Wells International College

18574  Jorge Trujillo

Contribute to Organizational Privacy and Contingency Plans

|  |  |  |  |
| --- | --- | --- | --- |
| Name of Student | Jorge Eduardo Trujillo Paez | ID | 18574 |

# Assessment 1- Case Study

Contents

[Assessment 1- Case Study 2](#_Toc136763947)

[Instructions 3](#_Toc136763948)

[Task 1: 4](#_Toc136763949)

[Task 2: 6](#_Toc136763950)

[Task 3: 8](#_Toc136763952)

[Task 4: 10](#_Toc136763953)

[Task 5: 12](#_Toc136763954)

[Task 6: 14](#_Toc136763955)

[Task 7: 15](#_Toc136763956)

[Task 8: 17](#_Toc136763957)

# Instructions

This task is to be completed individually. You need to analyse number of case scenario related to professional conduct, Intellectual property, copyright, privacy and contingencies and complete all the tasks or answer all the questions provided after each scenario.

You need Internet access to analyse and complete some of the tasks.

#### Duration:

Trainer will set the duration of the assessment.

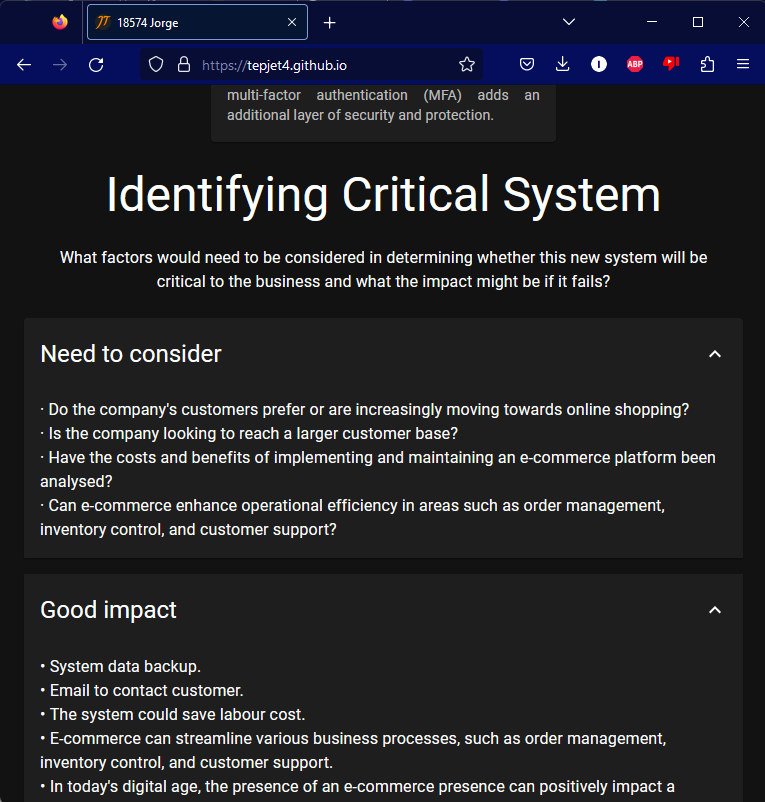
#### Scenario 1: identifying critical systems

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.

# 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?

Write at least 4 questions you need to consider.

Do the company’s customers prefer or are increasingly moving towards online shopping?

Is the company looking to reach a larger customer base?

Have the costs and benefits of implementing and maintaining an e-commerce platform been analysed?

Can e-commerce enhance operational efficiency in areas such as order management, inventory control, and customer support?

Good impact:

* System data backup.
* Email to contact customer.
* The system could save labour cost.
* E-commerce can streamline various business processes, such as order management, inventory control, and customer support.
* In today's digital age, the presence of an e-commerce presence can positively impact a brand's perception. Consumers may view a business without an E-commerce as outdated or less trustworthy, affecting the overall brand reputation.

Impact if failure:

* If the e-commerce becomes a significant revenue channel, its failure can result in a decline in sales and revenue.
* Frustrated customers may turn to competitors if they cannot easily purchase products online.
* If the system is not successful the cost of the system development would be a loss.

