KZN Archives and Records Service Conference 2014

Prevention is better than cure:

Understanding records risk as a first step to disaster planning

Paul Mullon
paulm@corconcepts.co.za
083 273 6087

Agenda

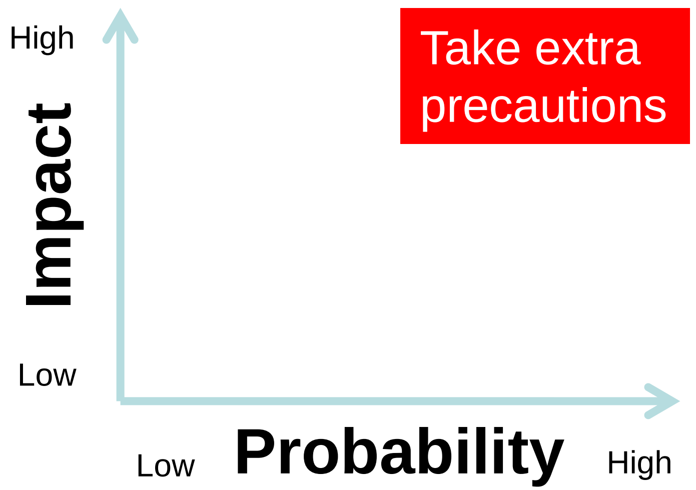
- Developing a roadmap for managing records risk
- Conducting a risk analysis
  - Areas of uncertainty
  - Likelihood of events
  - Impact of events
- Responding to risks

A roadmap for Records Disaster Prevention and Recovery

- Understand your records
  - Create a records inventory
- Initiate a formal vital records (or records risk) programme
  - Include records on all mediums
  - Cross networks, systems and databases
- What are vital records in YOUR business?
  - Titles
  - Descriptions
  - Rationale for inclusion
  - Business unit responsible
  - Method of protection used
- If no Vital records programme , ask which records should be included?

Risk analysis

- Internal
- External
- Natural
- Malicious and deliberate
- Accidental
- Careless work procedures



Risk Probability and Impact

Impact of loss or damage		Low (1)	Medium (2)	High (3)
	High (3)	• Protect vital records • Recovery procedures included in BCP	• Reduce risk where possible • Protect vital records • Recovery procedures included in BCP	• Reduce risk • Protect vital records • Recovery procedures included in BCP
	Medium (2)	• Recovery procedures for important records included in BCP	• Reduce risk where possible • Recovery procedures for important records included in BCP	• Reduce risk • Recovery procedures for important records included in BCP
	Low (1)	• Accept and monitor risk	• Protect useful and important records through management procedures	• Protect useful and important records through management procedures
		Probability of loss or damage		

Risk assessment

- What records are located where?
- Which hazards are a real threat
- Are records included in Business Continuity plans
- What cost to reconstruct files?
- Back-up and recovery procedures?
- What business cost of lost records?
- What legal cost of lost records?
- What cost of incorrectly retained records?

Risk identification
Context: External factors

- Legal and Regulatory Context
  - Is a process in place that monitors changes in legislation, regulatory environment and standards framework?
  - Are the capacities present or attainable to translate the changes in external regulatory environment into organization’s records management policies?
  - Can the records management change of terms in third-party service contracts?

Risk identification
Context: External factors

- Changes in Cultural context
  - Is records management embedded in the organizational culture?
  - Can the records management change of terms in third-party service contracts?

Risk identification
Context: External factors

- Economic/business environment
  - Will there be adequate funding and staffing for the records management program if the economic environment of the organization changes?
  - Can the records management program respond quickly to pressure to cut costs of services?
  - Is the records management program prepared for new (service) opportunities and technologies?
  - Are there processes in place to identify technological changes that can impact the organization?

Risk identification
Context: External factors

- Physical Environment and infrastructure
  - Is there a process in place to monitor the likelihood of relevant environmental concerns?
  - Are back-up copies of important digital information held in other/off-site locations?
  - Can you continue if there is no power?
  - Have physical precautions been taken against most likely local natural
  - Are disaster plans in place and tested regularly?
  - Are awareness briefings of disaster recovery plans regularly provided and updated to relevant staff?

