Wells International College

[Company name]  [Company address]

Contribute to Organizational Privacy and Contingency Plans

|  |  |  |  |
| --- | --- | --- | --- |
| Name of Student | Kevin Wen | ID | 18549 |

# Assessment 1- Case Study

Contents

[Assessment 1- Case Study 2](#_Toc65661060)

[Instructions 3](#_Toc65661061)

[Scenario 1: identifying critical systems 4](#_Toc65661062)

[Scenario 2: analysing critical areas 4](#_Toc65661063)

[Scenario 3: determining system criticality 5](#_Toc65661065)

[Scenario 4: identifying possible threats 7](#_Toc65661066)

[Scenario 5: identifying critical systems and threats 7](#_Toc65661067)

[Scenario 6: evaluating preventive and recovery options 10](#_Toc65661068)

[Scenario 7: presenting a strategic recommendation 11](#_Toc65661069)

[Scenario 8: reviewing procedures 13](#_Toc65661070)

[Index 15](#_Toc65661071)

# 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.

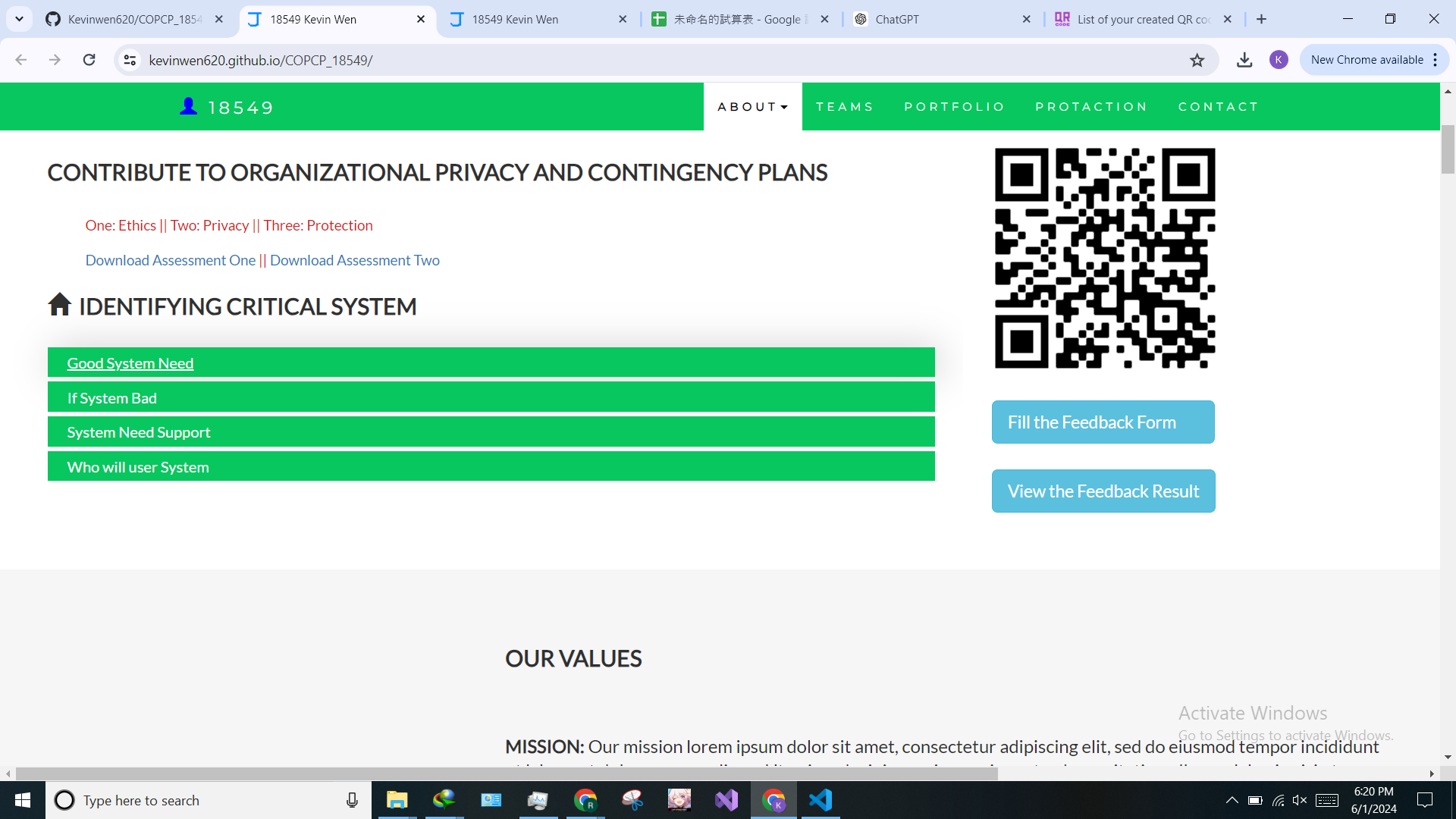
Good impact:

