An Introduction to Digital Records Management

To support the continuing flow of business, comply with the regulatory environment and provide necessary accountability, organizations should create and maintain authentic, reliable and usable records, and protect the integrity of those records for as long as required.1

Organizations are increasingly reliant on information communications technology (ICT) as a crucial component of business operations. As a result, information is often partially or fully in electronic form.

The main objective of this article is to introduce the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records in an electronic environment, based on international standards ISO 15489, part 1 and part 2.

REGULATORY ENVIRONMENT

All organizations need to identify the regulatory environment that affects their activities and the requirements to document their activities. The policies and procedures should reflect the application of the regulatory environment to the organization’s business processes. An organization should provide adequate evidence of its compliance with regulations in the records of its activities.2

The regulatory environment might consist of:

- Statutes, case laws and regulations governing the sector-specific and the general business environment, including laws and regulations relating specifically to records, archives, access, privacy, evidence, electronic commerce, data protection and information
- Mandatory standards of practice
- Voluntary codes of best practice
- Voluntary codes of conduct and ethics
- Identifiable expectations of the community about what constitutes acceptable behavior for the specific sector or organization

For example, in Bosnia and Herzegovina:

- The taxation retention period for the original application for entry into a unified system is five years from the date of submission of the application, while the data entered into the database in electronic form have to be kept permanently
- Records maintained by the bodies responsible for issuing permits for the movement of weapons and military equipment must be kept permanently
- Records obtained pursuant to an act against money laundering and financing of terrorist activities must be kept at least 10 years after identification, the conduct of transactions, closing the account or termination of the business relationship, etc.

The nature of the organization and the sector to which it belongs determine which regulatory elements (individually or in combination) are most applicable to the organization’s records management requirements.

RESPONSIBILITIES

ISO 15489 defines “records management” as a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.3 The term “records” is defined as information created, received and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.

Records management responsibilities and authorities should be defined, assigned and promulgated throughout the organization so that, where a specific need to create and capture records is identified, it is clear who is responsible for taking the necessary action.
POLICY
Organizations should define and document a policy for records management. The objective of the policy should be the creation and management of authentic, reliable and usable records that are capable of supporting business functions and activities for as long as they are required. Organizations should ensure that the policy is communicated and implemented at all levels in the organization.4

However, a policy statement on its own will not guarantee good records management. Critical to its success are endorsement and active and visible support by senior management as well as allocation of the resources necessary for implementation.5

A records management policy statement sets out what the organization intends to do and sometimes includes an outline of the program and procedures that will achieve those intentions. The policy statement should refer to other policies relating to information (e.g., those on information systems policy, information security or asset management), but should not seek to duplicate them. It should be supported by procedures and guidelines, planning and strategy statements, disposition authorities, and other documents that together make up the records management regime.6

CHARACTERISTICS OF RECORDS
A record should correctly reflect what was communicated or decided or what action was taken. Records management policies, procedures and practices should lead to authoritative records that have the following characteristics:7

• **Authenticity**—An authentic record is one that can be proven to:
  - Be what it purports to be
  - Have been created or sent by the person purported to have created or sent it
  - Have been created or sent at the time purported

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

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

If the information is going to be used in a criminal proceeding, organizations must be able to identify who has had access to a particular record at any given time from collection, to creation of the evidence copy, to presentation as evidence. The evidentiary weighting of records will be substantially reduced if the chain of custody cannot be adequately established or is discredited.8

• **Usability**—A usable record is one that can be located, retrieved, presented and interpreted. It should be directly connected to the business activity or transaction that produced it. The contextual linkages of records should carry the information needed for an understanding of the transactions that created and used them. It should be possible to identify a record within the context of broader business activities and functions. The links between records that document a sequence of activities should be maintained.