URL:

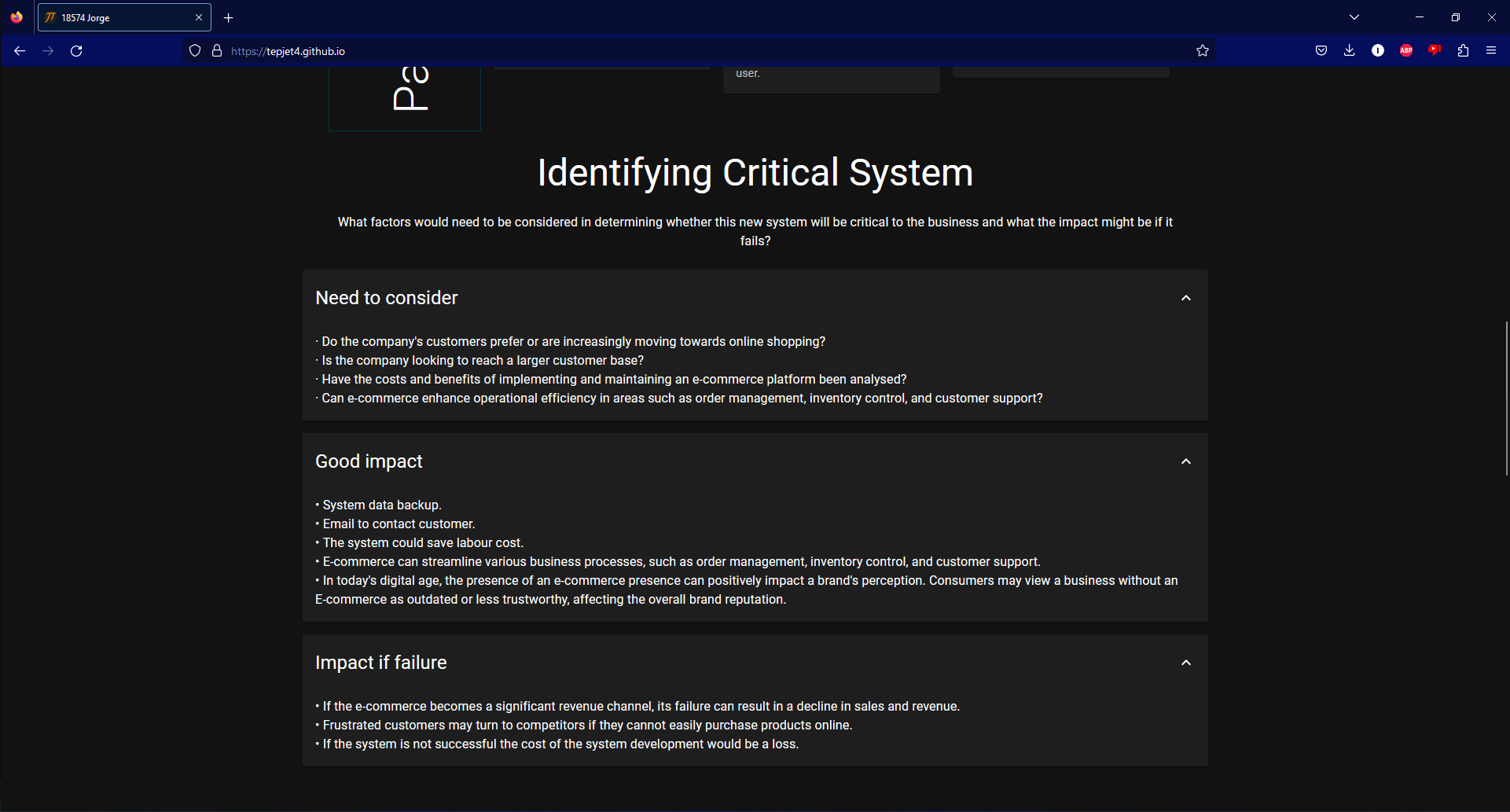
<https://tepjet4.github.io/>

#### Scenario 2: analysing critical areas

You have been given the following form for the Urban Wear e-commerce site. Most of the data will be input online via the Internet.

Table 1: critical areas

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Update corporate data files** | **Create own data files** | **Create shared documents** | **Create own temporary documents** |
| **From source documents** | 70% | 50% | 20% | 20% |
| **From other data files** | 10% |  |  |  |
| **From irrecoverable sources such a telephone call** |  |  |  |  |
| **Developed at the workstation such as report writing** | 0 |  |  |  |
| **Other—specify** | 0 | 50% | 50% | 0 |



# Task 2:

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

* The frequency of data backups should be determined.
* An appropriate storage medium for backups, such as external hard drives, network-attached storage (NAS), cloud storage, or tape drives, should be selected.
* Encryption measures should be implemented to secure the backup data, ensuring confidentiality during storage and transmission.
* Automated backup solutions or scripts should be considered to streamline the backup process and minimize the risk of human error.