* Report daily profit and lost using system
* System data back up
* Email to contact customer
* The best system could save labour cost
* How much money could be saved if open online shop
* …

Bad side:

* if fail down, you will be lost customer
* need easier to contact to customer
* could be big cost
* …

URL: <https://kevinwen620.github.io/COPCP_18549/>



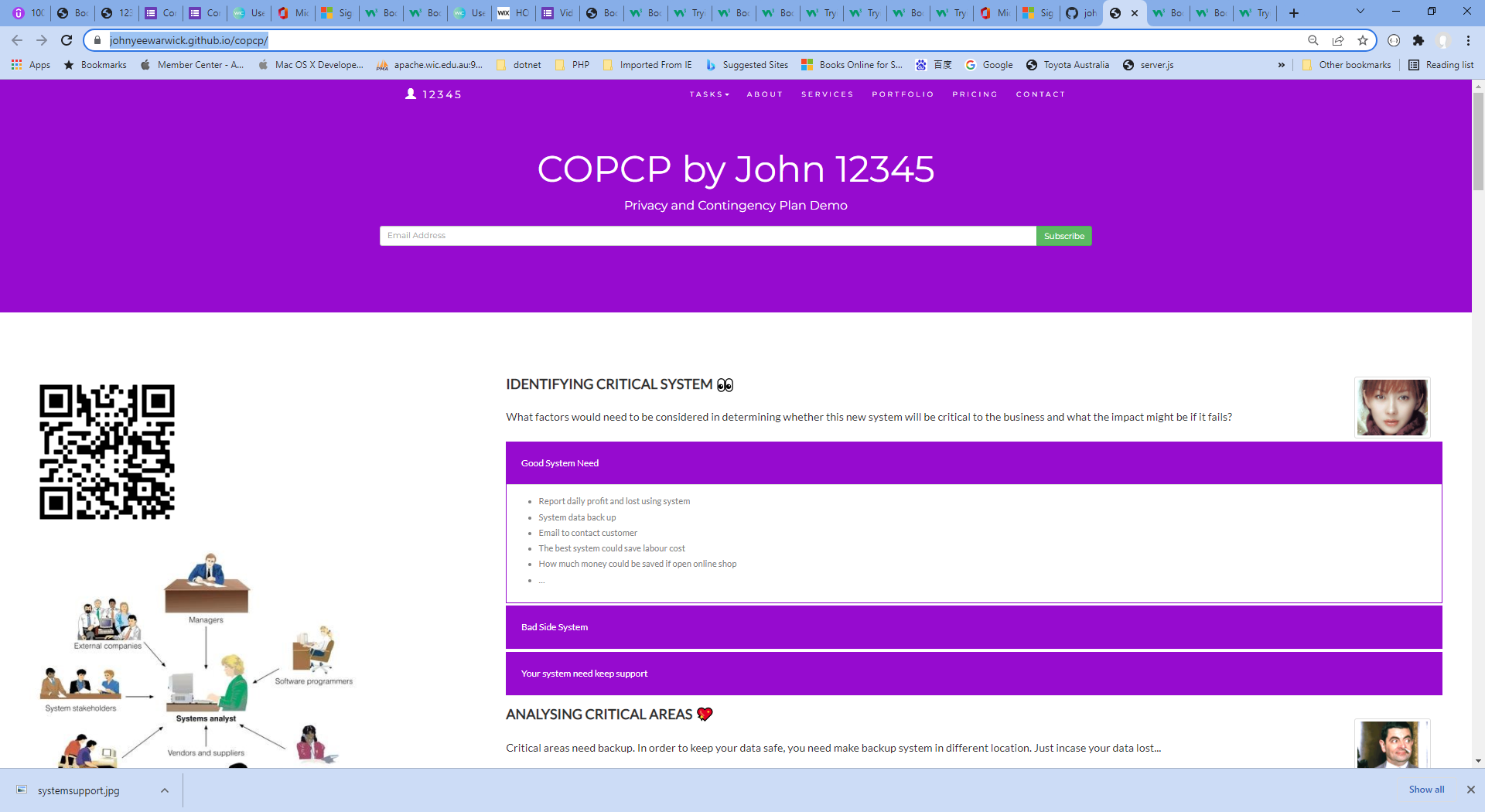
## Scenario 2: analysing critical areas

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 calls** |  |  |  |  |
| **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?**

* Important data is backup daily base
* At least need three different version stored different locations
* Fast and reliable hardware to support backup
* …

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

* Did not shut down or close link
* Data has been written during backing up
* Software did not do good validation when transaction occur
* …

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

You comment:

1.Issues to Consider for Backup and Restoration of Data:

When contemplating the backup and restoration of data, several critical considerations emerge. Firstly, it's imperative to ensure that important data is backed up daily, minimizing the risk of data loss in case of unexpected events. Additionally, maintaining multiple versions of backups stored in different physical or geographical locations enhances resilience against disasters or hardware failures. Investing in fast and reliable hardware infrastructure is essential to support efficient backup processes, ensuring timely and reliable data backups. Moreover, implementing encryption and robust security measures safeguards backed-up data from unauthorized access, adding an extra layer of protection. Regular testing of backups is also crucial to verify their accessibility and completeness, while a comprehensive disaster recovery plan outlines procedures for data restoration in emergencies. Lastly, staff training on backup procedures and consistent execution of backups further fortify data protection measures.

2.Problems with Backing Up Online Transactions:

