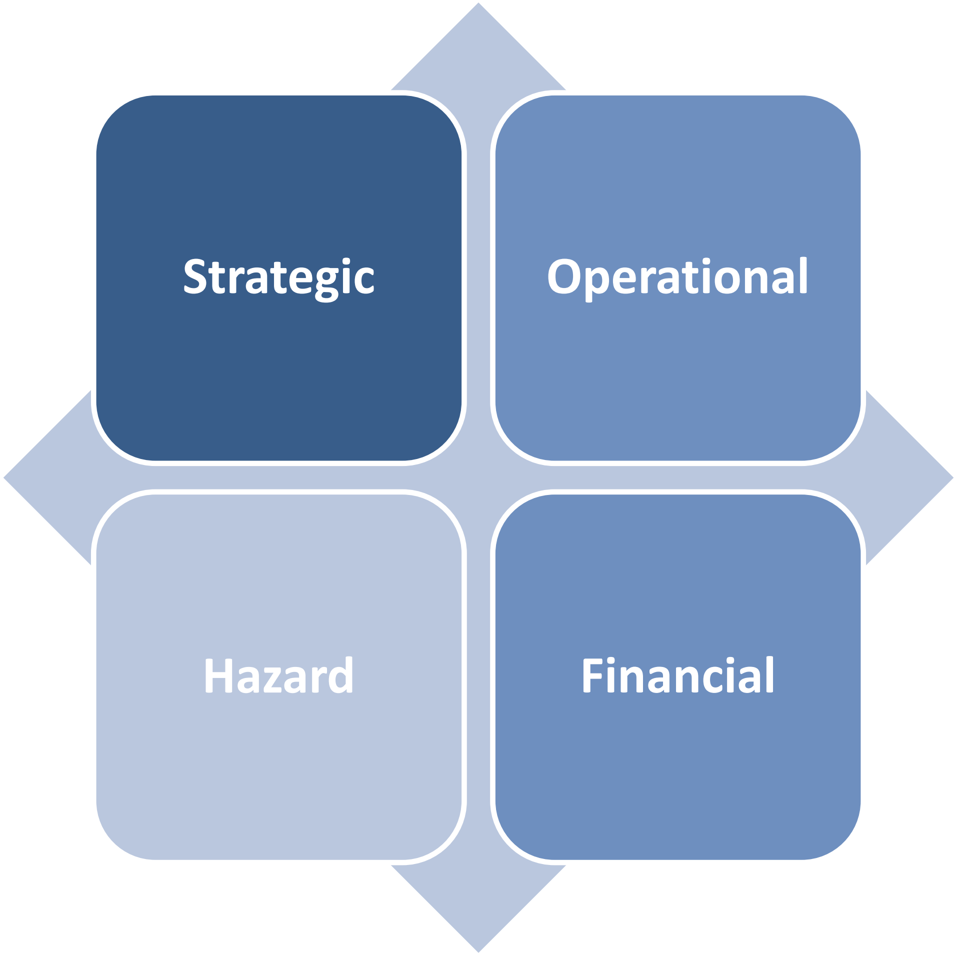
UNITED NATIONS
Department of Management
Archives and Records Management Section

