Debre Birhan Polytech. College

Sector: **Economic Infrastructure**

Sub Sector: **Information Communication Technology**

Occupation: **IT Service Management/Level V**

Unit Title: Prepare Disaster Recovery and Contingency Plan

LO1: Evaluate impact of system on business continuity

LO2: Evaluate threats to system

LO3: Formulate prevention and recovery strategy

LO4: Develop disaster recovery plan to support strategy

April,2017

DPTC

LO1: Evaluate impact of system on business continuity

What is a critical business system?

- A system is critical for a commercial organization if
  - its failure results directly or indirectly in loss of life (for example, an air traffic control system) and/or
  - major financial loss.
  - When developing a disaster recovery plan (DRP) it is essential to identify **critical systems** and ensure they are **restored** as soon as possible.
- Each critical system has a maximum allowable **downtime** beyond which **its loss will severely impact the business**.
- The shorter the period of time before losses start to occur, the more critical the system is.
- The size of the financial loss, relative to the financial worth of the business, is also significant.
- The greater the financial loss in percentage terms, the more critical the system is.

Identifying critical systems and data

You will need to collect information about how the system uses:

- software
- hardware
- networks
- data
- facilities (chairs, tables ,projectors etc).

An example of critical assessment

- You are working late on a 50-page assignment that must be handed in by 9 :30am the next day otherwise you will fail the course.
- You are using the Internet to book a holiday you intend taking in three months time.
- You have **developed** a spreadsheet to calculate your tax return.
- You have created a database of CDs, records, tapes and videos which you will need to show your insurance company if the collection is destroyed or stolen.
- You have saved several versions of your favourite computer game.

Table 1: Levels of critical systems	
Item	**Critical assessment**
1	Critical until 9:30am and then not critical
2	Not critical
3	Critical when completing tax return
4	Critical if event occurs
5	Not critical

Impact of system failure

- financial impact
- impact on cash flow
- If systems are regularly down or slow then customers may eventually go elsewhere

Activity 1 – identifying critical systems

Consider this case study.

- A clothing retail organisation, Urban Wear, intends to develop a website to manage orders and payments for its products.
- It will display a picture of each product, its price and availability.
- Customers will be able to order and pay for the goods online.
- The organisation believes that this will extend its sales to other countries and allow **24-hour selling.**
- *What **factors** would need to be considered in determining whether this new system will be critical to the business and what the **impact** might be if it fails?*

Write at least 4 questions you need to consider.

Feedback: Questions include:

- **What volume of sales is the new system expected to generate, especially compared to traditional sales?**
  - (The higher the percentage of overall sales it generates, the more critical the system will be.)
- **How will the new system impact traditional sales?**
  - Will customers prefer to use the website rather than visit a store?
  - How will this affect the profitability of the stores?
  - If it reduces their profitability, what will happen to the stores?
- **What are the implications of 24-hour access?**
  - Will deliveries be made 24 hours a day?
  - Can the organisation's current distribution resources cope with overseas orders?
  - Does the organisation have the skills to maintain a 24-hour website? What extra ongoing support will be required?
- **Are the goods of a type that may attract hackers or terrorists to the site in an attempt to attack it?**
- **What sensitive information, such as customer credit card details, may be on the site?**

1 What *issues* need to be considered for backup and restoration of data?

Most organisations backup once a day, usually overnight.

The first issue to consider is that the system is planned to be *available* on a continuous basis.

This means that special backup arrangements may need to be considered.

These may require the system to be down for a brief period during backup or the use of backup software that can backup files in use.

2 What ***problems*** can occur with backing up **online** transactions?

Feedback

- Records of transactions can be lost if the system crashes between backups.
  - Suppose a backup is undertaken at 3 am after which orders continue to be received.
  - At 2 pm the system crashes and needs to be restored from backup. There may be no record of all the orders received between 3 am and 2 pm.
- In traditional paper-based systems the original order would be available which could be re-keyed.
- It may therefore be necessary to maintain ***a transaction log on another server*** which is a mirror of the data entered on the main file.