The process of backing up online transactions can encounter various challenges that jeopardize data integrity and reliability. Incomplete backups are a common issue, often stemming from failure to properly shut down or close links during the backup process, resulting in data loss or corruption. Moreover, the dynamic nature of online transactions means that data may be written to the database while the backup is in progress, leading to inconsistencies between the backup and live data. Inadequate validation processes during transactions can exacerbate this issue, potentially backing up corrupted or incomplete data. Network interruptions pose another significant challenge, as they can disrupt the backup process, potentially leading to data loss. Ensuring proper transaction rollback mechanisms in the event of a failed backup is crucial to maintain data consistency and integrity. Moreover, scheduling backups during periods of low activity helps minimize the impact on online transactions, ensuring smooth and uninterrupted operations.

## 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 | X |  |
| **Impact on profitability** | X | X |  |
| **Impact on customer or supplier relations** | X | 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



#### Your comment:

…

#### Task 3:

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

???

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?

I think during

* Weekend or public holiday, max is 10 minutes
* Normal working days, max is 30 minutes
* At night or mid night or before 6 am, max is 60 minutes.
* In order to make your custom happy, you need minimize your server down times.
* …

You comment:

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

This e-commerce system is highly critical to Urban Wear due to its significant impact across various areas of the business. Firstly, any downtime could severely affect cash flow and profitability, which are vital for sustaining operations. Additionally, disruptions could damage customer and supplier relations, leading to potential loss of trust and business. Moreover, failing to meet legal requirements due to system downtime could result in regulatory penalties or legal issues. Furthermore, impacts on staff morale could lower productivity and hinder business performance. Considering Urban Wear's projection to conduct 50% of its business online within a year, any downtime risks losing customers to competitors, making the system's reliability paramount for long-term success.