United Nations
Peacekeeping

Risk Universe



Entebbe, June 2014

UNITED NATIONS
Department of Management
Archives and Records Management Section

United Nations
Peacekeeping

Managing Information Risks in PKOs

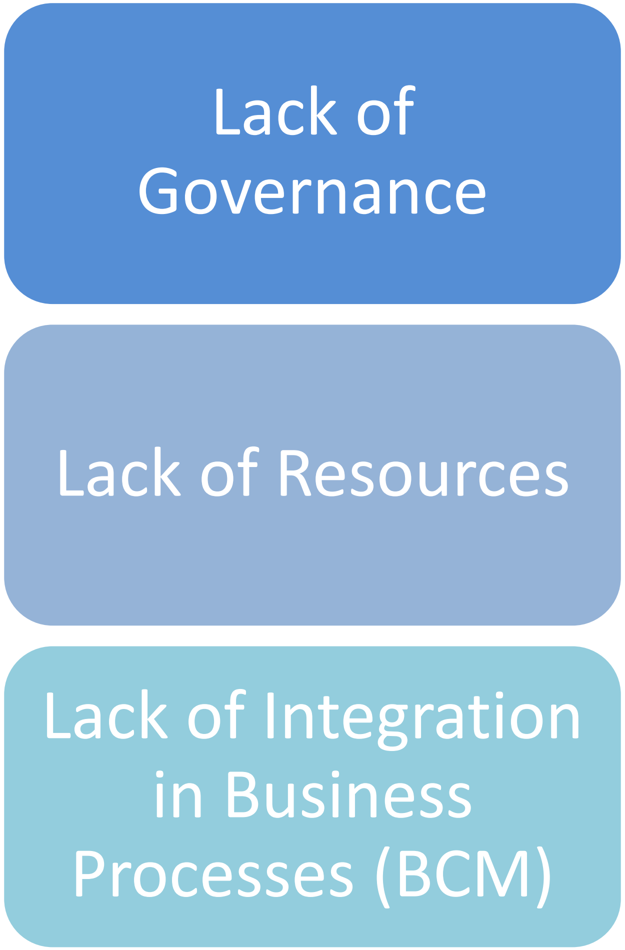
Administrative Recordkeeping Risks

Records Control Risks

Technology Risks

Entebbe, June 2014

Administrative RK Risks



Lack of Governance

Lack of Resources

Lack of Integration in Business Processes (BCM)

Problems: Administrative RK Risks

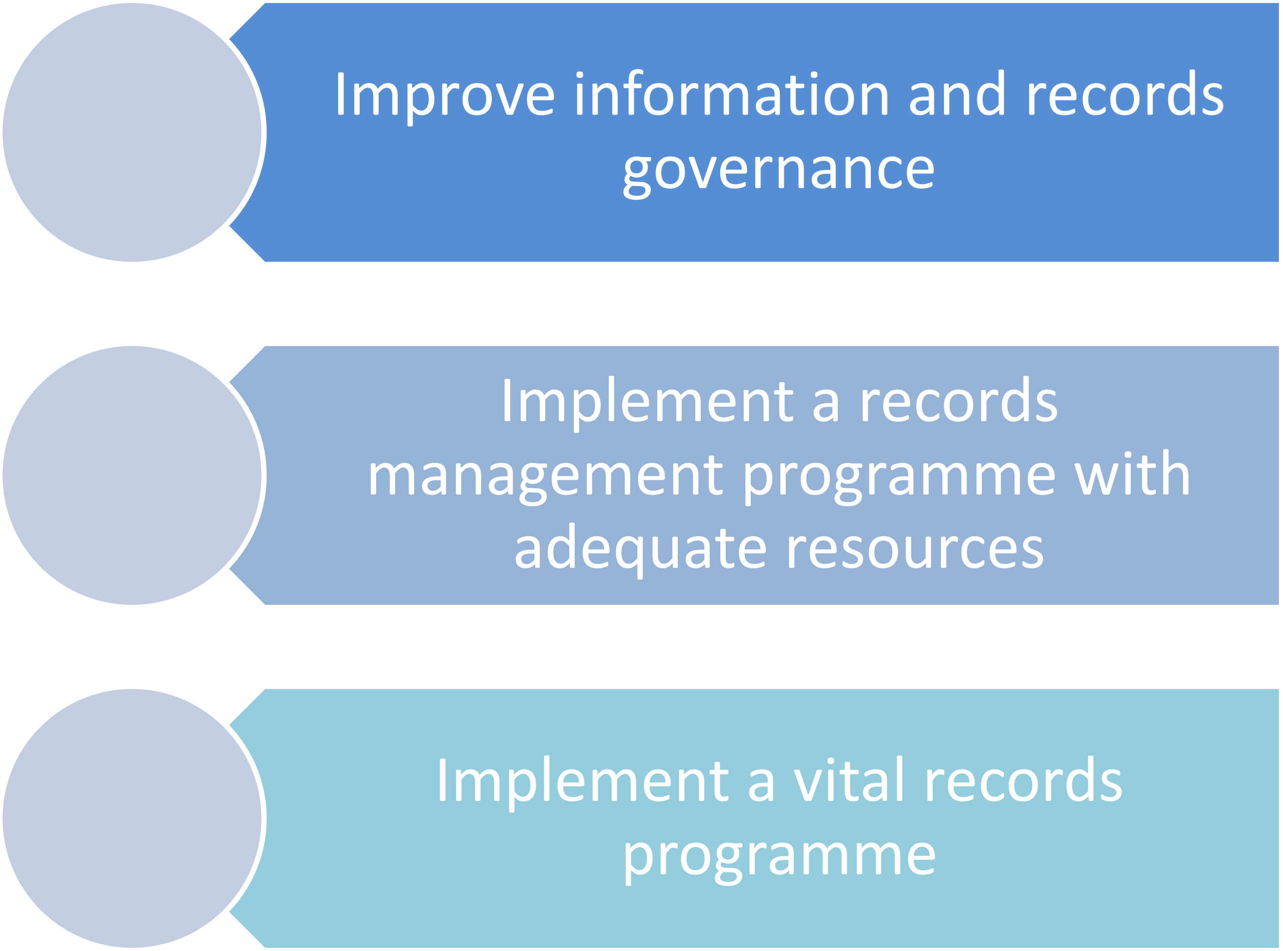
- Lack of clear roles and responsibilities for RM and decision-making regarding records
- Lack of awareness of the importance of records as evidence
- Low profile and lack of resources for RM
- RM not incorporated in mission planning and operations
- Absence of mandatory recordkeeping requirements
- Inability to provide evidence of actions or decisions
- Poor decision making because core information is not easily available
- Difficulty responding to audits
- Inability to continue business in emergency because of lack of access to records