1. **What problems can occur with backing up online transactions?**

* Maintaining the integrity of online transactions during the backup process is crucial. If backups are taken while transactions are still in progress or incomplete, it can result in inconsistent or corrupted data during restoration.
* Online transactions often involve sensitive customer information, such as payment details or personal data. Backing up this data requires strong security measures to protect against unauthorized access or data breaches.
* Performing backups of online transactions may require temporary system downtime or reduced availability.

## Credit Card Transaction Processing Online Payment System Ppt PowerPoint Presentation Show - PowerPoint Templates

Addressing these problems requires careful planning, implementation of robust backup solutions, adherence to security best practices, and regular testing and validation of backup and restoration procedures. It is crucial to ensure that online transaction data is effectively protected and can be restored accurately to maintain business continuity and safeguard customer information.

#### Scenario 3: determining system criticality

Consider the case study of Urban Wear again. You have the following information about its e-commerce system.

Table: Analysing critical areas: impact of system down for less than 1 hour.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Very costly** | **Serious** | **Little or no effect** |
| **Impact on cash flow** | X |  |  |
| **Impact on profitability** | X |  |  |
| **Impact on customer or supplier relations** | X |  |  |
| **Impact on legal requirements** |  |  | X |
| **Impact on staff or morale** |  |  | X |

Some questions and answers related to the impact of critical areas:

* Are there any other implications? Please specify.
  + We expect to do 50% of our business online within one year. As the products we sell are readily available from our competitors, it is likely that customers would purchase elsewhere.
* Estimate the maximum amount of time you could operate without access to the system?
  + 30 minutes
* Are there any peak periods when the impact of a disruption would be more serious?
  + Christmas sales time from mid-November until Christmas Eve.
  + Public holidays
  + School holidays
* Are there any applications or data that you believe must be continuously available?
  + No—subject to no more than 10 minutes downtime



It's essential for businesses to prioritize the stability and availability of their e-commerce sites to minimize the impact of downtime. Implementing measures such as redundancy, proactive monitoring, and quick response to resolve any issues can help mitigate the negative consequences and ensure uninterrupted service for customers.

# Task 3:

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

An E-commerce plays a critical role in the success and growth of the retailer. It enables expanded market reach, convenience for customers, increased sales opportunities, competitive advantage, data-driven decision-making, brand building, and the flexibility to integrate with other sales channels.

1. 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?

This maximum downtime could vary depending on how busy the web traffic is:

* On weekends, public holidays, max should be 10 minutes.
* On normal working days, max can go up to 30 minutes.
* At low traffic hours, mid night to 6 am, max can go up to 60 minutes.
* Overall, the goal is to provide a seamless and uninterrupted online shopping experience for customers, and minimizing downtime is crucial to achieve that objective.

#### Scenario 4: identifying possible threats

A small communications company, 4phones, is about to introduce an e-commerce system. A list of the possible threats to the system has been provided below.

Table: Threats

|  |  |
| --- | --- |
| **Threat** | **Category** |
| Hackers attempting to get to the data stored on the site.   * Change data * Delete data * Add fake or wrong data | External\* |
| Hardware failures that stop the site operating.   * Hard disk broken * Power supply down * Cable is failed to link | Internal |
| Denial of service attacks to bring the service down.   * Service disruption * Financial losses * Damage to reputation | External |
| Data destruction by any means such as a user deleting a file.   * System Failures * System restoration from outdated backup | Internal |
| Misuse of information by internal staff.   * Potential Identity theft | Internal\* |
| Power problems so site is down.   * Financial losses | External |
| Overloaded site so response is slow.   * Bad user experience * Need to review code or increase system resources | External |
| Customers falsifying information to avoid payment.   * Financial losses | External |
| Incorrect information such as wrong prices so customers pay too little.   * Financial losses | Internal |
| Incorrect information such as wrong quantity in stock so customers have to wait for delivery.   * Bad purchasing experience for customers | Internal |
| Major disaster so site is down.   * Earthquake, bushfire, terrorist attacks * Site could be down for an extended period | External |
|  |  |

