Wells International College

18156  Hoang Ngan Vu

Contribute to Organizational Privacy and Contingency Plans

|  |  |  |  |
| --- | --- | --- | --- |
| Name of Student | Hoang Ngan Vu | ID | 18156 |

# Assessment 1- Case Study

Contents

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

[Instructions 2](#_Toc65661061)

[Scenario 1: identifying critical systems 3](#_Toc65661062)

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

[Scenario 3: determining system criticality 6](#_Toc65661065)

[Scenario 4: identifying possible threats 9](#_Toc65661066)

[Scenario 5: identifying critical systems and threats 10](#_Toc65661067)

[Scenario 6: evaluating preventive and recovery options 14](#_Toc65661068)

[Scenario 7: presenting a strategic recommendation 15](#_Toc65661069)

[Scenario 8: reviewing procedures 18](#_Toc65661070)

[Index 24](#_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:

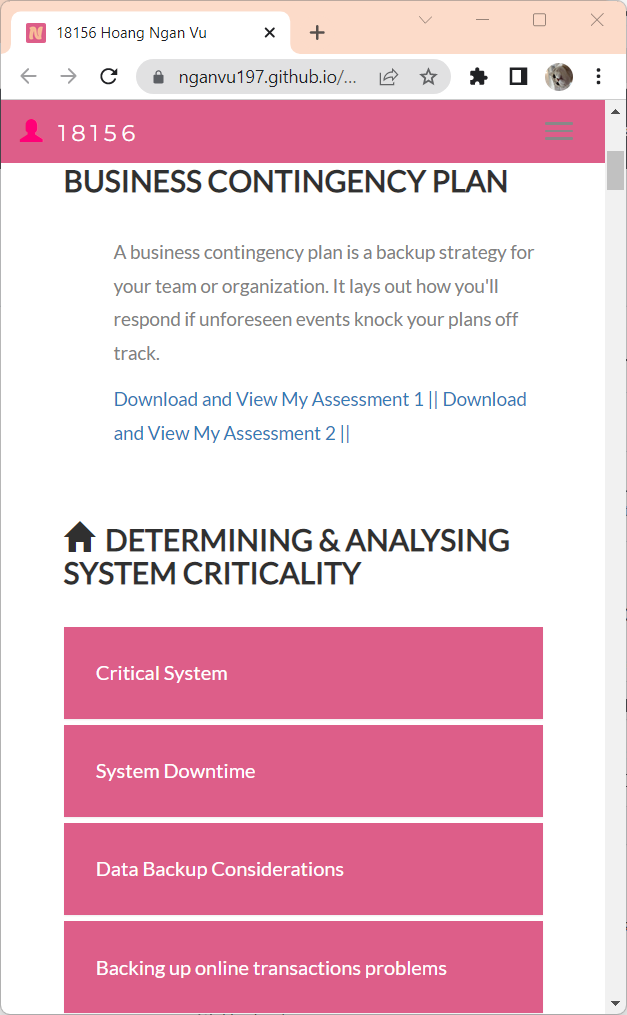
Trainer will set the duration of the assessment.

## 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://nganvu197.github.io/projectnganvu/>

#### Your comment:

**The questions Urban Wear needs to take into consideration are:**

1. Will the introduction of the new website raise a significant number of sales, customers’ interest in the brand or the overall profitability?
2. How much support should go into the system to ensure it runs smoothly? i.e., minimum down time, insignificant wait between loading times, security measures to prevent frauds or scams etc.
3. How would it affect current business structures? i.e., will the use of the website increase or decrease customer traffic in the physical store, should the store retaining or resigning customer-facing staff, will there be a need for additional employees handling shipping, warehousing or item returns etc.
4. Will the cost outweigh the benefits? i.e., the costs to rebuild the customer experience team , implement a well-run and safe system, cope with legal issues that comes with online retailing.