Vital Records Programme

Key components of disaster mitigation plan for an organization:

Vital records, database or file	Form: hardcopy or electronic	Storage location	Maintenance frequency
UMOJA	Electronic	DFS server in Valencia	Annually
MoU with host country	Electronic /Hardcopy	OSRSG and Valencia	Annually
Telephone tree	Electronic /Hardcopy	DMS and Valencia	As necessary
Emergency plan for X mission	Electronic /Hardcopy	DMS and Valencia	Annually

Mitigation

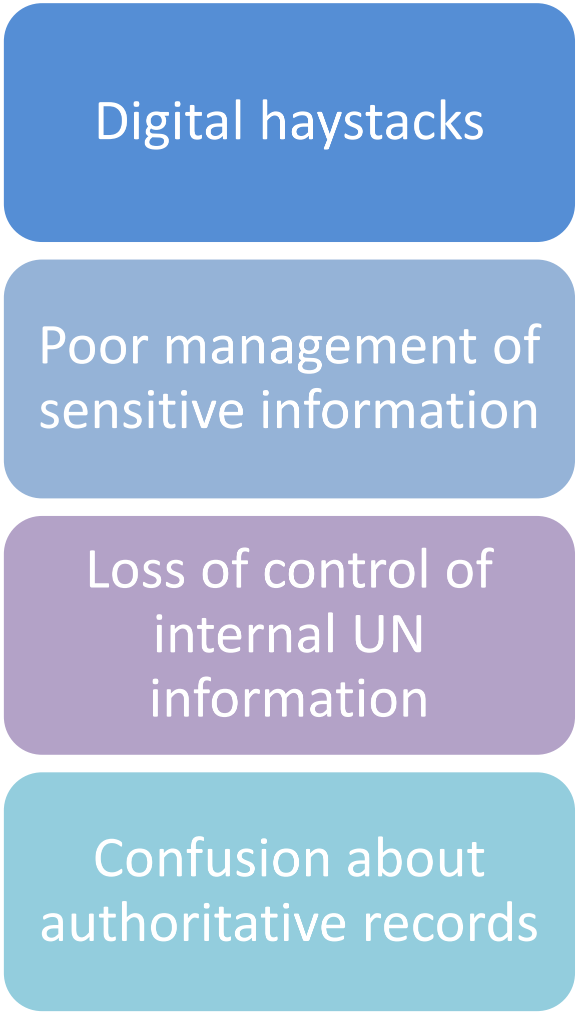


Improve information and records governance

Implement a records management programme with adequate resources

Implement a vital records programme

Records Control Risks



Digital haystacks

Poor management of sensitive information

Loss of control of internal UN information

Confusion about authoritative records

Problems:

