Wells International College

You ID  Your Name

Contribute to Organizational Privacy and Contingency Plans

|  |  |  |  |
| --- | --- | --- | --- |
| Name of Student | Jonathan Tanuwijaya | ID | 18399 |

# 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.

Please browser my web support site: <https://wellsjohn220.github.io/copcp>

## 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.

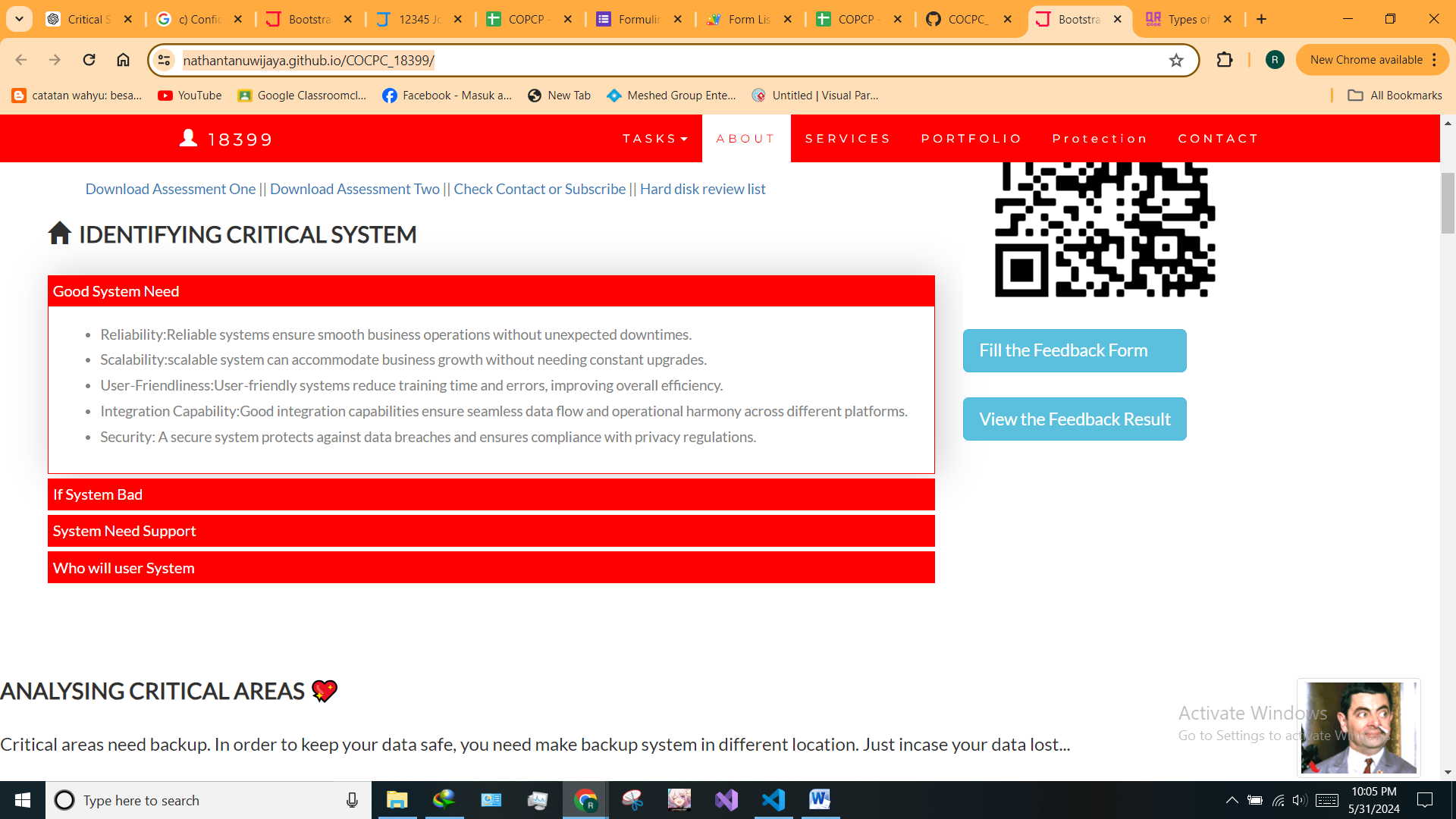
Good impact:

* 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://nathantanuwijaya.github.io/18399\_COPCP/