LO2: Evaluate threats to system

- Risk Analysis
- Identify system threats

Risk analysis

- Risk analysis is an analytical process undertaken to evaluate **system assets** and examine their **susceptibility to threats**.

- Through this process we evaluate the ***possible commercial*** *losses that may result from the loss of these assets.*

Figure 1 Risk Analysis

Why do we carry out a risk analysis?

- To identify ***preventive*** and ***recovery*** options for assets.
- Computer systems (including hardware, software and data) are ***valuable* assets of an organization**.
  - It is therefore very important that a risk analysis be undertaken ***to identify and safeguard*** these systems.
- A major ***factor*** in risk analysis is to identify the **impact** of systems on ***business continuity***. '***Mission critical***' systems require the greatest level of protection.

An organisation undertakes an IT risk analysis to identify:

- how dependent it is on IT systems(dependability)
- what could go wrong with these systems(threats)
- what system assets they might lose(estimate loss)
- what can be done about it.(profitability)

- **Identify system threats**
- IT systems can comprise many parts including:
  - *Hardware, software, networks, data, technical skills, projects.*

- There are **ways** to categorise threats.

1. **Internal threats**
   - Internal threats mainly result from **actions by users and/or IT staff**. These can include:
- **viruses corrupt or delete data**.
  - Users can unknowingly transfer viruses to the corporate network via mobile devices.
- **the wrong disk is formatted destroying data and software.**

Cont…

- **sabotage**. Data and software are intentionally destroyed or corrupted.
- data and software files are deleted.
- a password is forgotten so data or software cannot be accessed.
- **input errors cause data to be corrupted/programming**
- processing errors cause data to be corrupted.* Poor software design changes data.
- hardware failure occurs so data and software are not available.
  - Hardware and networking equipment is delivered with ***a mean time to failure or mean time to repair***. This is the expected time after which hardware will need to be replaced or repaired. Preventive maintenance can prolong /extend this period.

Cont…

- **fraud**. Data is corrupted in order to steal assets.*
- **poor testing**. bugs are left in software so errors or delays occur.*
- **incorrect processes or calculations** occur in programs so errors or delays occur.*

2. External threats

External threats can include:

- **theft of data and loss of confidential information**
- **breakdowns of Internet or wide area network**
  - *connection or failure of critical systems hardware*
- **fire or earthquake** which renders the system inaccessible.
- **flooding** which renders the system inaccessible.
- **hackers corrupt or steal data**
- **power problems make the system inaccessible**. Power spikes or outages can disrupt critical systems.
- '**buggy**' **software** from a package vendor may cause errors in data or delays.

Example of system threats

- What threats can be identified for these systems?
- Internal threats
  - **viruses – deleting important data**.
  - **hardware failure**. Computer servers or networking equipment fail causing loss or inaccessibility of data.
  - **deleting or changing data**. Accidental deleting or changing of data by employees or software programs.
  - **input errors**. Mistakes by operators.

External Threats

- **theft of data**. Corporate espionage by competitors or by a hacker.
- **break down of telephone connections**. Inability to transfer data to head office.
- **fire, earthquake, flood.** Causes disruption to facilities or supply chain.

Activities

- **Activity 1 identifying possible threats**
  - Identify whether they are ***internal*** or ***external*** and flag with an * any threats that are also ***security threats.***

Table 1: Threats	
Threat	Category
Hackers attempting to get to the data stored on the site. *	
Hardware failures that stop the site operating.	
Denial of service attacks to bring the service down*	
Data destruction by any means such as a user deleting a file*	
Misuse of information by internal staff	
Power problems so site is down*	
Overloaded site so response is slow*	
Customers falsifying information to avoid payment*	
Incorrect information such as wrong prices so customers pay too little*	
Incorrect information such as wrong quantity in stock so customers have to wait for delivery*	
Major disaster so site is down*	