**Advantages:**

* Easy access to market - in many ways the access to market for entrepreneurs has never been easier.
* Reduced overheads - selling online can remove the need for expensive retail premises and customer-facing staff, allowing you to invest in better marketing and customer experience on your e-commerce site.
* Potential for rapid growth - selling on the internet means traditional constraints to retail growth.
* Widen your market / export - one major advantage over premises-based retailers is the ability expand your market beyond local customers very quickly.
* Customer intelligence - ability to use online marketing tools to target new customers and website analysis tools to gain insight into your customers' needs.

**Disadvantages:**

* Website costs - planning, designing, creating, hosting, securing and maintaining a professional e-commerce website isn't cheap, especially if you expect large and growing sales volumes.
* Infrastructure costs - even if you aren't paying the cost of customer-facing premises, you'll need to think about the costs of physical space for order fulfilment, warehousing goods, dealing with returns and staffing for these tasks.
* Security and fraud - the growth of online retail market has attracted the attention of sophisticated criminal elements.
* Legal issues - getting to grips with e-commerce and the law can be a challenge and you'll need to be aware of, and plan to cope with, the additional customer rights which are attached to online sales.
* Advertising costs - while online marketing can be a very efficient way of getting the right customers to your products, it demands a generous budget.
* Customer trust - it can be difficult to establish a trusted brand name, especially without a physical business with a track record and face-to-face interaction between customers and sales staff.

## 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 |

A screenshot of a computer screen

Description automatically generated with medium confidence

#### 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

#### Your comment:

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

* Cost: Like everything else, backups cost money. You may have to buy hardware and software, pay for a maintenance agreement, and train your staff.
* Backup location: Today, many default their backups to the cloud. However, you should still consider potentially keeping a copy of your data in another location as well. Cloud outages are rare but do happen.
* Backup method: You can choose from different kinds of backups. Each backup method requires a different amount of storage, impacting costs, and a different amount of time, impacting both the length of the backup procedure and the length of the recovery procedure.
* Backup (and recovery) flexibility: When creating backups, you generally want to backup everything, but that’s not true for recovery. Recovery needs to be able to scale from restoring a single file to restoring an entire server.
* Backup schedule: Your backups should be automated and run on a schedule, not rely on someone remembering to execute them manually. They should be scheduled to run frequently enough that you’ll capture data that changes often as well as data that changes rarely. They should be scheduled around production workflow needs.
* Scalable: You can expect your data to grow and your backup needs to grow along with it. Your backup process should be able to handle expected volumes of new data. You should have a process that ensures new servers, applications, and data stores are added to your backups.
* Backup security: Backups need to be accessible when needed, but they shouldn’t be accessible by just anyone. Making sure backups are safe from tampering is vital to protect your business.

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

* Corrupted backup: Backups can be corrupt for several reasons. Old media can get damaged or corrupted through poor handling or simply through age. Readable backups may not have application-consistent data, so even though you restore files, applications may not come up successfully.
* Inaccessible backup: If you have only one copy of your backup, and you can’t access it during a disaster, you can’t use it to restore your data.
* Backup job failed to start: Schedule backup jobs to run automatically, rather than relying on a staffer to manually kick off the job. Automation also eliminates the chance of making errors in parameter settings when starting the job manually.
* Backup job failed to complete: If the job runs into problems during its run, critical data isn’t protected.
* Incomplete backup: Be comprehensive rather than selective when deciding what to backup. When a new application or database is deployed, make adding it to the backup process part of your change management and deployment process.
* Slow backup: Backup jobs need to complete as part of your end of day process. Slow backup procedures can cause delays that impact the start of work the next day.

## 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



#### 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.
* …

#### Your comment:

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

Creating an eCommerce website is a critical step in assisting businesses in spreading their brands and increasing their ability to reach potential customers on the Internet, thereby increasing revenue and profit. The system is forecasted to increase profitability by 50% and if it does not run in an optimal state, it can create frustration among potential buyers, which can take a toll on brand trust. Buyers are also more likely to purchase from different competitors with similar product ranges as the market is polyamory.

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?**

Evidently, it’s ideal for the organisation to have zero downtimes, however, it is difficult to achieve. Hence, the acceptable downtime must be calculated.