ELECTRONIC RECORDS
Traditionally, corporations have considered the evidentiary implications of electronic documents only when they are required for litigation, or when forensic practitioners have focused on collecting IT evidence as artifacts of an investigation. However, successful management of IT evidence is much broader than a mere postmortem activity, and the IT evidence must be managed continuously throughout the records life cycle.9

In an electronic business environment, adequate records will not be captured and retained unless the system is properly designed.10 It is important to note that media for storing digital data, and also formatting the data, are subject to change. For example, a significant number of documents archived by an organization over the past decade may now be largely illegible and incomprehensible because of damage to storage media or because the older file formats are incompatible with newer, currently used formats.
Sometimes digital records need to be archived for a certain period of time, so that, if necessary, they can be presented during the court process. With the current pace of technological development, it is very likely that problems with outdated storage media or formats of data can make the process of returning data very expensive. This can be because of the need to complete the conversion of all data to new media as technology develops or because of the need to keep the old equipment and software.

Digital evidence as a form of physical evidence creates several other challenges:

- It is a messy, slippery form of evidence that can be difficult to handle.
- Digital evidence is generally an abstraction of some event or digital object.
- The fact that digital evidence can be manipulated easily raises additional challenges for digital investigators.
- Digital evidence is usually circumstantial, making it difficult to attribute computer activity to an individual.

Therefore, digital evidence can be only one component of a solid investigation.

SECURITY

A formal instrument that identifies the rights of access and the regime of restrictions applicable to records is a necessary tool to manage records in organizations of all sizes and jurisdictions. Reasonable security and access depend on both the nature and the size of the organization, as well as the content and the value of the information requiring security.

Access to records may be restricted to protect:

- Personal information and privacy
- Intellectual property rights and commercial confidentiality
- Security of property (physical, financial)
- State security
- Legal and other professional privileges

Information security is key when discussing legal admissibility issues. The main discussion on this topic is likely to be the authenticity of stored information. When the electronic information was captured by the storage system, was the process secure? Was the correct information captured, and was it complete and accurate? During storage, was the information changed in any way, either accidentally or maliciously? When responding to these questions, information security implementation and monitoring are key to demonstrating authenticity.

Proof of compliance with the recommendation of ISO/IEC 27001:2005 may provide helpful supporting evidence in court. It indicates that the organization has exercised its duty of care, and will assist the court in assessing the authenticity and integrity of information.

RECORD STORAGE DECISIONS

The decision to capture a record implies an intention to store it. Appropriate storage conditions ensure that records are protected, accessible and managed in a cost-effective manner. The purpose served by the record, its physical form, and its use and value dictate the nature of the storage facility and services required to manage the record for as long as it is needed.

It is important to determine efficient and effective means of maintaining, handling and storing records before the records are created and, then, to reassess storage arrangements as the records’ requirements change. It is also important that storage choices be integrated with the overall records management program.

Backup copies of essential business records should be taken regularly. Adequate backup facilities should be provided to ensure that all essential business information can be recovered following a disaster or media failure.

Backup information should be given an appropriate level of physical and environmental protection consistent with standards applied at the main site.

Technologies used for the initiation and control of the secure transfer of information between the organization and an archive, whether the archive is operated in-house or by a third-party service provider, should be documented. Using cryptographic techniques can be one way to ensure authentication of the sender and the electronic document.

The method of ensuring that received and subsequently stored information is identical to that originally sent should be documented. Information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance, when sending record media to another location, e.g., the off-site backup facility.

The following controls should be applied to safeguard computer media being transported between sites:

- Reliable transport or couriers should be used. A list of authorized couriers should be agreed upon with management, and a procedure to check the identification of couriers should be implemented.
• Packaging should be in accordance with manufacturers’ specifications and should be sufficient to protect the contents from any physical damage likely to arise during transit.