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?

The maximum downtime figure of 30 minutes may vary depending on different factors such as trading hours and peak periods. During weekends, public holidays, or off-peak hours, such as late nights or early mornings, the tolerance for downtime might be lower, possibly around 10 minutes. However, during normal working days, the 30-minute threshold seems reasonable. To ensure customer satisfaction and minimize the risk of losing business, Urban Wear should aim to keep server downtime to a minimum across all times of operation.

## 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 | Ex\* |
| Hardware failures that stop the site operating.   * Hard disk broken * Power supply down * Cable is failed to link | in |
| Denial of service attacks to bring the service down.  ... | ex |
| Data destruction by any means such as a user deleting a file.  ... | in |
| Misuse of information by internal staff.  ... | in |
| Power problems so site is down.  ... | ex |
| Overloaded site so response is slow.  ... | ex |
| Customers falsifying information to avoid payment.  ... | ex |
| Incorrect information such as wrong prices so customers pay too little.  ... | in |
| Incorrect information such as wrong quantity in stock so customers have to wait for delivery.  ... | in |
| Major disaster so site is down.   * Earthquake, bushfire, terrorist * ... | Ex\* |
|  |  |

#### Task 4:

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

Example:

## Your comment:

1.Hackers attempting to get to the data stored on the site.

* Category: External
* Subcategories: Change data, Delete data, Add fake or wrong data
* Security Threat

2.Hardware failures that stop the site operating.

* Category: Internal
* Subcategories: Hard disk broken, Power supply down, Cable failure to link
* Security Threat

3.Denial of service attacks to bring the service down.

* Category: External
* Security Threat

4.Data destruction by any means such as a user deleting a file.

* Category: Internal
* Security Threat

5.Misuse of information by internal staff.

* Category: Internal
* Security Threat

6.Power problems so the site is down.

* Category: External
* Security Threat

7.Overloaded site so the response is slow.

* Category: External

8.Customers falsifying information to avoid payment.

* Category: External

9.Incorrect information such as wrong prices so customers pay too little.

* Category: Internal
* Security Threat

10.Incorrect information such as wrong quantity in stock so customers have to wait for delivery.

* Category: Internal
* Security Threat

11.Major disaster so the site is down.

* Category: External

12.Subcategories: Earthquake, bushfire, terrorist

* Security Threat

## 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 select
  + Students’ answers
  + Test results
  + …

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

* + Hack the question
  + Get answer key
  + System is going down
  + …

Your comment:

This system, the critical data and software areas include:

* Questions random selection: The system needs to efficiently manage a database of questions from various vendors and randomly select questions for each test to ensure fairness and integrity.
* Students' answers: It's crucial to accurately capture and store students' responses during the test to evaluate their performance and generate results.
* Test results: The system must securely store and manage test results, ensuring accuracy and confidentiality. This data is vital for issuing certificates and providing feedback to students.

As for potential threats to the system and testing facility:

* Hack the question: Malicious actors may attempt to breach the system's security to access and manipulate the database of test questions. This could lead to compromised test integrity and unfair advantages for certain individuals.
* Get answer key: Hackers might try to obtain the answer keys for tests, either by infiltrating the system or through other means. This could result in cheating and undermine the credibility of the testing process.
* System downtime: Any disruptions to the system's availability, whether due to hardware failures, cyber attacks, or other issues, could prevent students from taking tests as scheduled. This would not only impact revenue but also damage the organization's reputation and relationships with vendors and students.

