BSc in Computer Engineering
CMP4103
Computer Systems and Network Security

Lecture 11

Business Continuity Disaster Recovery

Eng Diarmuid O'Briain, CEng, CISSP

Department of Electrical and Computer Engineering,
College of Engineering, Design, Art and Technology,
Makerere University

Table of Contents

This page intentionally left blank

1. Business Continuity Planning (BCP)

BCP is the creation and validation of a practiced logistical plan for how an organisation will recover and restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption.

BCP is working out how to stay in business in the event of disaster. Incidents include local incidents like building fires, regional incidents like earthquakes, or national incidents like pandemic illnesses.

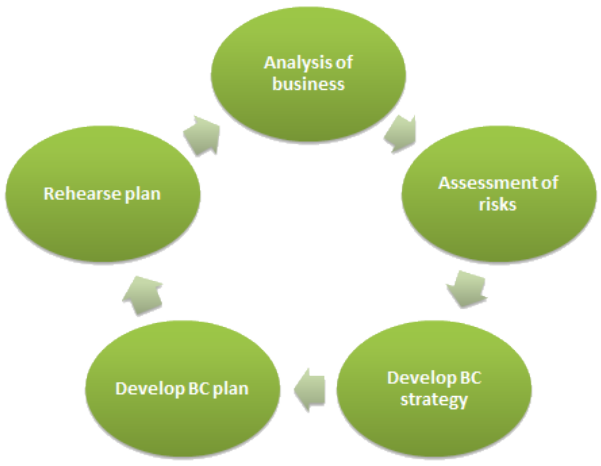
BS 25999 is British Standards Institution (BSI) standard in the field of Business Continuity Management (BCM). This acted as the base for the ISO/IEC 27000-series, which comprises information security standards published jointly by the International Organisation for Standardisation (ISO) and the International Electro-technical Commission (IEC). The series provides best practice recommendations on information security management, risks and controls within the context of an overall Information Security Management System (ISMS).

2. Business Continuity Lifecycle

The Business Continuity Lifecycle is a five-step plan.

2.1 Analysis of Business

This initial phase if the lifecycle is an opportunity to look critically at the business to identify vulnerabilities. All-important processes within the business and between the business and customers will need to be evaluated for vulnerabilities.



2.2 Assessment of Risk

Having identified the possible risks it is now a matter of identifying the likelihood of the risk ever occurring and what the impact of such a risk on the business should it ever happen.

2.3 Develop a Business Continuity Strategy

For each risk a strategy will be needed, such strategies will normally be determined by available budget, either:

- Accept the risk.
- Accept the risk but get a business continuity partner who can help in the event of an incident.
- Reduce the risk.
- Reduce the risk but get a business continuity partner who can help in the event of an incident.
- Reduce the risk adequately that a business continuity partner is not necessary.

2.4 Develop a Business Plan

Now that risks have been identified and a strategy to deal with them decided a full business plan will be needed. Such a plan should be simple because employees will need to act quickly and decisively after an incident.

2.5 Rehearse Plan

There is a military maxim that applies at this stage "*Train hard, fight easy*". The plan must be rehearsed so that employees will know exactly what to do in the event of an incident.

3. BCP Process

The BCP Process has the following four steps:

3.1 Project Scope and Planning

- Structured analysis of the whole business from the perspective of crisis management.
- Appointment of a BCP team with Senior Management approval. The team should consist of:
    - Representation from each department with responsibility for the company core systems
    - Representation from support departments
    - IT personnel with technical expertise in the core systems
    - Information Security officer
    - Legal representation with knowledge of the contractual requirements that may impact the plans
    - Senior management representative
- Identification of all resources available to the team for BCP.
- Understanding of the regulatory and legal situation that governs the companies response to an major event requiring a business continuity response.

3.2 Business Impact Assessment (BIA)

The Business Impact Analysis (BIA) is performed to identify the key business processes and technology components that would suffer the greatest financial, operational, customer, and/or legal and regulatory loss in the event of a disaster. The main intent of a BIA is to identify all the critical resources, systems, facilities, records, etc., that are required for the continuity of the business. Additionally, the time it would take to recovery such resources will be identified.

- For each urgent function, two values are then assigned:
    - ***Recovery Point Objective (RPO)*** - the acceptable latency of data that will be recovered
    - ***Recovery Time Objective (RTO)*** - the acceptable amount of time to restore the function

The RPO must ensure that the ***Maximum Tolerable Data Loss (MTDL)*** for each activity is not exceeded. For example if the RPO is set to six hours, then backups must be continuously maintained within that time or more often, say every four hours, i.e. a daily backup will not suffice.

The RTO must ensure that the ***Maximum Tolerable Period of Disruption (MTPD)*** for each activity is not exceeded.

3.2.1 Risk analysis

Now that the recovery requirements are defined, an identification and documentation of potential risks should be undertaken. Identifying the risks give the opportunity to review each and define a specific set of work instructions. Here is a list of common risks:

- Terrorism
- Cyber attack
- Sabotage
- Disease
- Fire
- Flood
- Utility outage

3.2.2 Assessment of Likelihood

Now that we have identified risks what is the likelihood of these occurring? For each produce an ***Annualised Rate of Occurrence (ARO)***. How often is it likely that this event will occur in any year?