• Special controls should be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification. Examples include:
  – Use of locked containers
  – Delivery by hand
  – Tamper-evident packaging
  – In exceptional cases, splitting of the consignment into more than one delivery and dispatching contents by different routes
  – Use of digital signatures and confidentiality encryption

Organizations should conduct a risk analysis to choose the physical storage and handling options that are appropriate and feasible for their records. It is important to specify the relationship between the risks and the selected options for treating them. The selection of storage options should take into account access and security requirements and limitations in addition to physical storage conditions. Records that are particularly critical for business continuity may require additional methods of protection and duplication to ensure accessibility in the event of a disaster.

Risk management also involves development of a disaster recovery plan that defines an organized and prioritized response to the disaster, planning for the continuance of regular business operations during the disaster and making appropriate plans for recovery after the disaster.

All activity is susceptible to disruption from internal and external events, such as technology failure, fire, flood, utility failure, illness and malicious attack. ICT continuity management provides resilience to prevent ICT disruptions and to recover when disruptions occur.

Disruption to ICT can be a huge risk; it can damage an organization’s ability to operate and undermine an organization’s reputation. The consequences of a disruptive incident vary and can be far-reaching, and might not be immediately obvious at the time. BS 25777 may help organizations plan and implement an ICT continuity strategy.

**DIGITAL STORAGE**

The storage of records in electronic form necessitates the use of additional storage plans and strategies to prevent loss:

• Backup systems are a method of copying electronic records to prevent loss of records through system failures. Such systems ought to include a regular backup schedule, multiple copies on a variety of media, dispersed storage locations for the backup copies, and provision for both routine access and urgent access to backup copies.

• Maintenance processes may be needed to prevent physical damage to the media. Records may need to be copied to newer versions of the same media (or other new media) to prevent data erosion.

• Hardware and software obsolescence may affect the readability of stored electronic records.

**USE AND TRACKING**

The tracking of records usage within records systems is a security measure for organizations. It ensures that only those users with appropriate permissions are performing authorized records tasks. The degree of control of access and recording of use depends on the nature of the business and the records it generates. For example, mandatory privacy protection measures in many jurisdictions require that the use of records holding personal information be recorded.

**CONTINUING RETENTION**

Records identified for continuing retention need to be stored in environments conducive to their long-term preservation. Preservation strategies for records, especially electronic records, may be selected on the basis of their ability to maintain the accessibility, integrity and authenticity of the record over time, as well as for their cost-effectiveness.

Preservation strategies can include copying, conversion and migration of records:

• Copying is the production of an identical copy within the same type of medium (paper/microfilm/electronic), e.g., from paper to paper, microfilm to microfilm, or the production of backup copies of electronic records (which can also be made on a different kind of electronic medium).

• Conversion involves a change of the record’s format but ensures that the record retains the identical primary information (content). Examples include microfilming of paper records, imaging and change of character sets.

• Migration involves a set of organized tasks designed to periodically transfer digital material from one hardware/software configuration to another, or from one generation...
of technology to another. The purpose of migration is to preserve the integrity of the records and to retain the ability for clients to retrieve, display and otherwise use them. Migration may occur when hardware and/or software becomes obsolete, or it may be used to move electronic records from one file format to another.

Information may be stored for a considerable length of time and for longer than the lifetime of the current technology. Thus, to ensure the integrity of stored information, it is important to plan from the outset that the information may be subject to a migration process. Such a process may involve a change of media, computer hardware or software.

As a rule of thumb, a storage media migration process will occur approximately every five years. A reliable methodology for dealing with this potential problem is to ensure that data files are stored in an industry standard format, or that viewers for each stored format are maintained. It is also recommended that a restricted number of formats is used for long-term storage, to reduce future storage migration issues.

When making provisions for migrating data files, it is important to include all relevant metadata, including index data and audit trails. These additional data should also be migrated to the new technology without loss of integrity. Records, including audit trails, should be kept of any migration process to which stored data have been subjected, to allow the integrity of the data to be demonstrated beyond any reasonable doubt at any time in the future.24

As new technologies become available, other methods may be used to retain electronic records for long periods.

Where records are transferred to an external storage provider or an external archives authority, documentation that outlines continuing obligations to maintain the records and manage them appropriately should be formally established by agreement between the custodian(s) and the transferring party.