A simple example illustrates this. We estimate tolerance to loss of a customer-facing service at 48 hours. This deadline is accepted by the business and everyone plans for it. After investing in a warm standby, the service is test-restored successfully in 36 hours and everyone is happy. Six months later we realise we overlooked a client contract that demands a tested 12-hour continuity response. We are now faced with either re-visiting our plans and spending considerably more or accepting the contractual risk. Getting it right is important.

You have to take into account the current exposure (the issue which causes downtimes in the first place, i.e., security risks, scheduled maintenance etc.) as well as available budget to determine how long can the downtime last.

## 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 | E\* |
| Hardware failures that stop the site operating.   * Hard disk broken * Power supply down * Cable is failed to link | I |
| Denial of service attacks to bring the service down.   * Flood the website with traffic * Send in information that triggers a crash | E |
| Data destruction by any means such as a user deleting a file.   * Overwriting * Degaussing * Physical destruction | I |
| Misuse of information by internal staff.   * Frauds * Identity theft | I |
| Power problems so site is down. | E |
| Overloaded site so response is slow. | E |
| Customers falsifying information to avoid payment.   * Phishing * Pagejacking * Advanced fee and wired transfer scams | E |
| Incorrect information such as wrong prices so customers pay too little. | I |
| Incorrect information such as wrong quantity in stock so customers have to wait for delivery. | I |
| Major disaster so site is down.   * Earthquake, bushfire, terrorist | E\* |

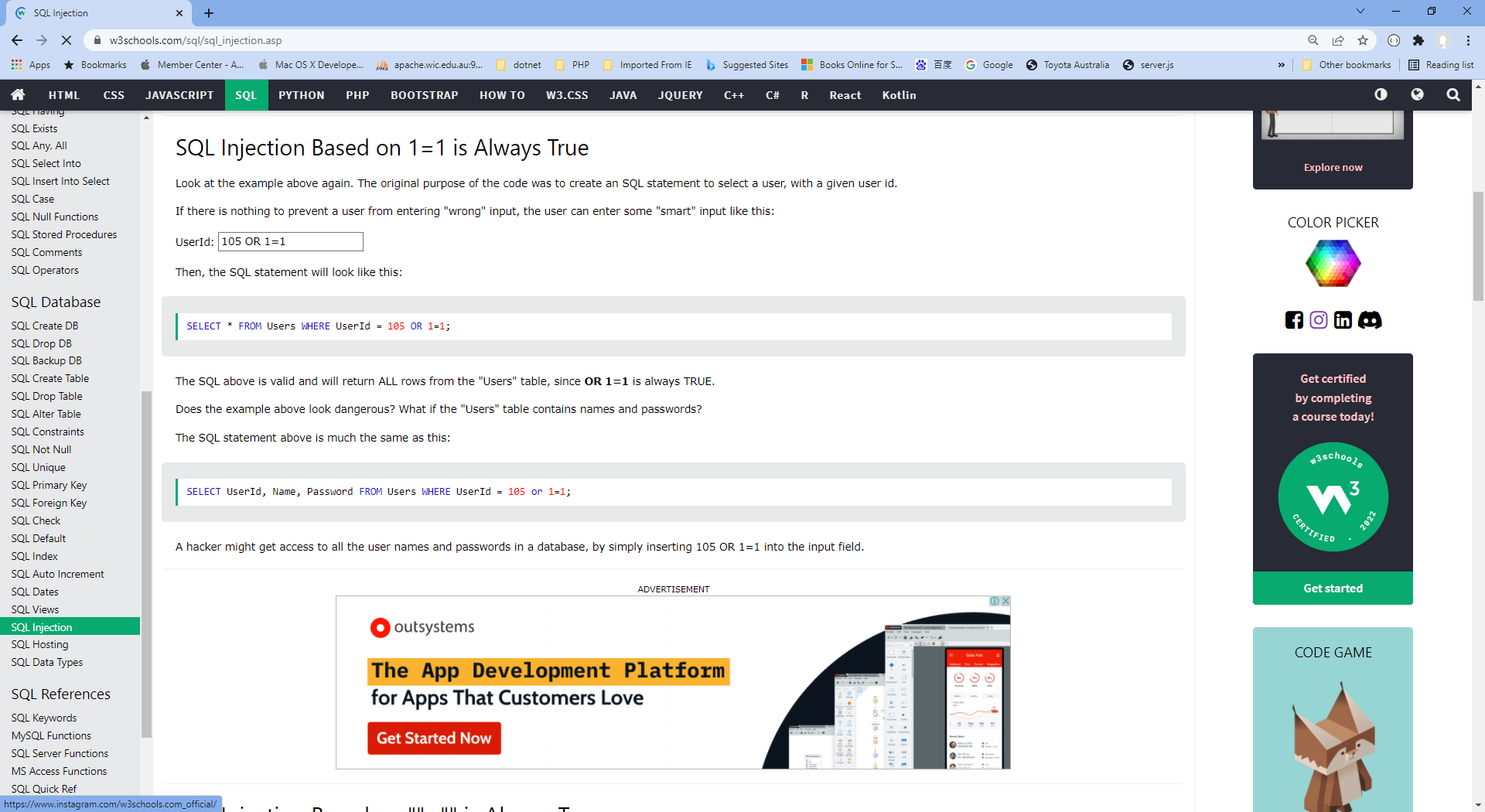
#### Task 4:

