DISASTER & RISK MANAGEMENT IN RM & INFORMATION MANAGEMENT

BY

ERICK OGOLLA

OUTLINE

- Records Management Programme
- Effective Disposal of Business Records
- Vital Records Programming
- Conclusion

Introduction to Recordkeeping Requirements

- The nature of an organization, and the context in which it operates, dictate the type of evidence of its activities it needs to create, the form that evidence takes, how long the evidence should be retained and what access should be provided to that evidence over time.

- These recordkeeping requirements are identified through a systematic analysis of the organization's business needs, legal and regulatory obligations, and broader community expectations, as well as an

- Recordkeeping requirements influence the type of record to be produced as evidence of business activity and how such records are to be maintained.

- Some recordkeeping requirements are stated explicitly in laws, regulations and other instruments of authority, while others are implied by the environment in which the organization operates.

For example, a recordkeeping requirement may direct:

- that a record be created, or particular information be captured;
- that recorded information be retained for a specified period;
- conditions surrounding disposal of the recorded information;

Nurturing Effective Records Management Programme (Records Management Process)

- The purpose of a recordkeeping system is to manage records throughout their life cycle, i.e. from the creation or receipt of a record, through its useful life to its final disposal.

- The records management processes in different stages of records life cycle include:
  - records capture;
  - registration;
  - records classification;
  - records storage;
  - access;
  - tracking; and
  - records disposal.

- Although the processes described above are presented as if in a sequence, it should be noted that in some recordkeeping systems, particularly electronic recordkeeping systems, some of them may take place simultaneously.
- For example, records capture, registration and classification are often carried out as an integrated series of actions) or in a different order (e.g. access control and tracking should be implemented for records during their whole life) from that described.

- Before examining the requirements of each records management process, an organization should first determine documents to be captured as records into a recordkeeping system and how long to retain records based on the values attached to the records.

- The value attached to records include;
  - Legal;
  - Administrative;
  - Evidential;
  - Historical etc.

Effective Disposal of Business Records (Regular disposal of records)

- Approved records retention and disposal schedules will not serve their intended purposes if they are not followed.
- An organization should initiate regular disposal of records in accordance with approved records retention and disposal schedules.
- To safeguard against premature disposal of records and destruction of records having archival value, disposal of records should be properly authorized in advance by a sufficiently senior staff in the organization.

- Specifically, the responsible staff of the organization should ensure that;
  - the retention and disposal requirements specified in the respective disposal schedules, and any governing legislation have been complied with; and
  - that there is no outstanding actions on any of the records.
- Care should be taken to minimize the risk of inadvertent, unauthorized destruction of records during the disposal process.

- The disposal process should be properly supervised by adopting the following procedures:
  - prepare an accurate list of records to be disposed of. Records (including those stored off-site) to be disposed of should be physically checked against the list to ensure its accuracy;
  - ensure the completeness (e.g. no enclosures of files are missing) of records having archival value;
  - segregate records approved for destruction to ensure that they do not mix up with those pending approval;
  - destroy classified records and records containing sensitive information (e.g. personal data) in accordance with the relevant requirements e.g. shredding the records to the required size to prevent reconstruction; and
  - document the procedures for accountability.

Records Monitoring and Process Auditing

- An organization should undertake compliance monitoring regularly to ensure that the records management processes and controls are being implemented according to the organizational policies and requirements.
- This is to ensure that its records management programme is functioning effectively.
- An organization should conduct regular review of its records management programme and practices to:
  - assess its compliance with key records management functions and requirements; and
  - identify areas requiring improvement with regard to desirable best practices and formulation of plans to implement improvement measures.

- The review and recommended improvements should be endorsed by the management.
- An organization should also consider the arrangements to deal with cases involving loss or unauthorized destruction of records.
- It should properly follow up any loss or unauthorized destruction of records; including ascertaining the facts and identifying the circumstances leading to the loss or unauthorized destruction, taking steps to prevent recurrence and taking disciplinary action or administrative action as appropriate.

Vital Records Programming (Protecting Vital Records)

- **What are Vital Records?**
- Vital records are those records containing information essential to the continued and effective operation of an organization in the event of an emergency or a disaster e.g. a prolonged electricity blackout, a serious flood, a blaze and an earthquake.
- Although an organization may take precautionary measures to protect records from perils in their day-to-day operations, even foolproof measures may

- Therefore, vital records protection should be put in place to reduce the risks of loss of records and to mitigate the possible adverse effects on the operation of organizations during and immediately after an emergency or a disaster.

- Vital records are specific to each organization having regard to its unique functions and responsibilities.

- In general, vital records are required to:
  - deal with emergencies and disasters e.g. building plans and rescue plans;
  - continue and/or resume business operation during and/or after emergencies and disasters e.g. operational manuals of mission-critical information systems;
  - protect and/or re-establish legal, financial and functional status e.g. property and revenue records; and
  - preserve the rights of the organization, its employees and clients as well as members of the public e.g. payroll and medical records.

- It is the responsibility of an organization to identify and protect (e.g. through duplication and/or off-site storage) its vital records to ensure uninterrupted operation of major business functions.

- If appropriate, a comprehensive vital records protection programme should be established.

Guidelines on Establishing a Vital Records Protection Programme

- Organizations wishing to establish their vital records protection programmes should follow the major procedural steps below:
- conduct a risk analysis to identify potential disasters/hazards (e.g. fire and flooding) that need to be addressed;
- identify vital records and document essential information about those vital records, e.g. responsible party for maintaining and protecting records, records storage medium, volume, location etc.;

- determine records protection methods (e.g. duplication of paper records through means such as scanning and microfilming for off-site storage and dispersal of records in different office locations);
- prepare or identify sources of supplies, equipment and services for records protection and recovery; and
- conduct staff training, programme testing and revision.

