategy, risk management and disaster plan.

Identifying potential threats and risks

The main risks and threats to current and semi-current records are:

- Fire
- Flood
- Terrorist activity
- Insect, pest and mould damage
- Poor handling

- System interruptions and crashes
- System hacking and viruses
- Theft

Preventative measures

Many of the threats and risks to records can be reduced by instituting measures and procedures, which will, as far as possible, prevent threats becoming reality. The section above on record storage gives advice and guidance on suitable storage conditions and how to prevent or detect adverse events such as fire or flood as early as possible. Insect, pest and mould damage can be prevented by ensuring the environment where records are stored is kept cool, dry and clean.

Theft can be prevented by ensuring the storage area is robust and secure and by controlling access. Poor handling can be improved by staff training and written guidance and procedures. The threat of terrorist activity to records can be reduced in the same way as the threat of terrorism to other business and personal areas: by vigilance and investigation or reporting of unusual behaviour and incidents.

Threats to electronic records can be more common – and therefore perhaps more routinely prevented and recovered from. The most common way of protecting electronic records is by backing up the system regularly so that if the system goes down and/or records are lost, most of them can be recovered from the back up. Preventative measures include:

- Following best practice and adopting standards to ensure good quality storage media
- Ensuring storage space has enough redundancy to enable a parallel system to run in the event of the primary system going down
- Adopting data security standards
- Complying with electronic media storage standards
- Current anti-virus and fire wall protection

Protecting vital records

The most effective way to protect vital records is by copying them and sending the copies off site. The off site storage needs to be subject to the same standards and specifications as other storage the organisation's records. It needs to be far enough away from the organisation's main premises to ensure that it will not be affected by the same disaster – but close enough to access the copy records if necessary.

Vital records need to be subject to a programme of copying, transfer to off site storage and updating as records grow non-current and their place is taken by new vital records. With records in microform, audio-visual or electronic formats the equipment and software necessary to access the records needs to be retained off site as well. As current systems are upgraded, provision will need to be made to ensure that operating systems and software required to access older vital records are available – or the records may need to be recopied.

It is possible to protect vital records other than by sending copies off site: this involves providing secure and fire proof storage which would protect the records for long enough to survive a fire and its aftermath. This strategy should not be adopted unless no other protection method is possible due to lack of resources or other issue specific to your organisation.

Vital record recovery

In the event of a disaster it will be necessary to access vital records that have been copied and sent off site. As with any recordkeeping system, efficient retrieval and access will depend upon the quality of the system. A plan should be developed and implemented to manage the recovery of vital records. The plan should include:

- Responsibilities and conditions for activating the plan
- Contact names and details
- Procedures for accessing off site storage, including written directions and maps
- Priorities and procedures for return of records to the organisation's operational centre
- Procedures for reconstituting records in non-paper formats

Once the plan has been developed and approved, all records management staff (or if there is no records management team, volunteer colleagues) should be trained in implementing the plan. Training should include as far as possible a simulation of an emergency situation.

Review and amendment

Periodic review of the system will ensure that all records are covered by the records management programme and that the procedures and practices are not only complied with but that they are appropriate and effective. There are a number of ways of carrying out review:

- Ongoing review whereby the system's performance is monitored and documented, for example by collecting and analysing use statistics or system failures if for instance a record cannot be easily located
- Periodic review where every year or so a comprehensive review of the system is conducted to investigate the system's strengths and

weaknesses (this can be done by the records management team or an external agency)

- Formal audit where internal or external audit personnel investigate the system

The National Archives' publication, *Complying with the Records Management Code: Evaluation Workbook and Methodology* gives detailed guidance on reviewing records management programmes.

Once the review has been completed, any recommendations for modification or change of the records management programme's policy, procedures and practice should be implemented. Full documentation on the review process should be maintained to provide evidence of the system's reliability.

Margaret Crockett
Consultant Archivist and Records Manager
August 2006

Further Guidance and Information

Standards

- *ISO 15489-1:2001 Information and documentation – Records Management (Part 1 General)*
- *PD ISO/TR 15489-2:2001 Information and documentation – Records Management (Part 2: Guidelines)*
- *BIP 0008:2004 Code of practice for legal admissibility and evidential weight of information stored electronically*
- *BIP 0009:2004 Legal admissibility and evidential weight of information stored electronically. Compliance workbook*
- *BS 7799, Code of Practice for Information Security Management*
- *BS 4783, Storage, transportation and maintenance of media for use in data processing and information storage*
- *BS 1153, Processing and storage of silver-gelatine-type microfilm*
- *BS 5454 Recommendations for the storage and exhibition of archival documents*

Guidance

- The National Archives Best Practice Guidance: *How to Complete an Information Survey of Records*

  http://www.nationalarchives.gov.uk/recordsmanagement/advice/pdf/best_complete_survey.pdf

- The National Archives Electronic Records Toolkit: *Compiling an Inventory of Electronic Record Collections*

  http://www.nationalarchives.gov.uk/electronicrecords/advice/pdf/inventory_toolkit.pdf

- The National Archives Records Management Standard: *Tracking Records*

  http://www.nationalarchives.gov.uk/recordsmanagement/advice/pdf/stan_tracking.pdf

- The National Archives Records Management Standard: *Business Recovery Plans*

  http://www.nationalarchives.gov.uk/recordsmanagement/advice/pdf/stan_business_recovery.pdf

- The National Archives: *Management, appraisal and preservation of electronic records Vol 2: Procedures* http://www.nationalarchives.gov.uk/electronicrecords/advice/pdf/procedures.pdf

- *Complying with the Records Management Code: Evaluation Workbook and Methodology*

  http://www.nationalarchives.gov.uk/documents/record_management_compliance.pdf

- *Requirements for Electronic Records management Systems* http://www.nationalarchives.gov.uk/electronicrecords/reqs2002/

- *Requirements to sustain electronic information over time* http://www.nationalarchives.gov.uk/electronicrecords/reqs_sustain.htm

- *Sustainable electronic records: Strategies for the Maintenance and Preservation of Electronic Records and Documents* http://www.nationalarchives.gov.uk/electronicrecords/advice/pdf/preservation_toolkit.pdf