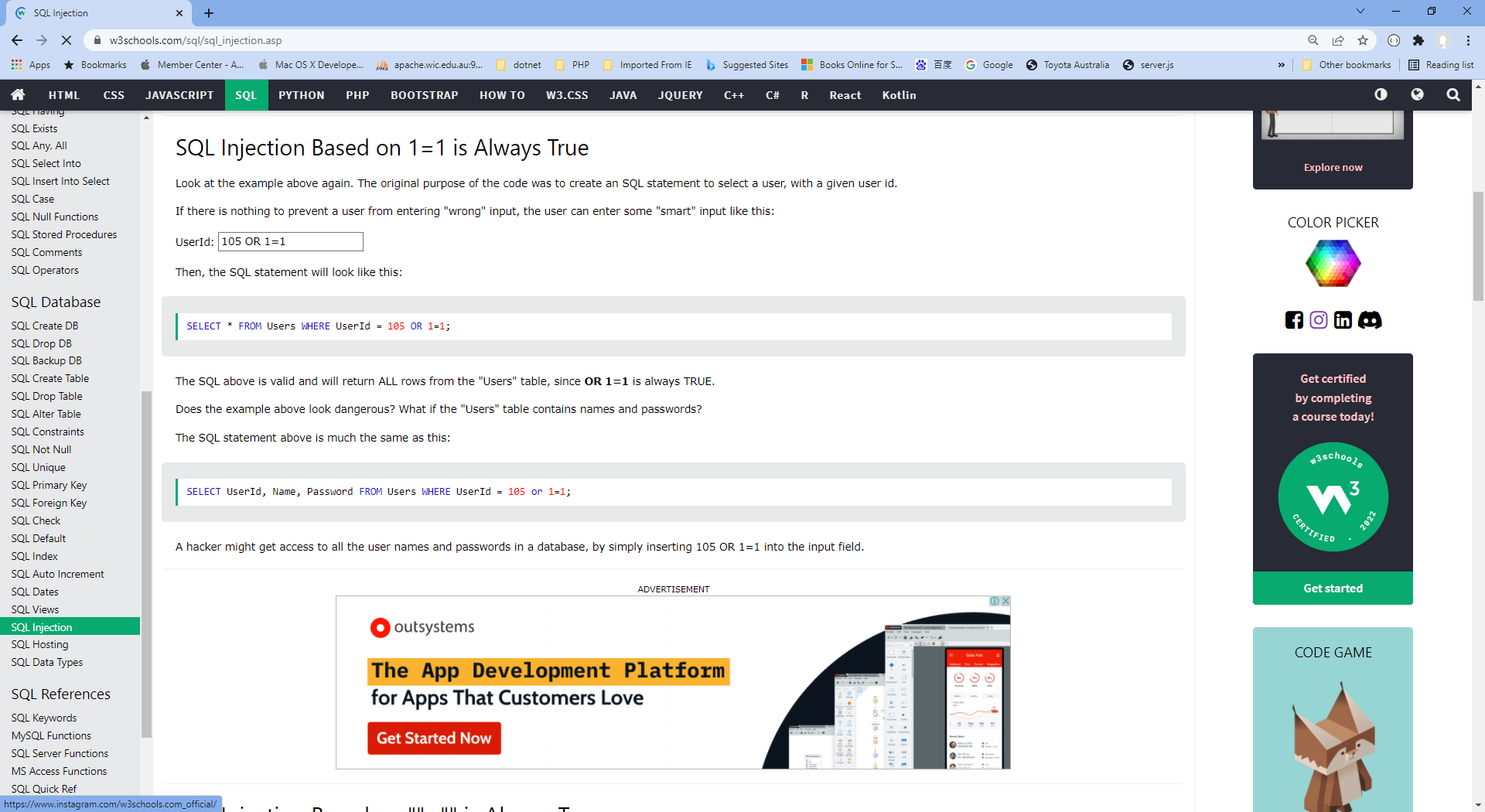
# Task 4:

Identify whether they are internal or external and flag with an \* any threats that are also security threats.

Example:

SQL injection:

<https://www.w3schools.com/sql/sql_injection.asp>



Thoughts:

To mitigate these threats, e-commerce sites should implement a comprehensive security strategy that includes measures such as strong access controls, regular security assessments, encryption of sensitive data, employee training on security best practices, robust network and application security, and monitoring and response mechanisms to detect and address security incidents promptly.

#### Scenario 5: identifying critical systems and threats

You are working for CIT (City Institute of Technology), an educational organisation that has an annual turnover of $2M. They intend to implement a new system to test students using computerised systems. These tests will include vendor exams such as Microsoft MCSE, Novell CNA, etc.

