FACTFILE:
GCE DIGITAL TECHNOLOGY

AS1 APPROACHES TO SYSTEMS DEVELOPMENT

Rewarding Learning

Security Issues

Learning Outcomes

Students should be able to:

- explain why data is archived;
- explain the need for backup and recovery;
- evaluate methods of backup: full backup, differential backup and incremental backup;
- explain the purpose of a disaster recovery plan;
- describe the contents of a typical disaster recovery plan;

Content in Implementation Fact File

Students should be able to:

- ✔ Data archiving; what is it and why it is necessary?
- ✔ The importance of backup and recovery
- ✔ Methods of backup
  - * Full
  - * Differential
  - * Incremental
- ✔ Purpose of a disaster recovery plan
- ✔ Contents of a disaster recovery plan
- ✔ Questions

Data Archiving

What is it and why is it necessary?

An archive is the storage of information for a long period of time. Archived data consists of information that is still important to the organisation but it may not be of immediate use or it may be important for future reference. It may also consist of data which must be retained for a period of time in order to comply with legislation or for auditing purposes.

Data stored in archive will most likely be compressed so as to take up less space. It may also be stored on a cheaper storage medium such as optical discs. Data stored in archive must still be accessible to the end user if the need so arises and as such it may be indexed to facilitate easy location and retrieval of desired files or data items

The importance of backup and recovery

The backup process is the process of making copies of software or data in case the originals are lost or damaged. Having appropriate backup means that if a system failure occurs then the system or data can be rebuilt with accuracy.

Following a system failure or data corruption the backup will allow the corrupt or lost data to be replaced using copies from the backup process.

Methods of backup

It is expected that backups should be made on a regular basis so that any updates or changes made since the last backup can also be accounted for. A

Method of backup	Advantages	Disadvantages
Full backup –copies all files to provide a complete picture of the data at a given moment in time	• Everything is backed up at once • Files can be restored quickly and easily as complete files copied from backup	• Most files do not change so may lead to redundancy in backups • Takes longer to carry out as everything is being backed up • Concerns over security – everything stored in one place
Differential backup – copies only those data files that have been changed since the last **full** backup	• Faster than incremental restore as only uses the last full backup and last differential backup • Only copies files that have been updated so backup is faster than full backup • Takes up less storage space than a full backup	• Requires more storage space than an incremental backup • Longer time needed to restore files than with incremental backup as all changes since the last full backup will be copied
Incremental backup – copies only those files that have been changed since the last backup of any type	• Faster backup time as only amended files need to be copied • Less storage medium required to store incremental file as only copy files where changes have occurred	• Recovery process can take longer as all previous incremental backups are required in the process • Problems may occur if any incremental backups have corrupted, the entire file will be unrecoverable

variety of approaches to backup exists; these are outlined below. Purpose of a disaster recovery plan
A disaster recovery plan is a document which details the procedures associated with the recovery of and protection of an IT system in the event of any kind of disaster. A good disaster recovery plan will incorporate a set of procedures to support the recovery of or continuation of vital technology infrastructure following natural, environmental or man-made disasters.
A well designed disaster recovery plan will take into consideration the processing and operational needs of the organisation in addition to considering the potential problems their IT systems might be exposed to.

Contents of a disaster recovery plan
A disaster recovery plan will contain, at the very least, the following:–

1. The potential causes of the disaster - details of likely causes of potential disasters, for example, it may identify concerns relating to fire, theft of data or hardware, problems associated with continued power loss or telecommunication failure.

2. Assumptions being made in the writing of the plan, for example there is the assumption that all relevant staff involved in the implementation of the recovery plan is available to support its implementation.

3. The scope of the plan – it will identify the areas of the infrastructure covered by the plan. In the identification of the scope of the plan it may also detail the areas of the organisation supported by the services being identified, the impact of potential disaster to that area of the organisation and a priority for recovery for each of the areas.

4. Policies to support continuity of the infrastructure in areas identified in the scope of the plan.

5. Staff with responsibility for ensuring adherence to each area of the plan.

6. Plan of action - in addition to identifying the staff members or teams with responsibility for the recovery of each area of the organisations infrastructure, the plan will also identify the steps they need to take to ensure recovery. The plan of action may contain details of steps to be taken within a given time frame from immediate steps to steps to be taken at intermediate stages during the recovery stages to on-going steps to be taken following the disaster and recovery from it.

7. Revision and testing plan - any disaster recovery plan should be tested and reviewed on a regular basis.

Questions

1 A local sports centre store data such as members details, accident and incident reports and booking details in archives for a number of years after they are initially required.

a. Explain what is meant by "archiving data". [2]

b. Explain why archiving is necessary in this instance. [2]

c. Archived data is often indexed. Why is this necessary? [1]

.....

.....

.....

.....

.....

.....

2 Data is often backed up to ensure it can be recovered in the event of some kind of disaster.

a. Many smaller organisations may opt to carry out a full back-up as they store a relatively small amount of data. Identify two advantages and two disadvantages of a full backup. [4]

b. Alternative backup methods include incremental and full differential backups. Explain the difference between these two methods of backup. [4]

.....

.....

.....

.....

.....

.....

3 A bank needs to be able to be able to restore data quickly in the event of any kind of system failure. Identify an appropriate type of backup in this case and give 2 reasons to support your answer. [5]

.....

.....

.....

.....

.....

.....

.....

4 A local business has installed a new computer system. They have been advised by the analyst involved in the development process to invest in a Disaster recovery Plan.

a. Describe the main purpose of a disaster recovery plan and why it is so important for a business to have such a plan in place. [3]

b. Outline the main contents of a disaster recovery plan. [6]

.....

.....

.....

.....

.....

.....

.....

Bibliography

BCS Academy Glossary Working Party, 2013, *BCS Glossary of Computing and ICT*, 13th Edition, Swindon, BCS Learning and Development Ltd

5 Outline the difference between a Context DFD and a level 1 DFD.

.....

.....

.....

.....

.....

.....

.....

.....

Bibliography

BCS Academy Glossary Working Party, 2013, *BCS Glossary of Computing and ICT*, 13th Edition, Swindon, BCS Learning and Development Ltd