## 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. | Implement Real-Time Fraud Detection | 5 | 5 |
| Student not turning up and exam lapses so $50 is lost. | Implement Payment Upon Confirmation | 2 | 3 |
| ISDN links broken delaying download of exams | Redundant ISDN Links | 4 | 4 |
| Hackers who may try to access test data or student data | Fire wall | 1 | 5 |
| Internal unauthorised access to test data or student data | Implement Strict Access Controls | 3 | 5 |
| Theft or misappropriation of test certificates | Implement Secure Certificate Handling | 3 | 3 |

Comment: …

* Disasters that stop the center operating: Implementing a backup system in a different location is essential (Business requirement: 4) to ensure continuity in case of disasters. While it's costly (Cost: 5), the investment is crucial for maintaining operations during emergencies.
* Hardware problems that stop system operating: Investing in best-quality hardware is essential (Business requirement: 5) to minimize the risk of hardware failures. While it's relatively costly (Cost: 4), the reliability and performance benefits justify the expense.
* Credit card fraud: Implementing real-time fraud detection systems is crucial (Business requirement: 5) to mitigate the risk of credit card fraud. While it may be costly (Cost: 5), the protection it provides to both the organization and its customers is invaluable.
* Student not turning up and exam lapses: Implementing a payment upon confirmation system can help reduce losses from missed exams, but it's not as crucial (Business requirement: 3). It's moderately costly (Cost: 2) but may not be essential compared to other measures.
* ISDN links broken delaying download of exams: Implementing redundant ISDN links is important (Business requirement: 4) to ensure uninterrupted access to exams. While it's somewhat costly (Cost: 4), the reliability it provides justifies the expense.
* Hackers: Implementing a strong firewall is crucial (Business requirement: 5) to protect against hackers. Despite being relatively low-cost (Cost: 1), its importance cannot be overstated for safeguarding test data and student information.
* Internal unauthorized access: Implementing strict access controls is crucial (Business requirement: 5) to prevent unauthorized access to sensitive data. While it incurs some cost (Cost: 3), it's essential for maintaining data security and integrity.
* Theft or misappropriation of test certificates: Implementing secure certificate handling procedures is important (Business requirement: 4) to prevent theft or misuse. It incurs some cost (Cost: 3) but helps maintain the credibility and integrity of the testing process.

## 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 costs only $12,000

…

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

Your comment: …

1.What RAID may give 4phones:

* Fault tolerance as regards disk drives: RAID provides redundancy by distributing data across multiple disks, ensuring that if one disk fails, data can still be accessed from other disks.
* Improved performance: RAID configurations such as RAID 0 or RAID 10 can enhance disk access speeds, leading to improved system performance.
* No downtime for single disk failure: With RAID, if a single disk fails, the system can continue operating seamlessly without any downtime, as data can be retrieved from the remaining disks.
* Hot swap to replace faulty disk: RAID systems often support hot swapping, allowing administrators to replace failed disks without shutting down the server, ensuring continuous operation.

2.Threats to be safeguarded against:

* Disk failure: RAID protects against disk failures by distributing data across multiple disks, minimizing the impact of individual disk failures.
* Multiple controllers guard against disk controller failure: Redundant RAID controllers ensure that if one controller fails, another can take over, preventing disruptions.
* Duplicate power supply guards against power supply failure: RAID systems often feature redundant power supplies, ensuring continuous operation even if one power supply fails.
* Quick connection to another unit if system unit goes down: RAID configurations can be quickly connected to another server unit in case of a system failure, minimizing downtime.

3.Cost benefit analysis:

* Orders placed on the web = $100,000 per day
* Assume 50% would go elsewhere if our system is down
* Loss = $50,000
* RAID costs only $12,000
* The potential loss due to system downtime far exceeds the cost of implementing RAID, making it a cost-effective solution to safeguard against revenue loss.

4.How RAID supports the business:

* 24X7 operation is a business strategy: RAID ensures continuous availability of the system, supporting the organization's strategy of operating round the clock.
* 99.9% uptime is an SLA requirement: RAID provides fault tolerance to meet stringent uptime requirements specified in service level agreements (SLAs), ensuring customer satisfaction and compliance with contractual obligations.

## 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.
7. ...

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.

#### Image result for computer virus warningTask 8:

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

**Computer virus protection procedures**

In order to safeguard against viruses, the following procedures must be adhered to by all staff:

Standard virus protection software must be installed on all PCs with updates organised automatically through the network.

Virus protection software must not be stopped or circumvented in any way

The virus software will be configured to run permanently so that files are always checked prior to opening.

