Guilherme Felipe Schneider - 18539

Project Link: https://guischneider100.github.io/copcp-18539/

Task 1: 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?

- Taking into account the issue of cost-benefit for website development, how does the process translate the amount invested into concrete results?

- How will this specific process help your company sell better, build customer loyalty and successfully fulfill a mission in line with your main objective?

- Will this process perform to its full potential if you decide to go ahead without providing the technology it needs?

- Faced with the issue of productivity, is the time invested worth spending compared to the results that can be observed?

Task 2: 1. What issues need to be considered for backup and restoration of data?

The treatment of data through backup is a very important point at the time of a possible restoration, the main points that must be evaluated are:

- backup location: the definition of a save location is a very important point in terms of the speed at which the restoration can be performed and the security of the data so as not to be lost or invaded;
- data consistency: backups must be regularly tested to prevent them from being recorded with inconsistencies and becoming useless in the future;
- auditing: the lack of auditing of backups can cause loss of important information for performing a safe restoration.

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

If proper security measures such as encryption and access controls are not in place, a lot of sensitive data can become vulnerable to unauthorized access, data breaches or malicious attacks.

Task 3: 1. How critical is this system to the organisation? Why?

Taking into account the high level of cost presented in the first 3 points addressed in the table, valuing the extreme importance of dependence on the customer and supplier relationship, this system would be extremely critical for the company, provided that if the company's website is not available for In a short period of time, other options become available to the user, generating a huge loss of trust between the customer and the company.

2. The person who completed the form claimed that 30 minutes is the maximum time the system can be down. Does this figure apply to a 24-hour trading period?

If the maximum system downtime is 30 minutes, this generally refers to a single instance of downtime rather than a cumulative duration over a 24-hour trading period. The system must not be idle for more than 30 minutes at any one time. If the system experiences multiple instances of downtime within a 24-hour trading period, the cumulative downtime may exceed 30 minutes.

Task 4:

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

Task 5: 1. What are the critical data and software areas for this system?

- Students personal registration information: all personal information must be kept extremely secure to prevent attacks or leaks;

- Test download and storage: the system needs to create and maintain secure ISDN connections with each vendor in order to download the necessary tests;

- Test results: all the test results must be kept extremely secure to prevent unauthorized data access by students;

- Accounting processes: the system must ensure receipt of all student expenses and control the tests that are charged by the supplier;

- Result management: the system should record and store test results for each student, as well generate and print certificates for students who pass the tests.

2. What are the potential threats to the system and testing facility?

- Disasters that stop the center operating such as fire, flood, earthquake;

- Hardware problems that stop the system operating;

- Credit card fraud. With the short time frame involved, the student could be tested before any credit card discrepancy is identified;

- Student not turning up and exam lapses so $50 is lost;

- Broken ISDN links delay download of exams;

- Hackers trying to access test data or student data;

- Internal unauthorized access to test data or student data;

- Theft or misappropriation of test certificates.

Task 6:

Threat	Options	Cost (1-5)	Business requirements (1-5)
Disasters that stop the center operating such as fire, flood, earthquake.	Secondary data centers or colocation facilities / Business Continuity Planning.	5	3
Hardware problems that stop system operating.	Monitor device performance / Updating and patching systems to eliminate vulnerabilities / Replace aging hardware before it fails.	2	5
Credit card fraud. With the short time frame the student could be tested before any credit card discrepancy was identified.	Robust security measures / Adherence to card data security standards / Fraud insurance	5	4
Student not turning up and exam lapses so $50 is lost.	Registration process that requires students to confirm their attendance / Fee policies and refunds	2	2
ISDN links broken delaying download of exams.	Multiple ISDN lines / Alternative connection methods	4	4
Hackers who may try to access test data or student data.	Encryption / Firewalls / Monitoring network / MFA	4	5
Internal unauthorized access to test data or student data.	MFA / Encryption / Training of data security	4	5
Theft or misappropriation of test certificates.	Secure storage protocols	1	5

Task 7:1. What RAID may give 4phones

- Partitioning between multiple disks that tolerates faults, the risk of data loss due to disk failure is significantly reduced, and allows the system to continue running without bottlenecks;

- Better disk access performance due to data distribution and processing;

- Good cost-benefit;

- Rapid recovery capability.

2. Threats to be safeguarded against

- Disk failure;

- Permanent data loss;

- System downtime;

- Backup reliance.

3. Cost benefit analysis (Assume 50% would go elsewhere if the system is down)

- RAID system: $12,000;

- The loss of server: $100,000 in terms of lost orders placed on the web;

- 50% of $100,000: $50,000 loss;

4. How RAID supports the business

- 24X7 operation as a business strategy;

- Data protection and integrity;

- 99.9% uptime as a SLA requirement;

- Improved system performance;

- Provides fault tolerance.

Task 8: 1. Rewrite the procedures to reflect the current virus protection processes and to improve the way users operate.

- All software new or present on the network must be checked through a complete virus scan before eventual installation;

- All computers must contain standard virus protection software, which must be updated regularly through schedules;

- Virus checking software should be run constantly for general evaluation of files and other software, not just isolated cases like floppy disk insertion;

- All protection software must be constantly running and must never be paused or interrupted;

- All protection software must be constantly running and must never be paused or interrupted;

- The use of any email service must be protected against any type of attack, and users must be aware of the same;

- Users should exercise caution when downloading software from the Internet and only reputable sources should be used;

- If any virus activity is suspected the user must shut down their workstation and inform the IT department.

2. You will need to recommend hardware or software purchases to improve backup and recovery in the event of a disaster.

Having reviewed and chosen IBM Cloud Object Storage as a disaster enhancement software, the following topics were covered:

Backup recommendations

IBM Cloud Object Storage provides the following features that will be used to improve the backup procedures:

- **Resilient and available:** IBM Cloud Object Storage geo-disperse capabilities provide backup and data protection. It's always accessible, even in disaster or multiple failure cases.

- **Cost-efficient:** multiple storage classes help optimize backup cost and data recovery objectives with pay-as-you-go pricing and no up-front capital investments.

- **Durable:** data-integrity mechanisms check, validate and apply self-repair capabilities. It's designed for data durability of 99.9%. Individual results vary.

- **Fast data recovery:** a single API helps data recovery for business continuity. Access backup data faster with tape storage to aid regulatory, legal or business needs.

- **Security-rich:** default server-side encryption keys are automatically managed by default. You can manage your own keys or use IBM Key Protect.

- **Scale on demand:** seamlessly scale to meet your needs to make it easier to cost-effectively manage and meet data protection requirements across your enterprise.

Backup procedures

- Automatic regular overnight backup of all data;

- Designation of enough or greater space for the volume of data;

- Backup in time before the work starts;

- Quick and easy recovery provided from the "last changed file" that is used for backup;

- All the backups and their relative tapes will be recorded in a log system to have a control about reutilization.