The following are extracts from the business case and other project documentation that has been developed for this project.

Computerised testing system is a competitive and growing area of business. There are currently five test centres in the city in which CIT is located. Anyone can take these tests: studying with the organisation is not a prerequisite. Students only need to give one day’s notice in order to sit the test.

To gain a marketing edge, CIT proposes that:

* students will only be required to give an hour’s notice prior to being tested. The student will call the test centre to be registered on the new system. They will be given a log-in account and a password and can come to the centre at any time after one hour has elapsed. They will pay by credit card or bring cash to the centre where they log-in and take the test.
* the centre will be open between 5 am and 11 pm, seven days a week.
* the centre expects to be able to process 20 students per hour and will make a profit of $100 per student.
* for security reasons, no tests will be stored at a test centre. Each centre will have an ISDN link with each of the vendors who supply the tests. There will be five such links. When a student registers, an automatic message is sent to the vendor and a test is downloaded to a server at the test centre. The centre must pay $50 for this test even if, for some reason, it does not get used. The test will expire after 12 hours.
* if a student passes the test, they will be presented with a certificate, which is printed at the centre. The centre will keep stocks of these certificates for each vendor.
* student information and test results will be stored on the server and each evening at the close of business this information will be sent to the appropriate vendor. Vendors exercise strict control over test centres and any centre that does not follow the contract obligations may have its test facility refused and suffer financial penalties.

The testing centres are viewed as potential ‘one stop shops’ offering, examination preparation courses as well as tests. Students will study a subject and then take the exam all for an exclusive fee. There is a lot of money to be made as students are willing to pay $5,000 or more to become qualified. The organisation aims to process around 200 students per month.



# Task 5:

##### What are the critical data and software areas for this system?

* + Questions random selection
  + Students’ answers
  + Test results
  + Verification of students’ identity
  + Follow each test’s requirements

##### What are the potential threats to the system and testing facility?

* + Hack the question
  + Get answer key
  + System going down
  + Cheating on exam
  + Identity supplantation

Strong measures have to be taken into place to safeguard students’ personal information, a reliable system that links each student to each test, a good contingency plan must be created in case of system failure.

#### Scenario 6: evaluating preventive and recovery options

The Windsor Institute of Commerce (WIC) will implement a new system to test students using computerised testing systems. These tests will include vendor exams such as Microsoft MCSE, Novell CNA, etc.

Before implementing the system, you need to evaluate potential threats and for each threat:

* evaluate what can be done to prevent/minimise or recover from the risk
* consider whether the option would be costly to implement on a scale of 1 to 5 (highest)
* Indicate whether the option should be considered an important or essential business requirement on a scale of 1 to 5 (highest).

# Task 6:

Use the following table to complete your evaluation.

Table: preventive and recovery options

|  |  |  |  |
| --- | --- | --- | --- |
| **Threat** | **Options** | **Cost (1-5)** | **Business requirement (1-5)** |
| Disasters that stop the centre operating such as fire, flood, earthquake | Backup System in Different location | 5 | 4 |
| Hardware problems that stop system operating | Best quality hardware | 4 | 5 |
| Credit card fraud. With the short time frame the student could be tested before any credit card discrepancy was identified. | Utilize fraud detection tools and services that employ advanced algorithms and machine learning to identify patterns and anomalies | 5 | 5 |
| Student not turning up and exam lapses so $50 is lost. | Attempt to reallocate test to a different student | 1 | 5 |
| ISDN links broken delaying download of exams | Multiple pathways to tests | 3 | 3 |
| Hackers who may try to access test data or student data | Fire wall | 1 | 5 |
| Internal unauthorised access to test data or student data | Strict authentication system with user roles | 2 | 5 |
| Theft or misappropriation of test certificates | Test certificate should be invalid without propper seal | 1 | 1 |

#### Scenario 7: presenting a strategic recommendation

 After completing the risk analysis for the 4phones e-commerce project, you believe that RAID (Redundant Array of Inexpensive Disks) should be used in the server to prevent hardware failure. You also wrote a report that justifies your decision.

RAID (redundant **array of independent disks**) is a data storage virtualization technology that combines multiple physical **disk** drive components into a single logical unit for the purposes of data **redundancy**, performance improvement, or both.