Records Growth, Chaos and Unauthorized Access

- Retention of excessive volumes of unwanted information because inability to enforce records retention schedule
- Uncontrolled use of ICT (Incomplete or inadequate classification/organization of records)
- Consistent use of cloud computing technology to share and access sensitive PKO records
- Sensitive records are not marked, staff not aware of information sensitivity toolkit and DPKO access policy
- Inability to manage versions of records and distinguish duplicates and draft from original copy

Protecting records and information

- ST/SGB/2007/6 - Information sensitivity, classification and handling (Classification levels: strictly confidential, confidential, unclassified)
- Handling of classified information in Missions (DPKO Information Sensitivity Toolkit)
- Access and Declassification of Missions records

Marking: Information Security Levels

STRICTLY CONFIDENTIAL - applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause **exceptionally grave damage** to or **impede the conduct of the work** of the UN

CONFIDENTIAL - applied to information or material the unauthorized disclosure of which could be reasonably expected to **cause damage to** the work of the UN

UNCLASSIFIED - applied to information or material the unauthorized disclosure of which could be reasonably expected to have **nominal consequences**

Exceptionally grave damage to UN

- Irreparable harm to the United Nations, its Member States or individuals
- Long-lasting and/or far-reaching impairment of a United Nations mission, operation or programme

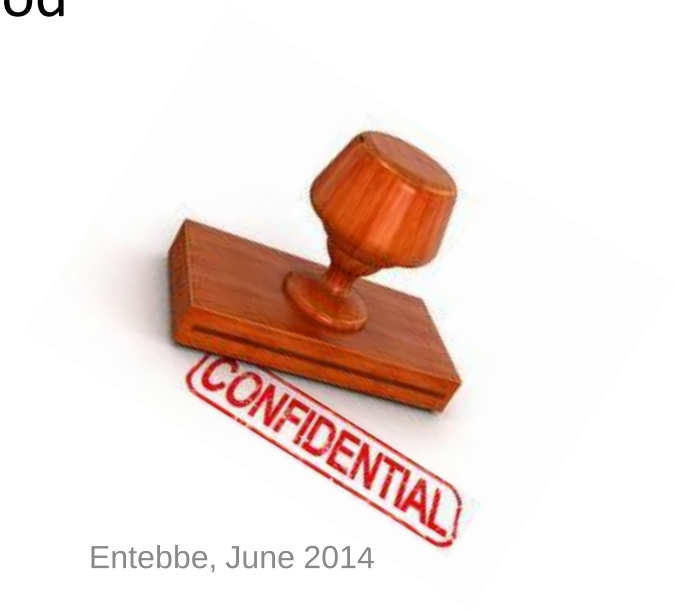
Example?

STRICTLY
CONFIDENTIAL

Reasonably expected to cause damage

Harm to the United Nations, Member States or individuals, where damages incurred could potentially be repaired through negotiation, good offices or other means

Example?



Nominal consequence to the work of the UN

No harm will occur to the United Nations, Member States or individuals

Example?

UNCLASSIFIED

Public

- **Unclassified information is not equivalent to Public information**
- Public: is for Information produced expressly for public consumption or that has undergone a declassification process and is available for public use such as archives

Rules for Code Cables

- **Code cables are no longer sensitive by default**

- Code cables must be marked as follows:
  - *Unclassified*
  - *Only/Confidential*
  - *No Distribution/Strictly Confidential*

Sensitive Information Handling

- Information Sensitivity Toolkit is the resource of reference

- All sensitive information **must be:**
  - **Transported** in sealed envelopes or containers, and clearly marked as such.

  - **Ideally Recorded** in a special registry.

  - **Duplicated** only with the authorization of either originator or the Head of the receiving or originating department or office, and such copies must be entered in the special registry

Classification Authority Principles

- The **originator** of the information
- The information **recipient** if the information is received from an outside source
- The security classification process is under the overall supervision and guidance of the Head of Mission

Declassification

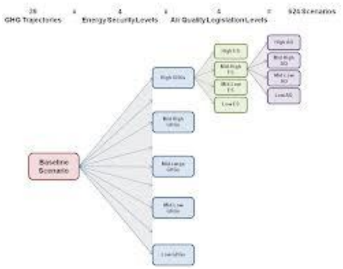
- Records marked as “confidential” and unclassified shall be declassified automatically after 20 years
- For strictly confidential records after 20 years, review if the strictly confidential status is still valid, if it is the case undertake periodic review every 5 years