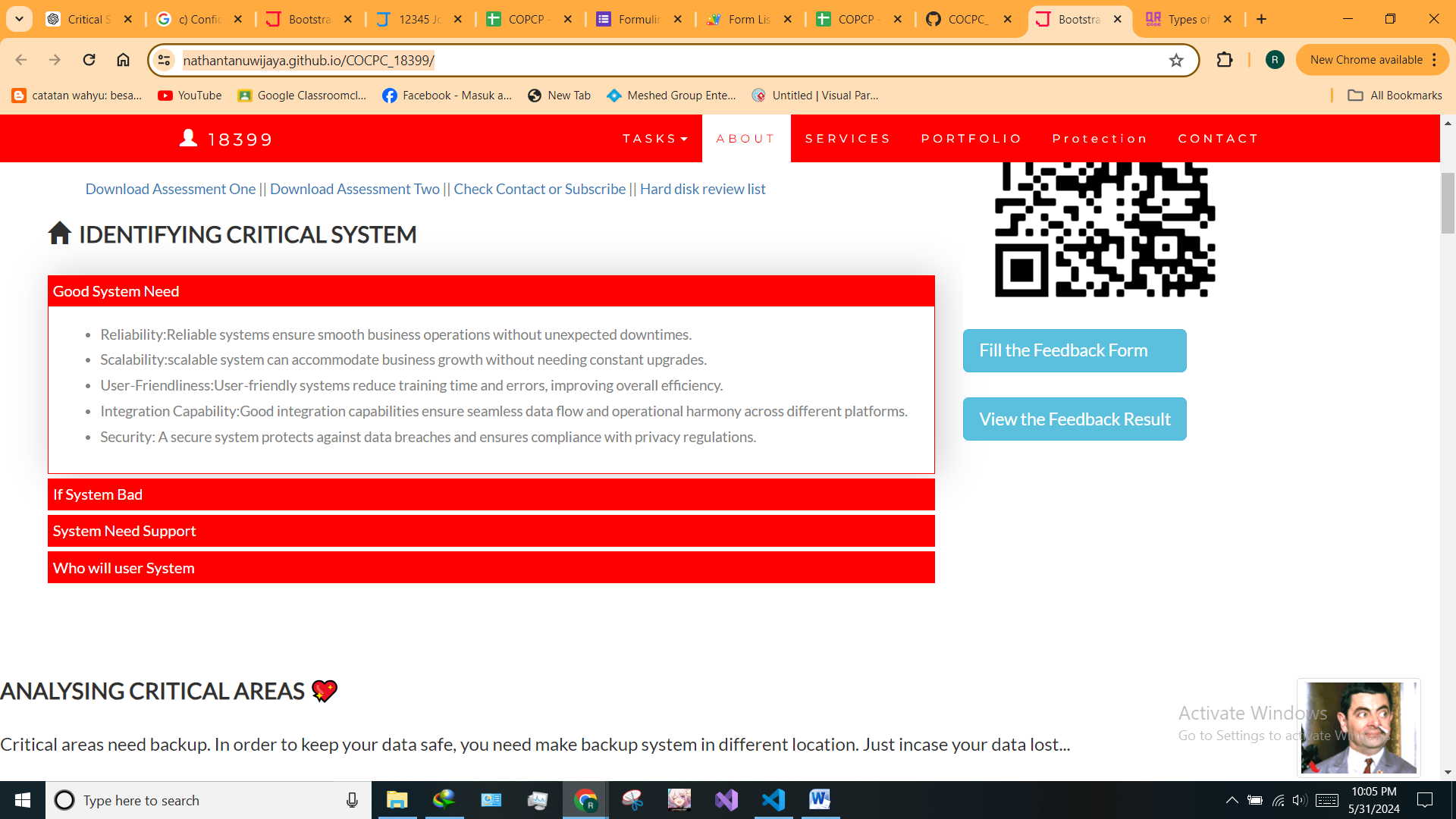


## Scenario 2: analysing critical areas

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?**

* 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
* …

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

-Daily Backups:

- Ensure important data is backed up every day.

- Multiple Versions in Different Locations:

- Store at least three versions of backups in different places.

- Fast and Reliable Hardware:

- Use hardware that supports quick and dependable backups.

- Regular Backup Testing:

- Regularly test backups to ensure they can be restored successfully.

2. Problems That Can Occur with Backing Up Online Transactions

- Active Transactions During Backup:

- Transactions might not be properly completed if backups are done while they are still active.