Any software which recommends that the virus checker be disabled must not be installed without consulting the IT department. Users must never disable the virus checker without authority from IT.

Applications will be configured to warn of the use of macros, which could be viruses. Macros should only be enabled if the document source can be verified and trusted.

If any emails or email attachments are received from an unknown e-mail address or if any attachment has macros this should not be opened or macros enabled until the file has been checked by IT.

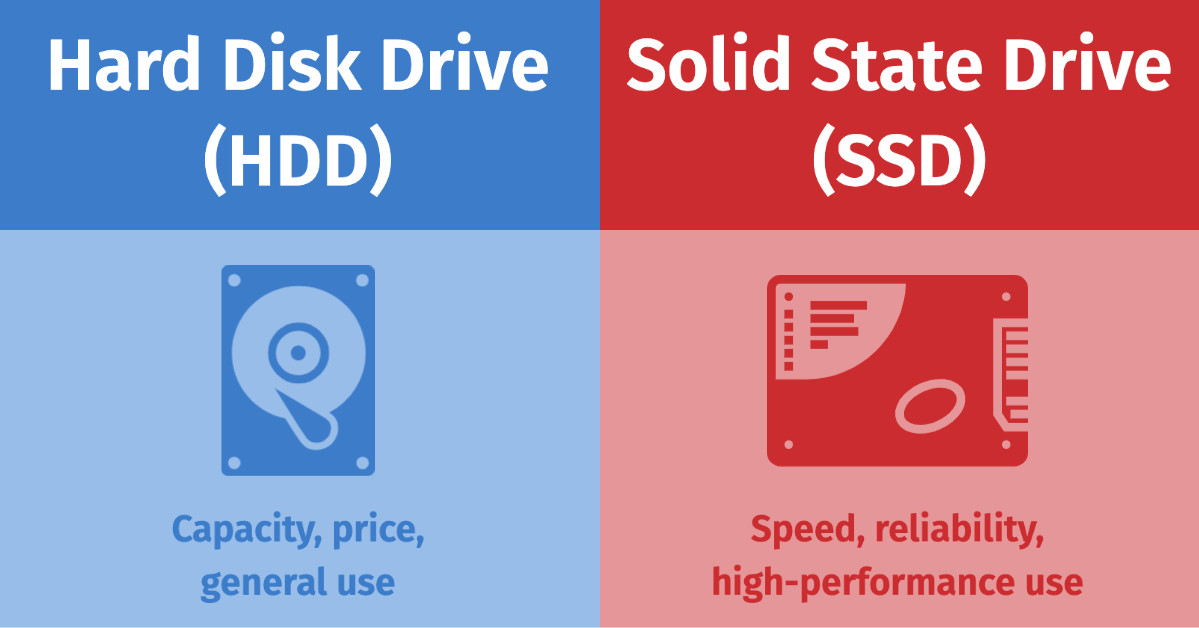
The IT department will obtain regular updates (daily) to virus files, which will be installed on the network in order to automatically update workstations.

All software, whether loaded from a CD-ROM or downloaded from the Intranet, must be scanned before opening.