- Some very sensitive records shall never be declassified or have a special regime in place (closed for 50 years)

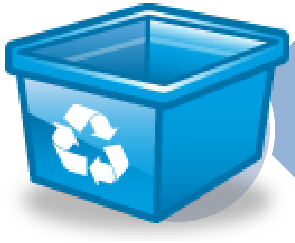
- The originator or recipient shall establish the marking which will trigger the automatic declassification

- If no marking specified the declassification authority is:
  - Originator or recipient at any time
  - UN Secretary-General or officials authorized at any time.

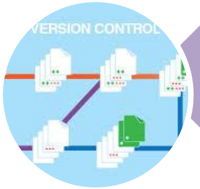
Mitigation



Complete development/ implementation of retention schedule with associated classification scheme



Dispose of obsolete information regularly



Implement documents management/recordkeeping system

Mark, actively manage and protect sensitive information

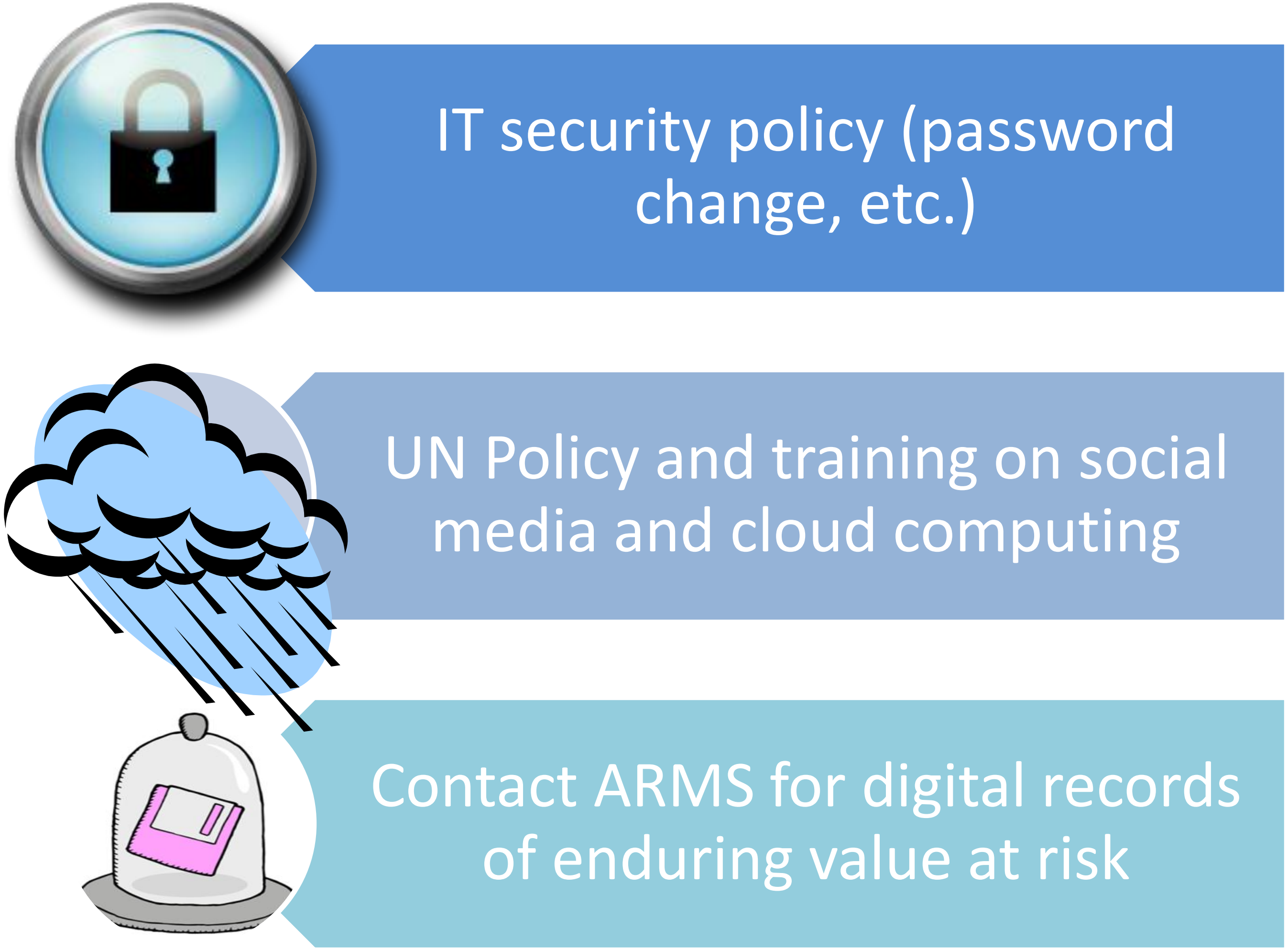
Technology Risks

- Weak information security infrastructure
- Use of non standard software, systems or repositories
- Technology obsolescence

Technology Risks

- Lack of information security policy, including passwords protection, etc.
- Use of social media and cloud computing to create, manage, store and share UN business records
- Digital obsolescence: media which hold digital records and format of digital records, leading to records’ loss

Mitigation



IT security policy (password change, etc.)

UN Policy and training on social media and cloud computing

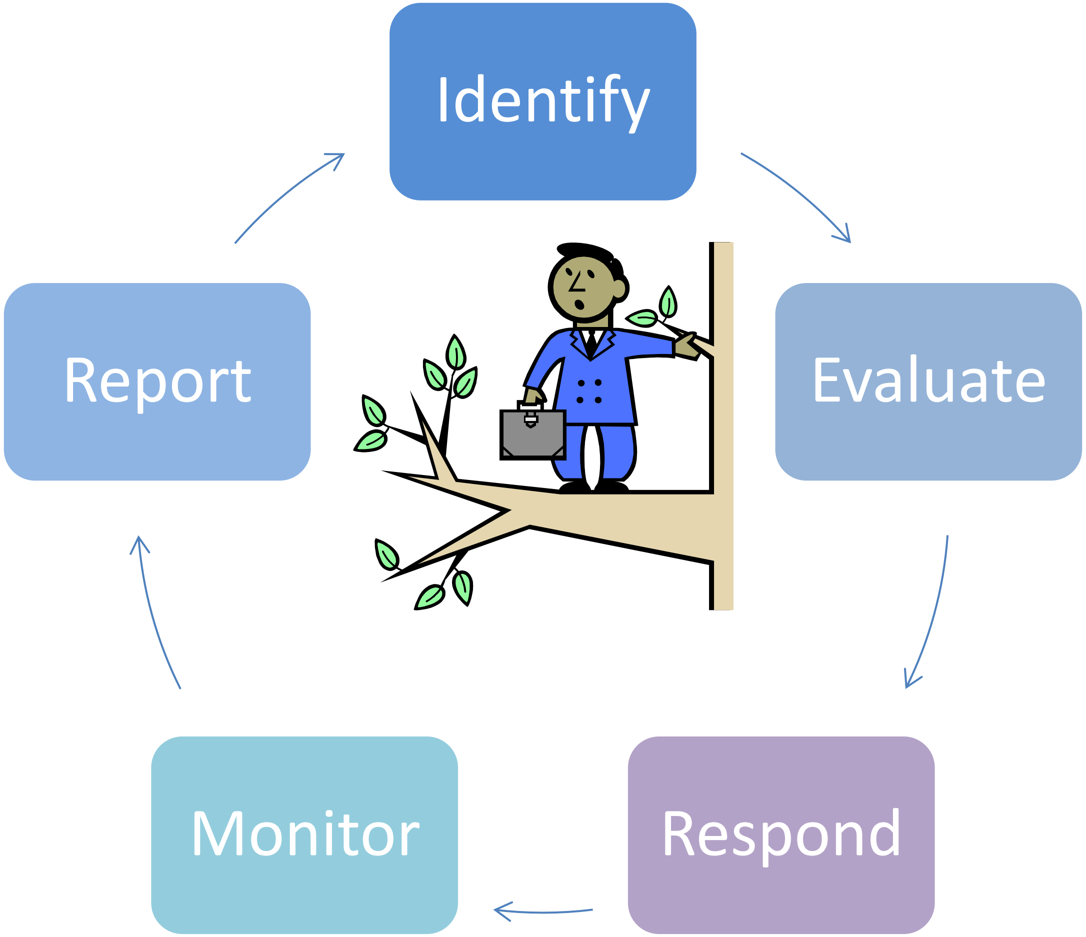
Contact ARMS for digital records of enduring value at risk