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>



#### Your comment:

The internal and external threats are categorised as shown in the table above.

If you are not aware of SQL Injections, please go to: <https://www.w3schools.com/sql/sql_injection.asp>

## 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:

1. **What are the critical data and software areas for this system?**

* Role-Based Access: The software offers role-based access to teachers, students, and admin.
* Mobile/Laptop Usage: The system can be accessed through a mobile phone or laptop.
* Assessment Accuracy: The software ensures high accuracy of student assessment and feedback.
* Anti-Cheating Methods: The system offers proctoring solutions to avoid cheating during exam.
* AI-Based Analysis: The software offers AI-Based report analysis for a better understanding of data.
* Report Generation: The software ensures easy report generation in required formats.

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

* Required Resources: Several resources are required for Computer-Based Testing administration.
* Item Bank Creation and Exposure Control: One of the main issues related to CBT is the creation and administration of item banks. CBT normally requires a huge number of item banks because of its frequent scheduling. Creation of item banks by subject-matter experts (SMEs) and their related security is one of the most important issues. Several algorithms have been proposed in order to control item exposure rates.
* Identification and Authentication of Examinee: Test security is one of the most important aspects of any exam, whether it is administered as paper-and-pencil based or CBT. The primary element of security in CBT is the procedure used to identify and authenticate the examinee. Different people use different ways to identify the examinee – username and password, biometric recognition etc.
* Invigilator/Proctor Authentication: Besides the examinee authentication, invigilator or proctor authentication is also an important aspect in online or computer-based tests, because the proctor has access to many aspects of the exam, including the examinee registration data, test data, or examinee test.
* Cheating during Exam: Another important security issue in the computer-based testing is cheating during the ongoing exam. The examinee can cheat either by communicating with their other colleagues or by browsing over the internet. Different people have used different techniques for the same problem – webcams to monitor the examinees, or arrange the test in a web lock environment, where the test is displayed in a full screen option and the browser and other applications are locked during the exam.

## 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 | Back up data (other locations, cloud) | 5 | 2 |
| Hardware problems that stop system operating | Regular hardware maintenance | 4 | 4 |
| Credit card fraud. With the short time frame the student could be tested before any credit card discrepancy was identified. | Identity authentication | 4 | 5 |
| Student not turning up and exam lapses so $50 is lost. | Pre-charge fee | 1 | 3 |
| ISDN links broken delaying download of exams | Different URLs, servers | 3 | 5 |
| Hackers who may try to access test data or student data | Firewall  Security solutions | 1  5 | 5 |
| Internal unauthorised access to test data or student data | Authentication  User based access | 3 | 5 |
| Theft or misappropriation of test certificates | Firewall  Security solutions | 1  5 | 5 |
| Identification and Authentication of Examinee | Username & password  Biometric recognition | 1  4 | 5 |
| Invigilator/Proctor Authentication | Data access restrictions | 3 | 5 |
| Cheating during Exam | Monitoring webcam  Web lock environment | 4  5 | 5 |

#### Your comment:

Please see above table for the evaluation.

