

BUSINESS CONTINUITY AND DISASTER RECOVERY

Records and Information Management is gradually gaining recognition in the Public Service. Many Ministries and Departments are now taking steps to manage recorded information as a strategic resource. Many departments have found that a good Records and Information management programme includes identifying potential risks to records and information and putting a plan in place to mitigate loss.

Disasters

Risk Management has gained visibility in many organizations, especially after the devastation of Hurricanes Katrina and Ivan. Risk may also be categorized as man-made, that is, accidental, deliberate, technological, or acts of terrorism. Risk Management activities are generally developed around core organizational functions. These functions include Information Technology, Facilities and so on.

In the event of a disaster, the Information Technology department may quickly provide network restoration with key systems up and running again. The Facilities Department may restore buildings and provide resources required for recovery. However, it is unlikely to regain full recovery without the organization's critical records and information.

The Business Continuity and Disaster Recovery plan for records and information should include identifying and analyzing potential risks that are likely to affect business continuity through records and information including the systems that manage and maintain them.

In preparing a Disaster Recovery plan, the impact of potential loss to the organization should be analyzed and a Business Impact Analysis carried out. The Records Manager should ask and answer questions like, how can the records be recovered? Where are they located? What would be the recovery time? What are the resources required for recovery? The analysis should include vital records, their location, media type, updates and accessibility. The analysis should also include electronic records.

Identifying and Protecting Vital Records

Vital Records Protection should be an integral part of the departments overall Business Continuity Plan. The plan should also include a vital records protection plan. Vital records are irreplaceable and constitute approximately 10% of an organization's records holdings.

Vital records protect the:

- ❑ the rights of employees and citizens'
- ❑ the Legal and Financial rights of the organization
- ❑ provide proof of the department's assets and obligations.

A Vital Records Protection plan is similar to an insurance policy, expensive to setup and maintain, but yield high dividends in the event of a disaster.

Examples of vital records include: minutes of board meetings, accounts payable and receivables, payroll records, social security and retirement records, titles, deeds, contracts, permits, engineering drawings, shareholders records.

Methods of Protection include:

- Dispersal – this is the least expensive, information is routinely dispersed to other departments
- Duplication – Duplicate the records for the purpose of protecting them. Records could be stored in fireproof cabinets, vaults and file rooms that provide protection for vital records.
- Remote storage – storing the records off-site in another building or location. With the current spate of devastating hurricanes, one ought to consider storing vital records in another Island. Access to records must be considered in this regard.

Keep the wheels in motion

The Records Manager should monitor and update the organization's vital records regularly, adding new records as is necessary. The consequences for failing to protect and secure your organization's vital records are enormous. You may not want to be in a situation where you would say, 'had I known'. Remember the old adage, 'prevention is better than cure'. Identify your organization's vital records, protect them and keep the wheels in motion.

Mrs. Vera Forde