MANAGING RECORDS TO MANAGE INFORMATION RISKS

Records and information-related risk assessment can be used to enhance an organisation's performance, reduce business risks and help information managers manage information strategically. More specifically the risk-based approach will promote:

- more effective planning of records and information management strategies and programmes to ensure alignment with the core business objectives of the Organization;

- official decisions from key areas of the Organisation is well documented, supporting accountability and transparency;

- improved decision making with reliable access to authoritative records;

- the identification and protection of sensitive information;

- better control of records and information management costs (e.g. avoidance of unnecessary storage costs);

- the Organisation's readiness for audit;

- the reduction of operational disruptions (e.g. finding vital records easily in an emergency);

- knowledge sharing because everyone can find and use information rapidly;

- the identification and protection of vital records are secured, supporting business continuity and disaster recovery efforts;

- records with archival value to be identified and protected for posterity.

Creating and managing records help organisations conduct their business and manage the risks associated with that business. Without adequate records, your Organisation may have difficulty providing evidence of its actions and decisions. Records and information risk management should ideally be integrated with the organisation's enterprise-wide risk management strategies. It will allow records management activities to be connected to specific business risks.

High-risk businesses are those that:

- receive a high level of public and media scrutiny;
- allocate, spend or collect large amounts of money;
- assess or mitigate significant public risk;

- involve issues that are politically sensitive;
- involve issues of international security;
- relate to sensitive or contentious activities;
- are outsourced to an external service provider.

All of these could expose an organisation to serious consequences. Records documenting these actions generally need to be more detailed and of a higher quality than those that document low-risk activities.

Such records will also require more intensive management to ensure their proper accountability and incorporate features such as audit trails.

Roles and responsibilities for records and information risk management will be clearly identified and a training programme for risk awareness would benefit from being developed. Consideration of records and information risk management requirements should be built into organizational planning processes such as strategy development.

Record-keeping Risks and Mitigation Requirements

PRIMARY RISKS

1) INADEQUATE RECORD-KEEPING GOVERNANCE FRAMEWORK

OPERATIONAL CONSEQUENCES

2) LACK OF AWARENESS OF THE IMPORTANCE OF RECORDS AS EVIDENCE

(1) Weak records protection as part of emergency management and business continuity planning

(2) Inadequate protection of records with regarding to information security and sensitivity

(3) Indiscriminate application of Information technology end tools without effective record-keeping

SECONDARY RISKS

SECONDARY RISKS

SECONDARY RISKS

- **Difficulty Identifying and protecting staff during an emergency.**
- **Risks to resources and facilities because vital records are not available immediately.**
- **Inability to maintain or restore core operations quickly because critical records are damaged or lost.**

- **Danger of security breaches and information leaks.**
- **Increased risk of sabotage or damage to missions or operations**
- **Danger to the security of UN staff, mission personnel, or Member states.**
- **Violation of Individual security or privacy.**
- **Collapse of public confidence in the UN.**

- **Inadequate management of electronic records and information, leading to confusion over which records are official.**
- **Multiplication of digital records and information, increasing the danger of security breaches, losses, confusion, and mismanagement.**
- **Inconsistent and uncoordinated development of electronic record-keeping tools, resulting in wasted resources, and duplication of effort, and unsustainable IT/IM systems.**

CORE MITIGATION REQUIREMENTS

(1) STRENGTHEN THE RECORD-KEEPING GOVERNANCE FRAMEWORK

(2) RAISE AWARENESS OF THE IMPORTANCE OF RECORD AS EVIDENCE