## 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:**

* Improved cost-effectiveness because lower-priced disks are used in large numbers.
* Using multiple hard drives enables RAID to improve the performance of a single hard drive.
* Increased computer speed and reliability after a crash, depending on the configuration.

1. **Threats to be safeguarded against:**

* When a drive fails, the probability that another drive in the array will also soon fail rises, which would likely result in data loss.
* RAID arrays, and the data in them, are vulnerable until a failed drive is replaced and the new disk is populated with data.
* Because drives have much greater capacity now than when RAID was first implemented, it takes a lot longer to rebuild failed drives.
* If a disk failure occurs, there is a chance the remaining disks may contain bad sectors or unreadable data, which may make it impossible to fully rebuild the array.

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

* The cost of RAID is $12,000, performance of disk access can gain by 10%.
* Assume 50% would go elsewhere if the system is down.
* Orders placed on the website worth $100,000 per day > $100,000 loss if the business loses server disks for a day.
* 4 hours to restore from backups, back-up tapes are 12 hours old.

1. **How RAID supports the business:**

* Allow input/output (I/O) operations to overlap in a balanced way, improving performance.
* Store data redundantly which increases fault tolerance.
* Requires operation continuation, minimum downtimes on a daily basis.

## 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.

#### Task 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.

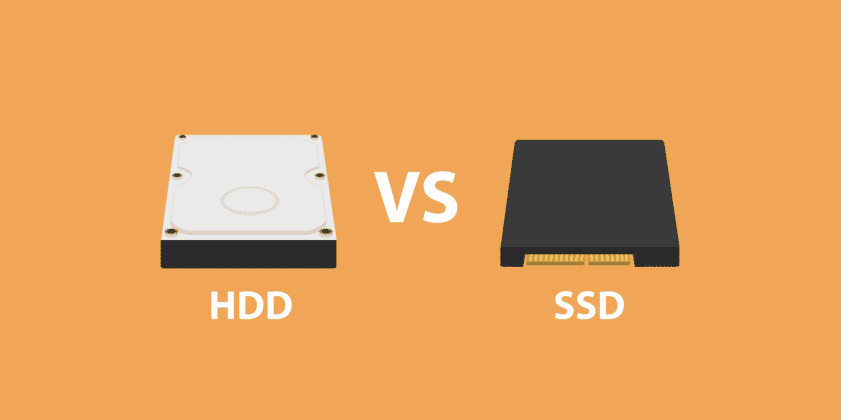
If any emails or email attachments are received from an unknown e-mail address or if any attachment has macros this should not be opened or macros enabled until the file has been checked by IT.

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 – Sandisk SSD Plus | Seq Read: 535 MB/s  Seq Write: 450 MB/s | US$43.99 |
| 2TB – Inland Performance SSD | Seq Read: 5000 MB/s  Seq Write: 4300 MB/s | US$129.99 |
| 4TB – Seagate FireCuda | Seq Read: 7300 MB/s  Seq Write: 6900 MB/s | US$451.49 |
| 8TB – Samsung 870 QVO SATA III SSD | Seq Read: 560 MB/s  Seq Write: 530 MB/s | US$427.79 |

<https://nganvu197.github.io/projectnganvu/#taskeight>

A screenshot of a computer

Description automatically generated

#### Your comment:

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

* Install (and turn on) antivirus software: Antivirus software - which is often included for free within popular operating systems - should be used on all computers and laptops. For your office equipment, you can pretty much click 'enable', and you're instantly safer. Smartphones and tablets might require a different approach.
* Prevent staff from downloading dodgy apps: You should only download apps for mobile phones and tablets from manufacturer-approved stores (like Google Play or Apple App Store). These apps are checked to provide a certain level of protection from malware that might cause harm. You should prevent staff from downloading third party apps from unknown vendors/sources, as these will not have been checked.

Staff accounts should only have enough access required to perform their role, with extra permissions (i.e. for administrators) only given to those who need it. When administrative accounts are created, they should only be used for that specific task, with standard user accounts used for general work.