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

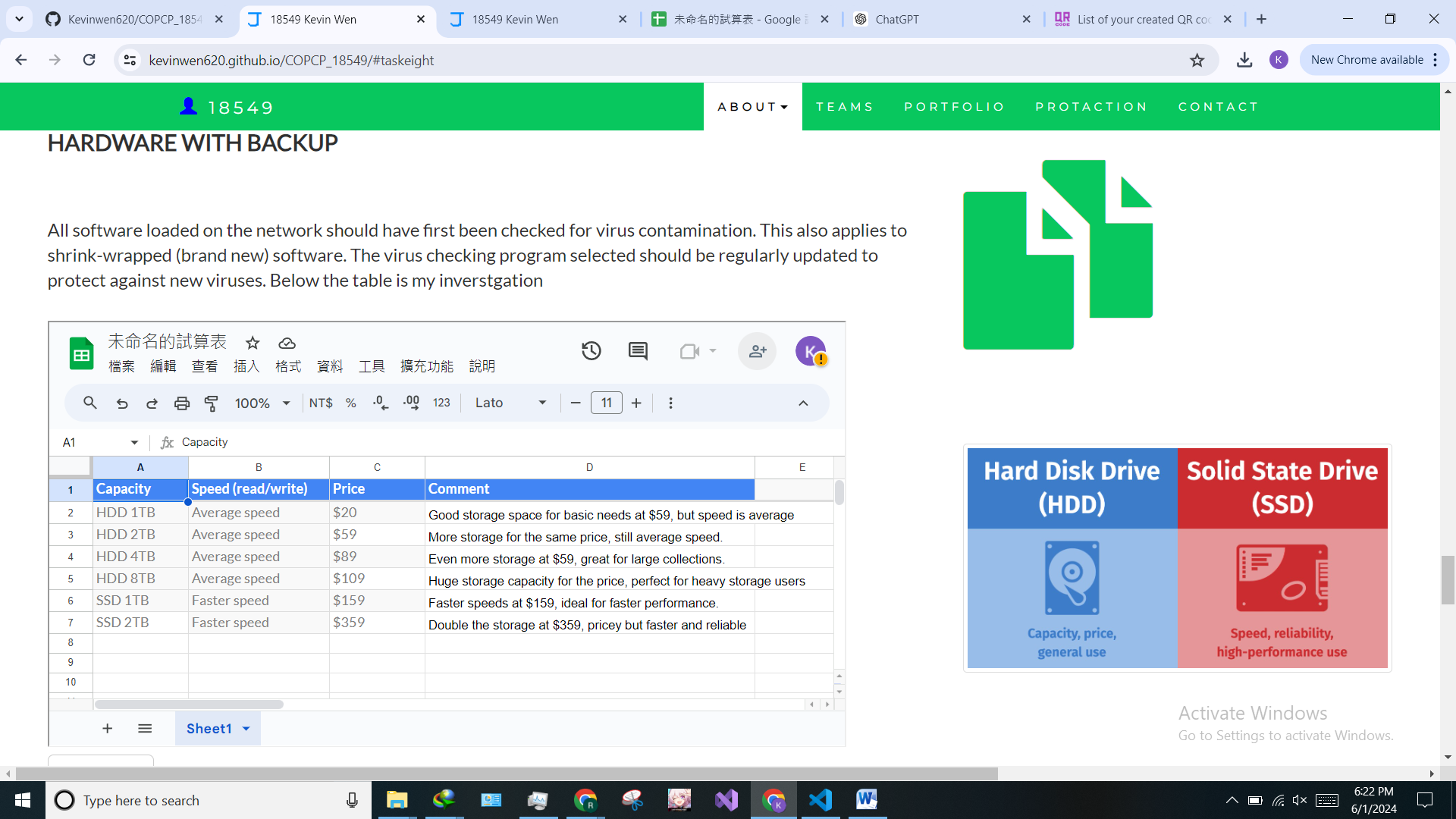
All computers will be regularly scanned for viruses on a daily basis as part of the start-up activity.

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

**Hardware recommendations**

The current tape unit is too slow and does not have the capacity to store a full back up on a single tape. Typical hardware specifications and costs are:

|  |  |  |
| --- | --- | --- |
| Capacity | Speed(read/write) | Price |
| 1TB | ... | $59 |
| 2TB | ... | $79 |
| 4TB | ... | ... |
| 8TB | ... | ... |
| SSD 1TB | Read speed 3,500 MBps max. Write speed 2,500 MBps max. | A$298 |
| SSD 2TB |  |  |



<https://kevinwen620.github.io/COPCP_18549/#taskeight>

<http://supercodepower.host20.uk/Copcpwebsite/>

## Index

C

configured 11

critical 3, 4, 5, 7, 10

D

duration 2

I

increased 11

N

New viruses 11

O

organisation 3, 4, 5, 6, 7, 10

P

privacy 2

R

recovery 11

S

software purchases 11

U

update workstations 11

V

virus 10, 11

virus protection 11