You covered the following matters in your report:

* The use of RAID will protect against the failure of a single disk in the server. Since disks are electromechanical devices, they are the most susceptible component to wear and tear and subsequent breakdown. They also store the data that may be difficult or impossible to recover depending upon when the breakdown occurs. They will not protect against other hardware failures such as power failures or major disasters such as fire.
* The server has been identified as a critical component in the system and its loss could cause considerable problems and loss of revenue and profit.
* All parts of the system will be impacted by the loss of disks in the server. The cost to the business of losing the server disks for a day could be $100,000. (Orders placed on the web $100,000 per day)
* The only current facility to cope with such an event is to restore from backup. This takes four hours during which time we would not be able to operate the system. In addition, the backup tapes could be on average 12 hours old and so will not have current information.
* While we will eventually have a high-speed link to a backup site, the use of RAID provides a cost-effective solution until this link is established in 10 months’ time.
* The cost of a RAID system would be in the region of $12,000. We will also gain an improvement in the performance of disk access in the region of 10%.
* If this recommendation is approved, we can order the RAID components and have it installed and operating within a week.

# Image result for Redundant Array of Inexpensive Disks Task 7:

Write some notes to support your RAID recommendation as a method of preventing hardware failure for the 4phones e-commerce project on the following topics:

1. What RAID may give 4phones

* Fault tolerance as regards disk drives
* Improved performance
* No down time for single disk failure
* Hot swap to replace faulty disk

1. Threats to be safeguarded against

* Disk failure
* Multiple controllers also guard against disk controller failure
* Duplicate power supply guards against power supply failure
* If system unit goes down RAID may be quickly connected to another unit.

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

* Orders placed on the web = $100,000 per day
* Assume 50% would go elsewhere if our system down
* Loss = $50,000
* RAID setup costs only $12,000
* If system is likely to go down for 6 hours total (during lifetime of the RAID system) because of a storage error, then the cost of a RAID system is justified.

1. How RAID supports the business

* 24X7 operation is a business strategy
* 99.9% uptime is an SLA requirement
* RAID provides fault tolerance to meet these requirements

Implementing a RAID (Redundant Array of Independent Disks) system in a server is not an absolute necessity, but it can provide several benefits in terms of data redundancy, fault tolerance, and improved system performance.

#### Scenario 8: reviewing procedures

You have been reviewing the procedures and actual operation of users in relation to virus checking. The current procedures, which were written several years ago, are as follows:

All software loaded on the network should have first been checked for virus contamination. This also applies to shrink-wrapped (brand new) software. The virus checking program selected should be regularly updated to protect against new viruses.

A review of the software and virus files used in checking found the following:

1. The software and files are two years old.
2. No new virus files have ever been obtained.
3. Users only run virus scanning software when they insert a floppy disk.
4. users will often download software from the Internet
5. E-mail is used extensively.
6. Documents are regularly exchanged.

The risk analysis and DRP process recognised viruses as a serious risk that could have a major impact on the organisation.

Viruses can be accidentally or deliberately introduced through infected files or software. Originally only found only in executable programs, viruses can now be carried by other documents, especially Word documents transmitted by e-mail.

New viruses are regularly created and with the increased use of e-mail and the Internet, the risk of a virus attack has also increased. This means that users have to be particularly vigilant and that virus checking of files has to be the norm, not the exception.

# Task 8:

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

In today's digital world, we rely on internet-connected devices for various aspects of our lives. Whether we're searching for information, shopping, banking, studying, gaming, or socializing, our devices hold valuable personal information that we must safeguard. Without proper protection, identity thieves and hackers can access and exploit our data, leading to financial loss and privacy breaches. Here are essential tips to reduce your online risks:

Keep your device secure:

* Download recommended updates for your device's software, including the internet browser.
* Use antivirus software, antispyware software, and firewalls to fend off attacks.

Stay up to date:

* Regularly update your system, browser, and important apps.
* Enable automatic updates whenever possible to fix vulnerabilities and protect your information.

Use antivirus software:

* Install and regularly update antivirus software to defend against viruses and spam.
* Configure your antivirus software to scan your system daily.

Employ antispyware software:

* Prevent spyware installation by downloading software only from trusted sources.
* Use antivirus software with built-in spyware protection or consider standalone antispyware programs.

Utilize firewalls:

* Activate and update firewalls to block unauthorized access to your computer.
* Particularly important for high-speed internet connections like DSL or cable.

Strengthen protection:

* Employ strong passwords and authentication methods for your accounts.
* Choose unique passwords and consider using password manager software.