3.2.3 Assessment of Impact

Should an identified risk actually occur what is the likely impact of the event on the business ? Determine the ***Exposure Factor (EF)*** to the business as a percentage of the Assets Value (AV) and from these figures calculate the ***Single Loss Expectancy (SLE)***:

$$SLE = AV \, x \, EF$$

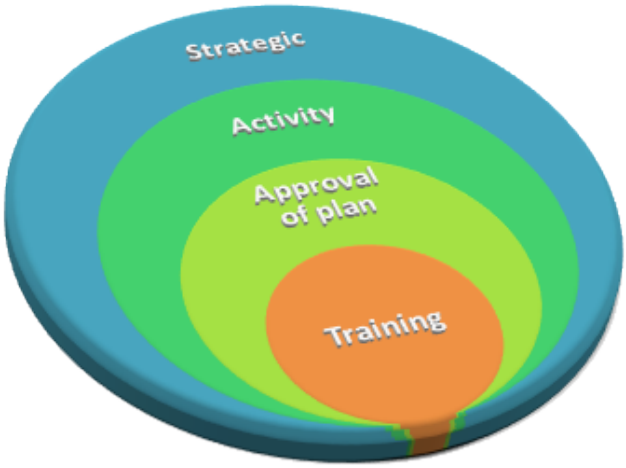
From the earlier ARO figure, it is a simple matter to calculate the ***Annualised Loss Expectancy (ALE)***:

$$ALE = SLE \, x \, ARO$$

3.2.4 Prioritisation of Resources

Taking all the risks analysed sort them in a descending list ordered by the ALE of each risk.

3.3 Continuity Planning



Having identified the risks, the impacts of these risks should they occur and the priority of resources to deal with risks should they occur we must now plan a strategy to minimise the impact that incidents that occur would have on assets. Continuity planning is in a number of levels:

3.3.1 Strategic Level

This is the identification of which of the risks will be considered in the Business Continuity Plan. Some risks for example may be deemed acceptable to the higher management.

3.3.2 Activity Level

At the Activity Level the complexity of interdependencies on services, business processes, data and technologies needs to be analysed and appropriate tactics chosen to address the needs of:

- People, workforce, skills and knowledge
- Premises
  - Alternative Sites
- Infrastructure
  - IT Backbone
  - Servers
  - Workstations
- Information
  - Backup off site
- Stakeholders partners and contractors
  - Alternative partners and contractors

3.3.3 Approval of Plan

Support from top-level management is essential otherwise; the plan is very likely to fail under test.

3.3.4 Training

All personnel that may need to be involved in the plan need training and regular exercise in the execution of the plan. Consider mock exercises regularly much like a fire drill to ensure personnel are “on their toes”.

3.4 Documentation

3.4.1 Continuity Planning Goals

A list of goals for continuity planning. It should start with:

"To ensure the continuation of the business in the event of an emergency situation"

Fill out the remaining goals as necessary for the organisation.

3.4.2 Senior Executive Statement

This statement should come from the C-level management to indicate to all employees the importance of the BCP. The statement should reinforce that Business Continuity is every employee's responsibility. It should also contain language as to the urgency of the BCP.

3.4.3 Timetable

This is the implementation timetable identified by the BCP team and agreed with upper management.

3.4.4 Priority List

This is a statement of the ordered priorities identified in the BIA.

3.4.5 Risk Assessment

This portion of the documentation captures the assessment performed in the BIA, it should include the analysis on each risk. All risks should have a status as to acceptance or mitigation and for the latter the process and provisions to be put in place.

3.4.6 Records

All vital data and records should be identified and the where they will be stored plus the backup processes and procedures for handling them. How and where.

3.4.7 '*Action-on*' Emergency Incident

Guidelines must be produced to document the immediate 'Actions-on' response procedures to each potential incident. Who is notified?

3.4.8 Change process

The BCP will need to be tweaked from time to time and the document should include the agreed mechanism for such change.

3.5 Testing

The BCP should document a testing programme and timetable designed to find the flaws in the BCP. The testing should include any elements of the plan that have been outsourced to a third party. Testing should include at different timescales the following types of test:

- ***Document check***
  - BCP documents checked to ensure changes in operations or administrative changes in personnel or contact details for example are updated
- ***Walk through test***
  - This is a paper exercise where necessary personnel are brought together to go through the plan to see if problems can be anticipated and fixed
- ***Simulation***
  - Mock emergency created to test personnel and systems. Exercise conditions with little risk
- ***Parallel test***
  - Run a full test at backup sites while still maintaining operations at the primary site. This is an important test particularly if the backup site is outsourced. It should be performed at least annually
- ***Full***
  - Shut down primary site and move operations to the backup site. This is an infrequent test as it is complex and expensive to perform, yet it is the best form of test that can be carried out

4. Exercise: Business Continuity and Disaster Recovery

You are the Chief Information Officer (CIO) for a specialised Credit company. The company specialises in Cloud bases services to the Micro-loan market and as such your company holds sensitive customer data that strictly cannot leave Uganda.

The company currently operates a pair of Xen servers in a data centre in Nairobi and a private data centre in Kampala, these servers offer High Availability (HA) Hipervisor to the virtual servers.

- Develop a BIA for 3 key business processes and technologies.
- Carry out a risk assessment and list 5 key risks.
- Order the risks.
- Describe the mechanism used to order the risks.
- Assuming the only risks are the 5 identified and develop a short BCP for them.
- Suggest a test regime for the BCP.

5. Bibliography

Faris C, Gilbert B, LeBlanc B. (2013). Integrating the triple bottom line into an enterprise risk management program. [ONLINE] Available at: http://www.coso.org/documents/COSO-ERM%20Demystifying%20Sustainability%20Risk_Full%20WEB.pdf. [Accessed 06 December 2013].

Henning D (2009). Tackling ISO 27001: A Project to Build an ISMS. [ONLINE] Available at: http://www.iso27001security.com/GIAC_GCPM_gold_henning.pdf. [Accessed 06 December 2013].

This page is intentionally blank