Approaches to Mitigate Risks

Event-based

Requirement-based

Risk Management Process



Identify

Evaluate

Respond

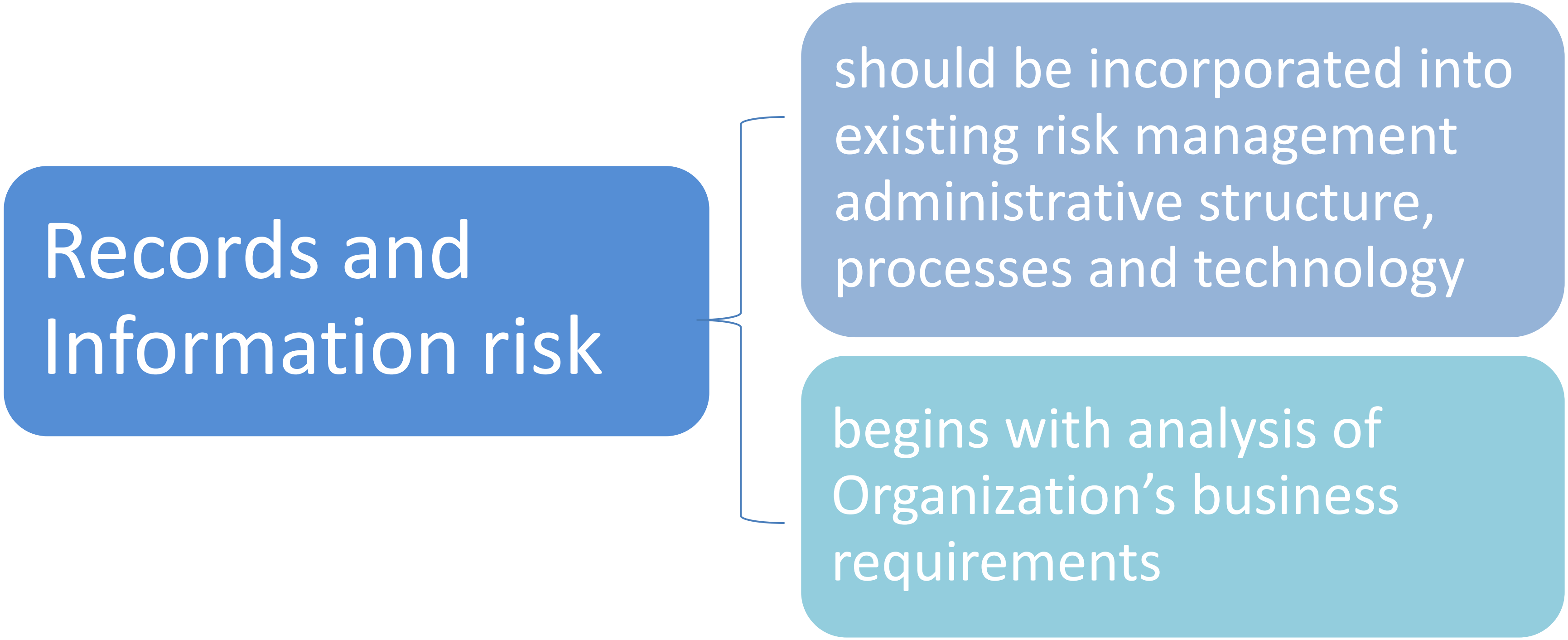
Monitor

Report

Events-based Approach

Trigger event	Risk	Risk Mitigation Strategy	Owner of risk
Fire	Loss of records	Disaster preparedness and recovery programme	Business continuity planning/ Records management team
Unauthorized disclosure of sensitive information	Loss of confidentiality leading to possible loss of lives, damage to reputation	IT security strategy	CITS
Inadequate retention period for records	Records unavailable to conduct important business with host country	Revise retention schedule	Records Management Team/ Legal Team

Records and Information Requirement-based Approach



Records and Information risk

should be incorporated into existing risk management administrative structure, processes and technology

begins with analysis of Organization’s business requirements