Protect your private information:

* Be cautious while clicking on links and sharing personal data online.
* Beware of phishing attacks and verify email addresses before providing sensitive information.

Shop safely:

* Research websites before entering personal information.
* Look for secure indicators such as "https" or a padlock icon.

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

Network Attached Storage (NAS): A NAS device can be purchased, providing a centralized storage solution for backups. Built-in redundancy features are often included, and integration into the existing network infrastructure is made easy.

External Hard Drives: External hard drives with ample storage capacity can be purchased to create additional backup copies of critical data. These drives can be used for local backups and stored in a secure offsite location.

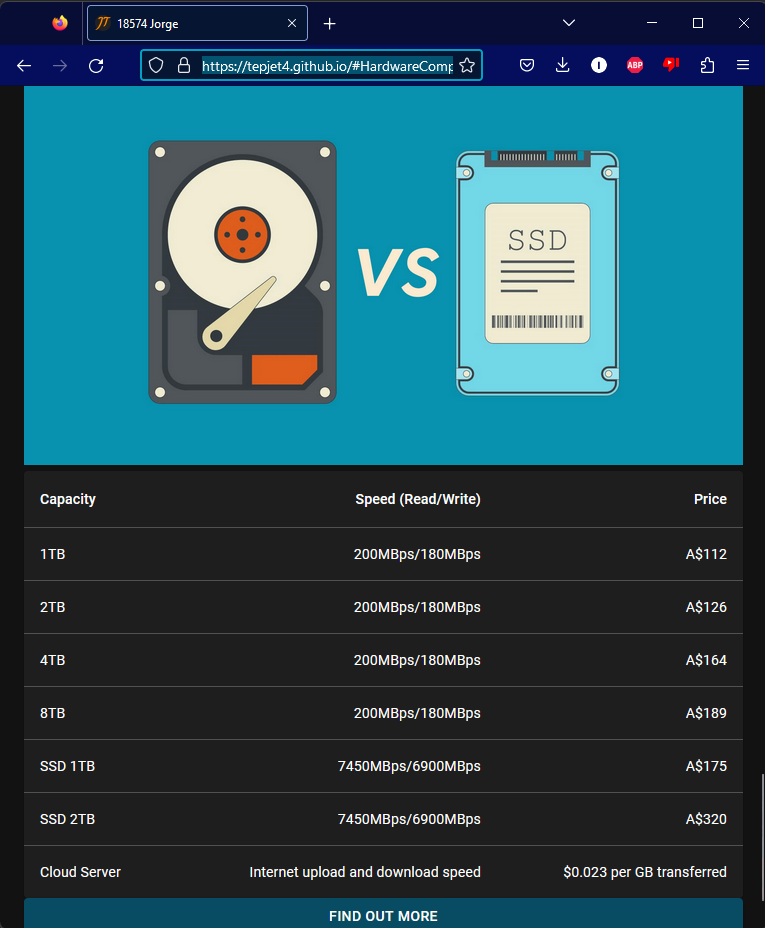
Typical hardware specifications and costs are:

|  |  |  |
| --- | --- | --- |
| Capacity | Speed(read/write) | Price |
| 1TB | 200MBps/180MBps | A$112 |
| 2TB | 200MBps/180MBps | A$126 |
| 4TB | 200MBps/180MBps | A$164 |
| 8TB | 200MBps/180MBps | A$189 |
| SSD 1TB | 7450MBps/6900MBps | A$175 |
| SSD 2TB | 7450MBps/6900MBps | A$320 |
| Cloud Server | Internet upload and download speed | $0.023 per GB transferred |