- Data Changes During Backup:

- Data written during the backup process can cause inconsistencies.

- Poor Transaction Validation:

- Inadequate validation can result in incomplete or incorrect transaction data being backed up.

- Network Interruptions:

- Network issues can cause incomplete backups of transaction data.

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

## 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.
* …

Answer:

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

The e-commerce system is very critical to Urban Wear because:

- Revenue: 50% of business is expected to be online within a year. Downtime means lost sales as customers can easily shop elsewhere.

- Customer Loyalty: Quick service is crucial. If the system is down, customers might not return.

- Operations: The system must be up and running most of the time; maximum allowable downtime is only 30 minutes.

- Peak Times: During Christmas, public holidays, and school holidays, any downtime would be even more damaging.

2. Does the 30-minute maximum downtime apply to a 24-hour trading period?

The 30-minute maximum downtime doesn't apply equally throughout the day. Here's a more detailed breakdown:

- Weekends or Public Holidays: Maximum downtime should be 10 minutes due to high customer activity.

- Normal Working Days: 30 minutes downtime is acceptable.

- Night or Early Morning (before 6 am): Maximum downtime can be up to 60 minutes since fewer customers are online.

To Minimize Downtime:

- Use backup systems to keep the site running.

- Schedule maintenance when fewer customers are online.

- Monitor the system to quickly fix problems.

- Have a plan ready for unexpected issues.

## 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 |
|  |  |

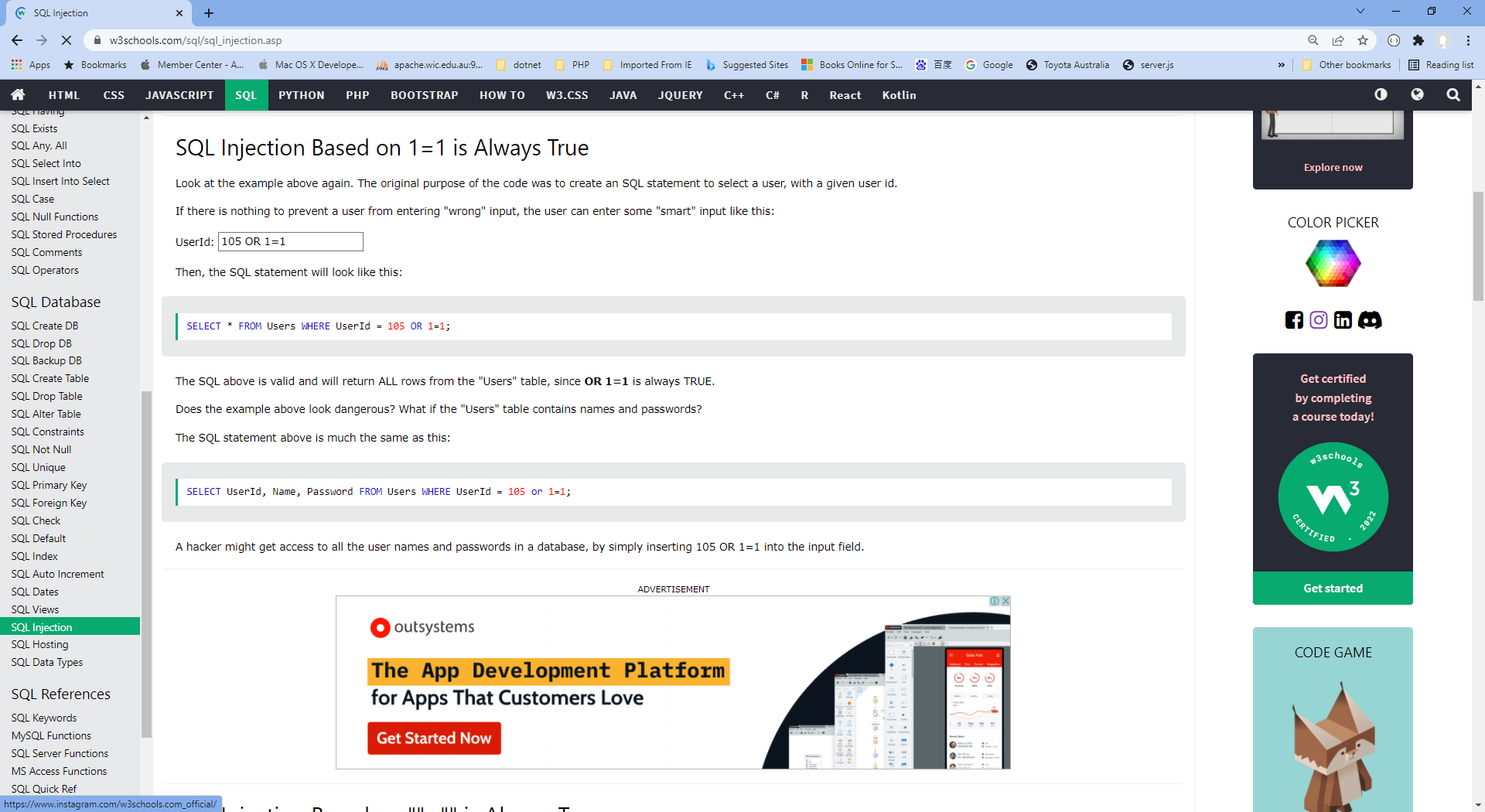
#### Task 4:

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

Example:

SQL injection:

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



If you do not know about this, please go to: <https://www.w3schools.com/sql/sql_injection.asp>

Answer:

Internal Threats:

* Hardware failures
* Data destruction by users
* Misuse of information by staff
* Incorrect pricing information
* Incorrect stock information

External Threats:

* Hackers accessing data
* Denial of service attacks
* Power problems
* Overloaded site
* Customers falsifying information
* Major disasters

Security Threats (Flagged with ):

* Hackers attempting to get to the data stored on the site:
  + Change data
  + Delete data
  + Add fake or wrong data
* Denial of service attacks to bring the service down
* Data destruction by any means such as a user deleting a file
* Misuse of information by internal staff
* Customers falsifying information to avoid payment

## 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
  + …

Answer:

Critical Data and Software Areas for CIT's Computerised Testing System

1. Questions Random Selection:

- System randomly selects different questions for each test.

2. Students’ Answers:

- Securely capturing and storing students' test responses.

3. Test Results:

- Accurately calculating and storing test scores.

4. Student Registration Information:

- Storing student log-ins, passwords, and payment details securely.

5. Test Downloads:

- Managing test downloads from vendors and their expiration.

6. Certificate Printing:

- Printing and managing certificates for passing students.

7. Data Transmission to Vendors:

- Sending student information and test results to vendors daily.

8. Payment Processing:

- Handling credit card and cash payments securely.

Potential Threats to the System and Testing Facility

1. Hacking the Questions:

- Unauthorized access to test questions.

2. Getting Answer Keys:

- Illegally obtaining answers to cheat on tests.

3. System Downtime:

- System outages disrupting test schedules.

4. Data Breaches:

- Unauthorized access to student information and test results.

5. Denial of Service Attacks (DoS):

- Overloading the system to make it unavailable.

6. Data Loss or Corruption:

- Loss or corruption of student data and test results.

7. Payment Fraud:

- Using stolen credit cards or fake payment info.

8. Test Expiration Issues:

- Failing to use downloaded tests before they expire.

9. Internal Misuse:

- Staff misusing their access to alter data or steal information.

10. Weak Security:

- Insufficient security measures making the system vulnerable.

11. Software Bugs:

- Errors affecting question randomization and result calculation.

12. Vendor Communication Failures

- Issues with downloading tests or sending results to vendors.

Recommendations to Mitigate Threats

- Encrypt Data: Secure data storage and transmission.

- Multi-Factor Authentication: Require multiple forms of verification for system access.

- Regular Updates: Keep software updated to fix vulnerabilities.

- Security Audits: Regularly check for security issues.

- Backup Plans: Have backups and disaster recovery plans.

- Continuous Monitoring: Watch system performance and security.

- Staff Training: Train staff on security protocols.

## 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 credit card verification system | 3 | 5 |
| Student not turning up and exam lapses so $50 is lost. | Pre-payment for exams | 2 | 3 |
| ISDN links broken delaying download of exams | Multiple redundant ISDN links | 4 | 4 |
| Hackers who may try to access test data or student data | Fire wall and Encryption | 2 | 5 |
| Internal unauthorised access to test data or student data | Role-based access control | 3 | 5 |
| Theft or misappropriation of test certificates | Secure storage and issuance logging | 3 | 4 |

## 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

Answer:

1. What RAID May Give 4phones

* Fault Tolerance for Disk Drives: RAID configurations provide redundancy by storing data across multiple disks. This ensures that if one disk fails, the data is still accessible from other disks in the array, minimizing data loss.
* Improved Performance: RAID can increase read and write speeds. This is particularly beneficial for an e-commerce platform where quick data retrieval and transaction processing are critical.
* No Downtime for Single Disk Failure: If a single disk fails, the RAID system will continue to operate without interruption. This is essential for maintaining continuous service availability.
* Hot Swap Capability: RAID systems often support hot swapping, allowing failed disks to be replaced without shutting down the server. This minimizes downtime and maintains business operations.

2. Threats to Be Safeguarded Against

* Disk Failure: RAID protects against the failure of individual disks, which are prone to wear and tear due to their electromechanical nature.
* Disk Controller Failure: Using multiple controllers in a RAID setup can guard against controller failures, ensuring data access even if one controller fails.
* Power Supply Failure: RAID systems can include duplicate power supplies, which protect against power supply failures by providing an alternative source of power.
* System Unit Failure: If the system unit fails, RAID can be quickly connected to another unit, ensuring that the data remains accessible and business operations can continue with minimal disruption.

3. Cost Benefit Analysis

* Orders Placed on the Web: The business generates $100,000 per day from online orders.
* Customer Loss if System Down: If the system is down, it is assumed that 50% of customers would go elsewhere, resulting in a potential loss of $50,000 per day.
* Cost of RAID: Implementing a RAID system costs $12,000.

Financial Justification: By preventing downtime and ensuring continuous operation, the RAID system can save up to $50,000 per day in potential lost revenue, making it a cost-effective solution at $12,000.

4. How RAID Supports the Business

* 24x7 Operation: The business strategy relies on 24x7 availability to meet customer demands at all times. RAID ensures that the system remains operational around the clock.
* 99.9% Uptime Requirement: The Service Level Agreement (SLA) requires 99.9% uptime, which equates to less than 9 hours of downtime per year. RAID provides the necessary fault tolerance to meet this stringent requirement.
* Fault Tolerance: RAID enhances the system’s resilience against hardware failures, ensuring that the e-commerce platform remains available and reliable, thus supporting the business's operational and financial goals.

## 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.

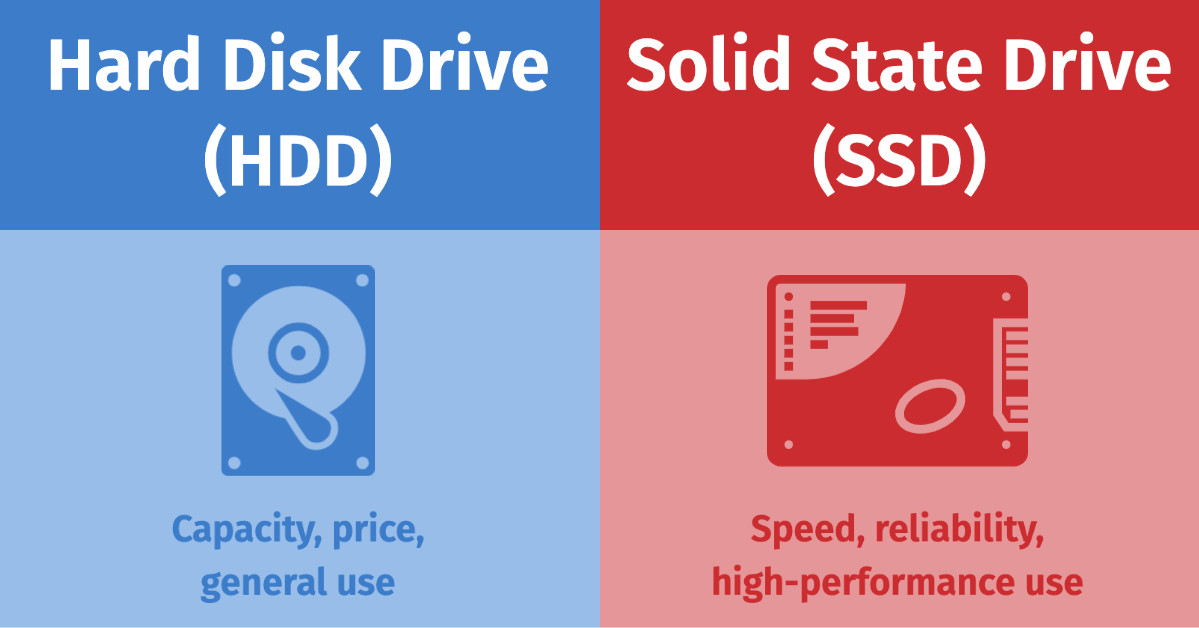
The IT department will obtain regular updates (daily) to virus files, which will be installed on the network in order to automatically update workstations.

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.

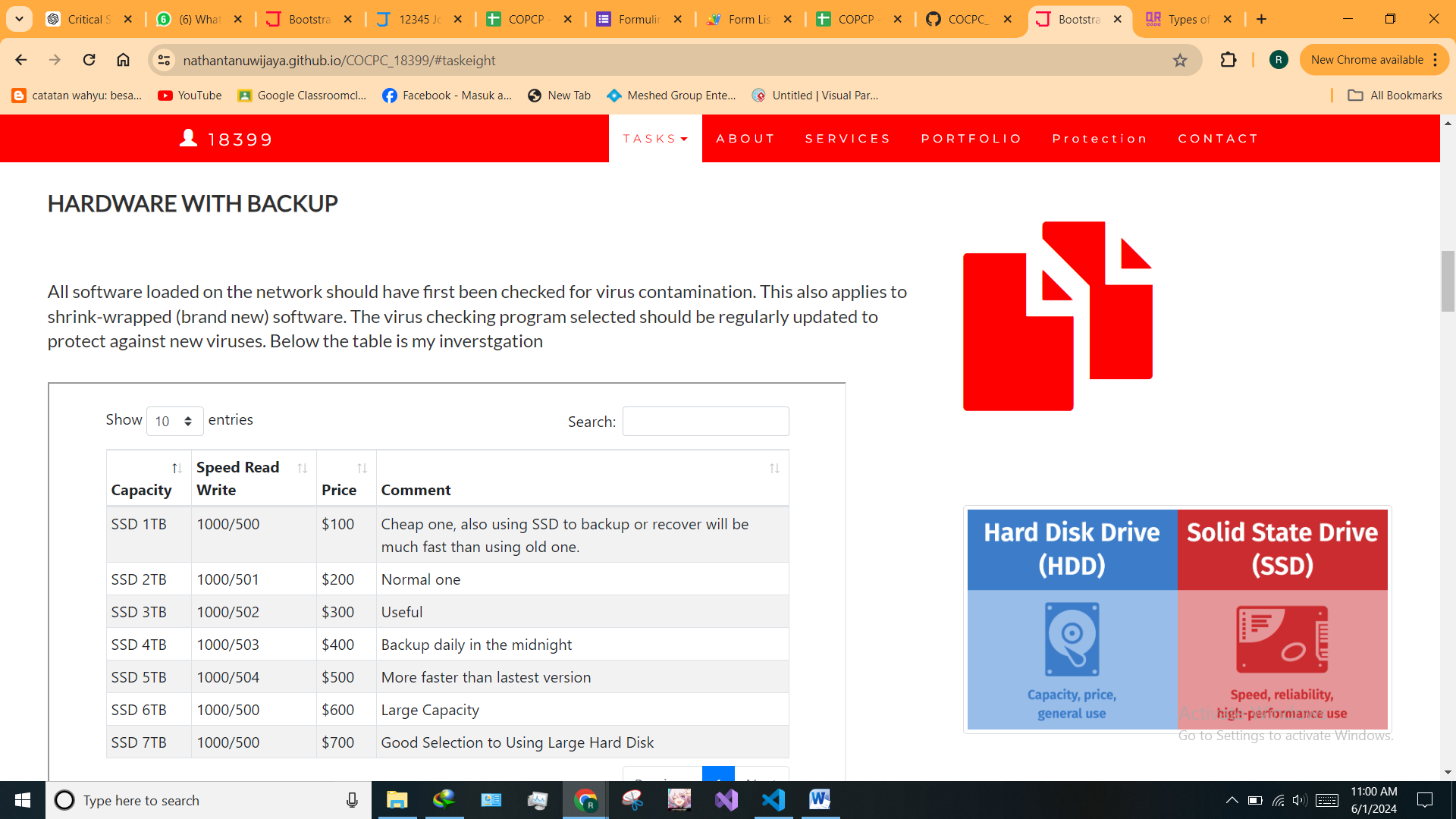
All computers will be regularly scanned for viruses on a daily basis as part of the start-up activity.

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 |  |  |
| Cloud Server | Internet upload and download speed | Monthly or Yearly Cost? … |

https://nathantanuwijaya.github.io/18399\_COPCP/ 

## 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