**PHYSICAL DESTRUCTION**

Physical destruction of records is carried out by methods appropriate to their level of confidentiality.

Records in electronic form can also be destroyed by reformatting or rewriting, if it can be guaranteed that the reformatting cannot be reversed. Deleting instructions is not sufficient to ensure that all system pointers to the data incorporated in the system software have also been destroyed. Backups containing generations of system data also need to be reformatted or rewritten before effective destruction of electronic information is complete. Physical destruction of storage media is an appropriate alternative, especially if deletion, reformatting or rewriting are either not applicable or are unsafe methods for destroying digital information (for instance, information stored on WORM [Write Once Read Many] media).25

It may be necessary to amend, dispose or expunge (i.e., remove without any trace of it ever existing) specific records from information management systems, perhaps to comply with a court order and/or to meet requirements of data protection legislation. The process should be auditable, such that the disposal of a particular document, for example, can be proven. It is also important to obtain any necessary authorization for such processes before implementation.

When positive removal of information from the system is required, identification and deletion of all copies of the information (including backup media) ensure that necessary action has been taken.26

The principles of good practice in record keeping are of value even if the need to produce electronic records in court never arises. The effort and resources required to comply bring business benefits, whether the organization is in court or not, in increasing organizational efficiency and improving control over information assets.

**EVIDENTIAL WEIGHT**

Records managers need to be aware of the potential for legal challenge when documents are presented in evidence to a court of law. If the integrity or authenticity of a record is called into doubt in court by suggestions of tampering, incompetence, improper system functionality or malfunction, the evidential weight or value put on the document by the court may be lost or, at least, reduced, creating a detriment to the case.

Records managers need to have readily available evidence to demonstrate and prove the organization’s compliance with legislation, policies and procedures throughout the life of the system. It should also be possible to show that the system was operating as intended in accordance with the organization’s normal business practices. This evidence would be available from records of the monitoring and auditing of system processes.

Because electronic records can be altered easily, opposing parties often allege that computer records lack authenticity because they have been tampered with or perhaps changed...
after they were created. Courts have rejected arguments that electronic evidence is inherently unreliable because of its potential for manipulation. As with paper documents, the mere possibility of alteration is not sufficient to exclude electronic evidence. When specific evidence of alteration is absent, such possibilities go only to the evidence’s weight, not its admissibility.27

The existence of an airtight security system (to prevent tampering) is not, however, a prerequisite to the admissibility of computer printouts. If such a prerequisite did exist, it would become virtually impossible to admit computer-generated records; the party opposing admission would have to show only that a better security system was feasible.

CONCLUSION

Records contain information that is a valuable resource and an important business asset. A systematic approach to the management of records is essential for organizations and society to protect and preserve records. A records management system results in a source of information about business activities that can support subsequent activities and business decisions, as well as ensure accountability to present and future stakeholders.

ICT brings potentially increased, or at least different, risks in terms of civil or criminal wrongdoing and organizations need to be able to protect themselves against those risks. Failure to do so raises governance and accountability issues for which the management of the organization could be held responsible. The fact that the electronic environment is unfamiliar territory does not excuse directors from liability based on lack of knowledge.

One way of proactively addressing electronic records management is to follow a standardized records management process, such as the one recommended in international standard ISO 15489.

ENDNOTES

2 Ibid.
3 Ibid.
4 Ibid.
6 Ibid.
7 Op cit, ISO 15489-1:2001
8 Standards Australia International, HB 171-2003, Guidelines for the management of IT evidence, 2005
9 Ibid.
10 Op cit, ISO 15489-1:2001
15 Op cit, Shipman
18 Op cit, Shipman
19 Op cit, ISO/IEC 17799:2005
20 British Standards Institution, BS 25777:2008, Information and communications technology continuity management, 2008
22 Ibid.
23 Ibid.
24 Op cit, Shipman
26 Op cit, Shipman