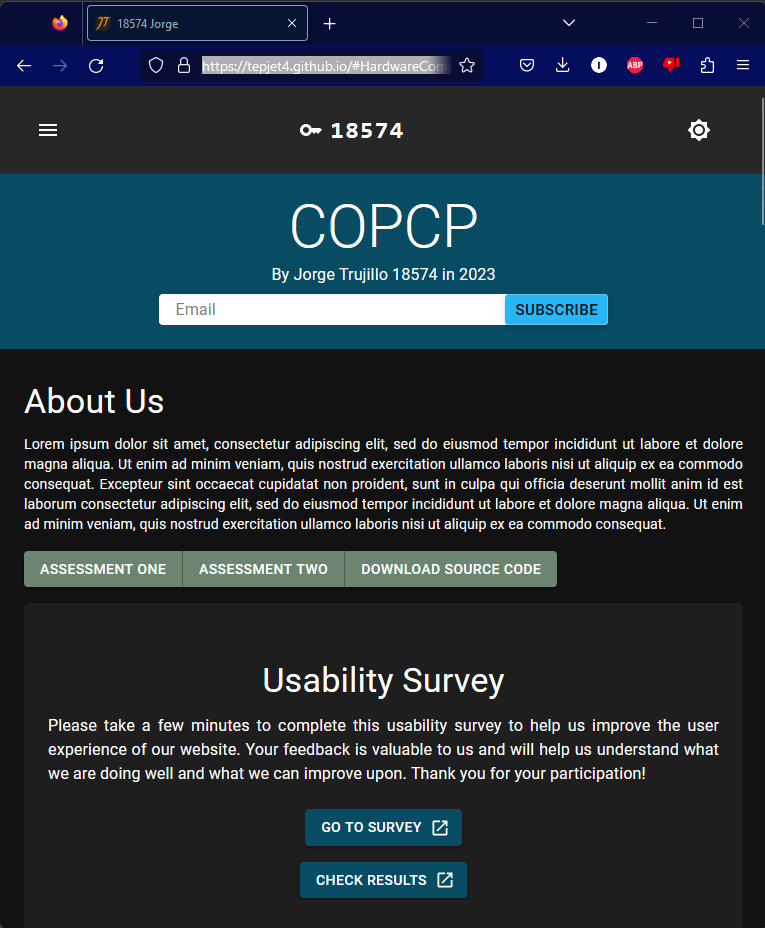
Software Purchases:

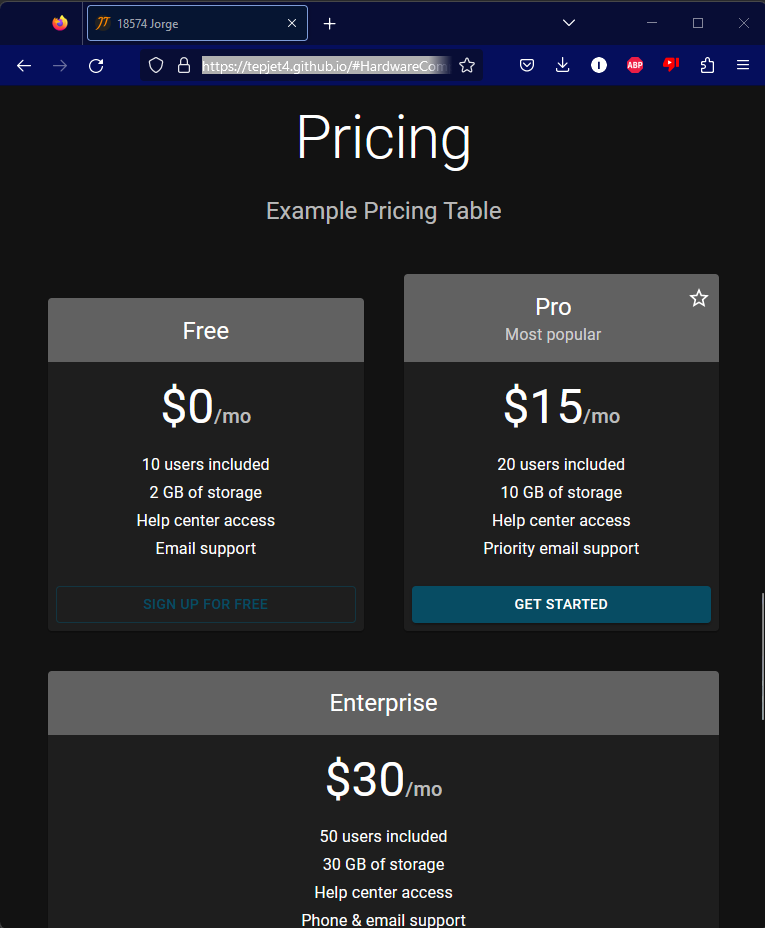
* Backup and Recovery Software: Robust backup and recovery software can be purchased, offering features such as scheduled backups, incremental backups, encryption, and easy data restoration. Solutions like Acronis True Image, Veeam Backup & Replication, or Backup Exec can be considered.
* Cloud Backup Solutions: Explore cloud backup services that automatically store data in secure offsite servers.

<https://tepjet4.github.io/#HardwareComparison>



Below these is my web contents support.



<https://tepjet4.github.io/>