* Keep all your IT equipment up to date (patching): For all your IT equipment (so tablets, smartphones, laptops and PCs), make sure that the software and firmware is always kept up to date with the latest versions from software developers, hardware suppliers and vendors. Applying these updates (a process known as patching) is one of the most important things you can do to improve security - the IT version of eating your fruit and veg. Operating systems, programmes, phones and apps should all be set to 'automatically update' wherever this is an option.

At some point, these updates will no longer be available (as the product reaches the end of its supported life), at which point you should consider replacing it with a modern alternative.

* Control how USB drives (and memory cards) can be used: We all know how tempting it is to use USB drives or memory cards to transfer files between organisations and people. However, it only takes a single cavalier user to inadvertently plug in an infected stick (such as a USB drive containing malware) to devastate the whole organisation.

When drives and cards are openly shared, it becomes hard to track what they contain, where they've been, and who has used them. You can reduce the likelihood of infection by:

* blocking access to physical ports for most users
* using antivirus tools
* only allowing approved drives and cards to be used within your organisation - and nowhere else.

Make these directives part of your company policy to prevent your organisation being exposed to unnecessary risks. You can also ask staff to transfer files using alternative means (such as by email or cloud storage), rather than via USB.

* Switch on your firewall: Firewalls create a 'buffer zone' between your own network and external networks (such as the Internet). Most popular operating systems now include a firewall, so it may simply be a case of switching this on.

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

A complete backup process should include the following steps:

* Create a backup of your current databases and any customizations or files specific to your organisations needs, such as import templates, custom reports, spreadsheets, etc.
* Store multiple copies of all backup files on external media, such as a tape drive or CD/DVD.
* Regularly test your backup:
* Make a backup of your database.
* Restore from a backup copy. Note: If you're testing a backup for the first time, we recommend restoring the backup in a test environment first (e.g. on a standalone workstation or isolated server). This way, if the backup is bad, restoring to it won't not affect your live database.
* Verify users can log into the database and that the correct data is present.
* Restore the original data.

Recommendations to protect your data files:

* Use only the supported backup procedures for your databases.
* Backup your databases prior to running any software update.
* Schedule the database backup to create a compressed file in a separate directory from the main database files, which can then be automated to copy to a removable media. Many backup systems can be automated to process backups overnight.
* Purchase and use an archival backup solution, e.g., a tape drive. Blackbaud is not a vendor of backup software or hardware and cannot determine which backup system is right for your organization. Consult with reputable dealers and qualified information systems professionals to implement a reliable backup system.
* Create three sets of daily backups, three sets of weekly backups, and three sets of monthly backups. All media types can fail. Multiple backup copies increase your odds of recovering data if another copy fails.
* Store one backup set in a safe, off-site location, preferably in a fireproof safe. If you evacuate, bring your backup with you.
* Periodically test the backup files to ensure your backup system is operating properly and that you are familiar with the database restore procedure.
* Never overwrite the most recent backup copy on a tape, disk, or CD/DVD.
* Never process an import, purge, global change without having a current backup.
* Create a backup schedule and keep it at the computer where the backups are performed.
* Use a separate backup schedule for each software program.
* Clearly label your backups with the date and type of data they contain.

Hardware recommendations:

|  |  |  |
| --- | --- | --- |
| Capacity | Speed(read/write) | Price |
| 1TB – Sandisk SSD Plus | Seq Read: 535 MB/s  Seq Write: 450 MB/s | US$43.99 |
| 2TB – Inland Performance SSD | Seq Read: 5000 MB/s  Seq Write: 4300 MB/s | US$129.99 |
| 4TB – Seagate FireCuda | Seq Read: 7300 MB/s  Seq Write: 6900 MB/s | US$451.49 |
| 8TB – Samsung 870 QVO SATA III SSD | Seq Read: 560 MB/s  Seq Write: 530 MB/s | US$427.79 |

Below are my website contents:

<https://nganvu197.github.io/projectnganvu/#myPage>

A screen shot of a diagram

Description automatically generated with low confidenceA screenshot of a computer

Description automatically generated with low confidence

## 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