- Amongst these major procedural steps, selection of vital records and adoption of proper protection methods are of significant importance and require thorough review and study.

Selection of Vital Records

- Identification and selection of vital records requires a comprehensive review on records kept by an organization so as to determine what records warrant protection under the programme.
- Records management staff should always bear in mind that vital records protection programme has to be well-justified and cost-effective.
- They should not incline to classify records as vital records simply for fear of potential loss/damage to those records.

- To select vital records, records management staff may, in consultation with subject officers, identify records that meet the purposes and protect the interests set out and select only those records that meet the following criteria:

i. records which are absolutely needed without which your organization is unable to function properly;

ii. records which are irreplaceable or can only be replaced/reconstructed in a costly and lengthy way; and

iii. finding aids, e.g. records classification scheme and indexes of records selected for protection as part of the vital records to facilitate prompt retrieval of records during and after an emergency or a disaster.

Protection Methods

- There are various methods to protect vital records. They should be adopted having regard to the business needs (e.g. records of rescue plans may need to be kept on site to facilitate timely retrieval during and after an emergency or a disaster), cost implications and expertise and skills required of the organization.
- Three common methods for protecting vital records are listed below for reference:
  - dispersal/off (site storage: prepare extra copies of records when the records are created and store them in location(s) away from the organization's primary place of business;

- duplication: prepare extra copies of records when they are created, or through scheduled reproduction such as microfilming and scanning at regular intervals specifically for protection or back-up purposes to support normal business;
- on-site protection: protect vital records in the primary place of business by use of special facilities and equipment such as fire resistant safes and records vaults (A vault is a fire-resistant enclosure constructed within an office building to protect large quantity of vital records stored in a non-fire-resistant building).

The criteria are not exhaustive. An organization may take into account its own business and operational needs to add, modify and/or delete the criteria.

- In addition, appropriate equipment and proper environmental conditions should be provided and used to protect vital records, particularly for those stored in fragile media such as microfilm and magnetic tapes and optical disks, to ensure the preservation of vital records for as long as required.
- With the increasing use of computerized information systems, including an ERKS to manage records, there is good potential for organizations to enhance their capability of protecting electronic vital records in a cost-effective manner.

- Unlike vital paper records which require considerable resources and efforts to duplicate or microfilm them for off-site storage, vital electronic records are far more convenient to be backed up for off-site storage in a large volume through automated processes.

- Functionality for protecting electronic vital records can be incorporated into information systems during system development or system upgrading/enhancement.

Management of Electronic Documents

- Electronic records are increasing as a percentage of organization's total records volume. Since they exist in a micro-format and a machine is needed to identify, retrieve and read them, managing electronic documents and electronic mail messages (referred to as "electronic documents") calls for requirements different from those that manage paper-based records.

- Electronic documents received and created while conducting business are considered official records and, as such, may be accessed in response to appropriate act, litigation, and operations. At the same time, most electronic documents are transitory and must be destroyed immediately after their usefulness has expired.

- This procedure aims to ensure that electronic document practices comply with industry standards and legislation, which include:
- Ensuring that electronic documents are verifiable as evidence (i.e., not altered)
- Destroying, with approvals, electronic documents when their use has expired and in accordance with the records retention schedules (i.e., not destroying them prematurely or keeping the documents for too long)
- Sending electronic documents to the official repository as indicated in Records policy; either:
  - Printing and filing in the paper-based records system those records for which a paper file is required according to the Directory of Records (e.g., for certain legal contracts), or
  - Submitting the electronic document to the custodian for the electronic document library.

- The Canadian General Standards Board (CGSB) has a standard for electronic records (CAN/CGSB-72.34).
- This standard is also compatible with an International Standards Organization (ISO) standard on records management (ISO 15489).
- E-mail messages in which the content is of a personal nature are not records in organizations and should be considered transitory in nature.
- Transitory electronic documents must be destroyed immediately after their usefulness has expired.

Electronic Documents in Business Processes

- Departments that rely on electronic documents to support business processes need to:
  - Document the business process in which electronic records support the business activity, stating how the process demands that electronic documents be managed.
  - Conduct regular audits and ensure the security of the information system
  - Document procedures for: imaging and capture of information, security, and audit trail of changes to the electronic documents
  - Demonstrate that the records in question are treated in a manner consistent with other records in organizations (e.g., demonstration of routine rather than ad-hoc records destruction)
  - Ensure that the structure (layout or format and links to attachments), content (the information contained in the message), and the context (information pertaining to the sender and recipients and transmittal date) are retained as evidence of business transactions.
  - Create appropriate indexing data concerning the document ("meta-data") and enter the meta-data into a suitable database.

Microfilming

- Microfilm reduces records storage space requirements by 98% and allows a low-cost back-up to be produced for vital records for the long term.
- The cost of filming documents is $.10 to $.25 per page plus the document preparation, quality assurance, and indexing time.
- It is economical to film paper-based records that must be retained for at least 10 years.
- Microfilm that is produced to archival standards will last more than 100 years.

Digital Imaging (or “Imaging”)

- Digital imaging involves scanning a paper or film original document into a digital format.
- The cost of digitizing documents is $.15 to $.25 per page, plus the document preparation, quality assurance, and indexing time.
- It is economical to digitize paper-based records when the business process efficiencies outweigh the costs of digitizing.
- Digital images that need to be retained for more than five years will need to be migrated to new technology standards as hardware and software change.
- Therefore, the future costs and responsibilities of migrating the digital images must be considered in the cost and benefit analysis.

CONCLUSION?

THANK YOU FOR LISTENING!

Q&A SESSION