**Author:** *Alessandro Ferro*

**ICTSAS505**

**Task 1**

Question 1: Compare and contrast backup methodologies.

**Answer**

Data backup is commonly done in two ways:

Full backup: All data is backed up

Incremental backup: Only the data that has changed since the last back up are backed up.

Most companies use a combination of the two. Any time data is changed, they are copied as a safety measure. Then, a full back up is done at regular intervals

Following are the most common Data backu methods:

**Tape:** Old backup method. It’s inexpensive, but both backup and data recovery are slower and the tapes need to be physically stored and managed.

**Disk Mirroring:** Data is written on two disks at the same time. In case of disuption of a disk, the twin disk can replace it immediately without any loss of either data or service. It is faster than tape and also allows for data compression.

**RAID:** Similarly to disk mirroring, in RAID the data is written simoultaneously on an array of hard drives. When one of the drives fail, the next one can replace it with all the functions of the previous one.

**Hybrid cloud:** Data is secured on a local device and is then replicated in an off-site data center. The local backup grants a first security measure without any effect on perfomrance of the machines or of the internet connection. After business hours the data are automatically backed up in the cloud.

**Direct-to-cloud:** Data is stored directly in the cloud without making any local copy. It could be slower than the hybrid cloud and it can affect performances of the machines or internet connection. It is best suited for Saas (Software as a Service) data that already lives in the cloud.

Question 2: Explain the following business planning process relevant to the development of information and communication technology (ICT) business solutions.

**Answer**

* **Accounting/Finance:** It involves the management of assets, income and expenditure of a company, together with the related documentation.
* **Production/Service delivery:** The creation of the product or the the delivering of the service offered by a company.
* **Sales/Marketing:** Defines the promotion of a product or service and the related market researches and sale strategy.
* **Human resources:** Deals with the management of the workforce.
* **Administration:** CRUD and secretarial tasks.
* **Information services:** It maintains the IT and the communication infrastracture of a company.
* **Purchasing:** It manages the acquisition of products, assets or services, relevant to the business of a company.

Question 3: What do you think is included in IT Infrastructure? What are the steps in disaster recovery and contingency planning?

**Answer**

Included in IT infrastructure:

* Hardware
* Software
* Facilities
* Data Center/Data storage facilities
* Network systems
* System interfaces
* People that maintain, support and uses the system.

Following are the steps in Disaster Recovery and Contingency Planning:

* Identify critical business process and the associated hardware, software and data
* Identify riskss to hardware, software and data
* Identify risk management strategies
* Identify resources to implement strategies
* Prepare, compile procedures associated with disaster recovery and preventin strategies
* Identify criteria for implementing the plan
* Write the Disaster Recovery plan
* Obtain approval for the plan
* Implement the plan
* Test and Update the plan
* Revise the plan.

Question 4: What are the **two** categories of threats? List **three** examples of physical threats. List **three** examples of electronic threats. Why some companies don't want to back up their data? So you have a virus on your system. As long as it doesn't cause any corruption of data or disruption of business processes, why do you need to spend money to remove it?

**Answer**

* **Physical:**
  + Extreme weather: It includes cyclone, typhoon, hurricane, tsunamis, lightning, etc. It can lead to floods, rain and wind damage and blackouts. According to severity it can cause minor inconvenience or even a major disruption of the business.
  + Fire: Flames and smoke can be extremely dangerous for people, electronic equipment and buildings. Fire can have disastrous consequences, but even a minor one can still have consequences, such as water damage and toxicity.
  + Earthquake: Can damage or destroy buildings and infrastractures and disrupt important services such as telecommunications, water, gas and electricity.
* **Electronic:**
  + Hackers: Can gain access to a system for malicius purposes.
  + Hardware and Software failure: Can impact the ability to perform business functions. Especially if appropriate measures are not in place.
  + Telecommunications and power outages: Same as above.