Risk identification
Context: External factors

- External security threats
  - Are adequate information security measures put in place to protect the records system from unauthorised access and malicious damage?
  - Are back-up copies of important digital information held offsite on a separate network?

Risk identification
Context: Internal factors

- Organisational change
  - Has the ownership of records from parts of the organization that are undergoing change been established?
  - Have the records been retained and records management policies consistently applied to them?
  - Are appropriate contractual conditions in place for ownership, retention and control of records in outsourcing, off-shoring or cloud arrangements?
  - Is a process in place to review and update the records management policies at regular intervals?

Risk identification
Context: Internal factors

- Technology changes
  - Are processes in place to ensure that records and their metadata are fully migrated when new technologies are introduced and checks for information loss or corruption exist.
  - Are processes in place to prevent unauthorised disposal of records, or retention of records that are no longer needed when systems are migrated or upgraded?

Risk identification
Context: Internal factors

- People and competencies
  - Are staff aware of policies and procedures of the records program?
  - Are top management involved in the records program?
  - Are recordkeeping responsibilities included in all staff job descriptions?
  - Are processes in place to ensure transfer of vital skills and operational know-how among records management program staff?
  - Is a continuous training program available for staff of the records program?
  - Is a monitoring process in place to map and assess skills and competencies among the staff of the records program?

Risk identification
Context: Internal factors

- Finances, Facilities and Materials
  - Is the records function adequately staffed and funded?
  - Are records storage areas properly equipped?
  - Proper shelving?
  - Proper consumables – boxes, files?
  - Fire prevention, detection, suppression?
  - Protection from water?
  - Protection from pests?
  - Do records get into the care of records staff?

Risk identification
Systems

- Maintenance
  - Are systems frequently changed?
  - Are administrators adequately skilled?
  - Are suppliers competent?

Risk identification
Systems

- Sustainability and continuity
  - Are backups conducted frequently?
  - Is there a disaster recovery site?
  - Are systems in place to ensure usability over time?

Risk identification
Systems

- Interoperability
  - Are all records systems documented?
  - Can be records be found across systems?
  - Is metadata complete and accurate in all systems?

Risk identification
Systems

- Security
  - Are information security policy and controls in place governing the access to and use of records and records systems by employees, contractors and third parties?
  - Are security procedures in place for changing user access rights to systems when employees change or terminate employment?
  - Is any regular assessment and reporting undertaken against information security policy and controls, and corrective action taken?

Risk identification **Processes**

- Records design
  - Was/is the appraisal of the organization’s activities:
    - based on adequate knowledge of the business of the organization;
    - comprehensive;
    - inclusive of all relevant legislation and regulation; and
    - inclusive of all interested parties?
    - Does the design cover all documented uses of the records?

Risk identification **Processes**

- Records design /cont….
  - Do the naming conventions and classification schemes fit the terminology of the organization and the Provincial Archives?
  - Are the dependencies of the records systems on other systems for data input identified and managed appropriately? – e.g., use of the personnel system of staff names and locations
  - Is the technology selected an appropriate fit for the size, complexity and activities of the organization?
  - Does the technology adequately support the functions of the records systems?

Risk identification
Processes

- Records creation & records system implementation
  - Are the record-creating processes appropriate, reliable, systematic and timely?
  - Are the records adequately identified and controlled from the point of capture?
  - Are records routinely created as designed?
  - Are records creators adequately trained in the processes?

Risk identification
Processes

- Are the processes for linking the metadata to records tested, secure, robust, sustainable?
- Is the metadata scheme flexible enough to respond to changes in the organization’s circumstances?
- Are records requiring restriction adequately identified and protected from creation?
- Is there need to monitor or record access to restricted records?

Risk identification
Processes

- Metadata
  - Is metadata routinely captured as part of business processes?
  - Does metadata capture meet Provincial Archives requirements?
  - Does metadata adequately allow for capture, search and retrieval of records?

Risk identification
Processes

- Use of records
  - Are processes in place to prevent staff misuse or unauthorised disclosure of records?
  - Are staff able to find records?
  - Are potential users (internal, external or data subjects) aware that records exist?
  - Are external users or data subjects aware of process to access records?
  - Is security classification consistent with legal / mandatory requirements?
  - Are appropriate mechanisms in place to resolve conflicts relating to access and use?
  - Is access to records adequately classified in order not to prevent use of records by relevant users?

Risk identification
Processes

- Use of records systems
  - Are staff able/willing to use records system?
  - Are adequate protections in place to prevent unauthorised access to records or to metadata about records?
  - Is information adequately protected to enable different levels of access?
  - Does the records system document who has accessed, processed or used records?
  - Is the records system designed to enable different levels of access for authorised users?
  - Does the records system provide timely service for users?

Risk identification
Processes

- Records usability
  - Can records perform their original purpose?
  - When encryption is used when storing records can it be decrypted?
  - Can revisions, comments and history or other notes attached to a record be accessed?
  - Is record’s creation and use documented through metadata and can it be accessed?
  - Are physical records, incl. sound and audio-visual records, still usable?
  - Are older versions of digital records accessible via current applications/versions of applications?

Risk identification
Processes

– Has content and structure of a record (e.g. database or spreadsheet) been documented and maintained through format conversions?
– Are records presented in formats that enable use in varied environments
– Are the storage media that records are stored on, readable and useable with existing technology?
– Are linkages within records that point to other records, still useable?
– Is there a documented process for doing records backups?
– Are backups undertaken according to a documented process?
– Are records and their metadata replicated in other locations (in case of disasters)?

Risk identification
Processes

- Disposition
  - Authorisation
    - Is there a disposition authority in place from the Provincial Archives?
    - Is the disposition authority current and relevant?
    - Has disposition been authorised by the appropriate manager?
    - Is there a process for reviewing existing authorities?

Risk identification **Processes**

- Disposition
  - Planning and implementation
    - Are there policies & procedures in place for the disposition of records?
    - Are roles and responsibilities for disposition defined and documented?
    - Is disposition undertaken on a regular and routine basis?
    - Is there a process for handlings exceptions?
    - Are there processes in place for managing off-site storage?
    - Are there plans in place to protect and preserve records of archival value?

Risk identification
Processes

- Disposition
  - Accountability
    - Is disposition documented?
    - Is the documentation appropriate?
    - Is the disposition of records monitored and reviewed?
    - Is there appropriate education and training in place for staff, including staff responsible for records?

Risk identification **Processes**

- Disposition
  - Security
    - Have security and privacy considerations been identified?
    - Are disposition methods appropriate to the level of security required?
    - Are there processes in place to ensure destruction of records is complete—e.g. are all copies deleted?

Impact:
Factors to consider

- Priority and /or significance of the records
- Numbers of users and other stakeholders affected
- Effect of damage or loss of records on current operations of the organization
- Measures already in place to respond to interruption to access to the records

Impact: Factors to consider

- Time and effort to recover or replace the records affected
- Impact of the loss of or damage to records on the rights or property of the organization
- Impact of the loss of or damage to records on the organization’s ability to discharge its obligations to all stakeholders
- Regulatory requirements to disclose information about damage, loss or unauthorised access to, records
- Impact on the public standing of the organization.

Loss Prevention

- Appropriate back-up locations
- Physical & climatic hazard avoidance
- Combination of physical and digital records systems
- Use of imaging as a means of reducing records risk
- Unauthorised entry (physical)
- Electrical stability
- Virus protection

Loss Prevention cont./..

- Limited network (and desktop) access
- Willingness to report irregularities
- Workstations turned off and locked
- Not left unattended whilst logged on
- S/W terminate after inactivity period
- Segment network
- Get tough – fireable offenses
- Train in “proper” use of passwords
- Multiple levels of passwords
- Encryption

Loss protection

- Business Continuity
- Use of vaults
  - Specially designed on-site cabinets
  - Off-site
    - Secure locations
    - Appropriate distance away
    - Delivery SLA’s
    - Environmental control
    - Mirrored or reciprocal sites

Conclusion

- Physical and digital records are exposed to risk
- Risk analysis must look beyond physical storage areas
- Records not in records storage areas (physical and digital) are at greater risk
- Focus on “real” risks
- Focus on areas of potentially greatest impact
- Look for opportunities to reduce risk and improve business processes at the same time (Scanning)
- Prevention is better than cure

Questions?

Any questions?