Reasons why some companies don’t want to backup their data:

* Equipment and resources allocated to data backup cost money and can be time consuming.
* They lack the techincal expertise.
* They underestimate or are unaware of the risks associated with the loss of data.
* Data are not critical to the business continuity.

Nonetheless, data backup should always be considered mandatory when planning for disaster prevention and recovery.

Virus should always be removed because even the most simple ones can be dangerous for the health of a system. A simple virus that can replicate itself can easily consume all the available memory, causing a system failure. Other virus can also navigate through a network, causing infections on a large number of machines in a little amount of time.

Question 5: List **five** measures used to prevent and/or minimize the effect of fire damage. List **two** types of fire detectors. List **three** measures to secure your building and protect data and equipment. List three strategies to manage power problems? What is the best strategy against water damage (not including flood)?

**Answer**

Measures to prevent or minimize fire damage:

* Fire hydrants
* Fire hose Reels
* Fire doors
* Fire extinguishers
* Automatic fire suppression systems

Fire detectors:

* Air Sampling Detectors
* Rate of Heat Rise Detectors

Building and equipment security measures:

* Lock and Key
* Highly Technological Scans: Fingerprints, face or biometrics scanning.
* Surveillance

Strategies to manage power issues:

* UPS (Uninterruptible Power Supply)
* Surge Arrestor
* Stand-by Generators

The best strategy to adopt against water damage (not including floods) is prevention. A monitoring system can detect leaks at an early stage, allowing for quick action.

# **Unit Assessment Result Sheet (UARS)**

## **Assessment Task 1 – Unit Knowledge Test (UKT)**

## **Student and Trainer/Assessor Details**

|  |  |
| --- | --- |
| **Unit code** | ICTSAS505 |
| **Unit name** | Review and update disaster recovery and contingency plans |
| **Outcome of Unit Assessment Task (UAT)** | |  | | --- | | **First attempt:** |   Outcome (please make sure to tick the correct checkbox):  Satisfactory (S)  or Not Satisfactory (NS)  Date: \_\_\_\_\_\_\_(day)/ \_\_\_\_\_\_\_(month)/ \_\_\_\_\_\_\_\_\_\_\_\_(year)   |  | | --- | | **Second attempt:** |   Outcome (please make sure to tick the correct checkbox):  Satisfactory (S)  or Not Satisfactory (NS)  Date: \_\_\_\_\_\_\_(day)/ \_\_\_\_\_\_\_(month)/ \_\_\_\_\_\_\_\_\_\_\_\_(year) |
| **Feedback to Student** | |  | | --- | | * **First attempt:** |  |  | | --- | | * **Second attempt:** | |
| **Student Declaration** | * I declare that the answers I have provided are my own work. Where I have accessed information from other sources, I have provided references and or links to my sources. * I have kept a copy of all relevant notes and reference material that I used as part of my submission. * I have provided references for all sources where the information is not my own. I understand the consequences of falsifying documentation and plagiarism. I understand how the assessment is structured. I accept that all work I submit must be verifiable as my own. * I understand that if I disagree with the assessment outcome, I can appeal the assessment process, and either re-submit additional evidence undertake gap training and or have my submission re-assessed. * All appeal options have been explained to me. |
| **Student Signature** |  |
| **Date** |  |
| **Trainer/Assessor Name** |  |
| **Trainer/Assessor Declaration** | I hold:  🗹 Vocational competencies at least to the level being delivered  🗹 Current relevant industry skills  🗹 Current knowledge and skills in VET, *and undertake*  🗹 Ongoing professional development in VET  *I declare that I have conducted an assessment of this candidate’s submission. The assessment tasks were deemed current, sufficient, valid and reliable. I declare that I have conducted a fair, valid, reliable, and flexible assessment. I have provided feedback to the above-named candidate.* |
| **Trainer/Assessor Signature** |  |
| **Date** |  |
| **Office Use Only** | Outcome of Assessment has been entered onto the Student Management System on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (insert date)  by (insert Name) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |