

CONTRIBUTE TO ORGANIZATIONAL PRIVACY AND CONTINGENCY PLANS

Wells International College

Name of Student	Princes Ericka Blauaro	ID	18635
-----------------	------------------------	----	-------

Assessment 1– Case Study

Contents

Assessment 1- Case Study	2
Instructions	2
Scenario 1: identifying critical systems	3
Scenario 2: analysing critical areas	4
Scenario 3: determining system criticality	5
Scenario 4: identifying possible threats	7
Scenario 5: identifying critical systems and threats	8
Scenario 6: evaluating preventive and recovery options	10
Scenario 7: presenting a strategic recommendation	11
Scenario 8: reviewing procedures	13
Index	15

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.

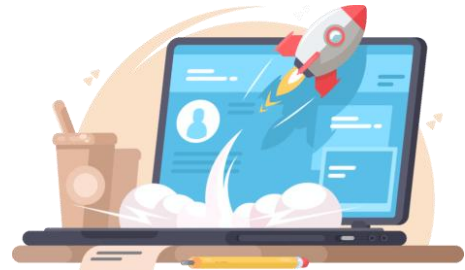
You need Internet access to analyse and complete some of the tasks.

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:

Comment: all bad side must be prevented...

<https://wellsjohn220.github.io/copcp>

or (old):

<https://johnyeewarwick.github.io/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.

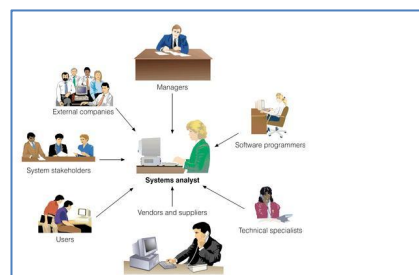


Table 1: critical areas

	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 calls				
Developed at the workstation such as report writing	0			
Other—specify	0	50%	50%	0

Task 2:

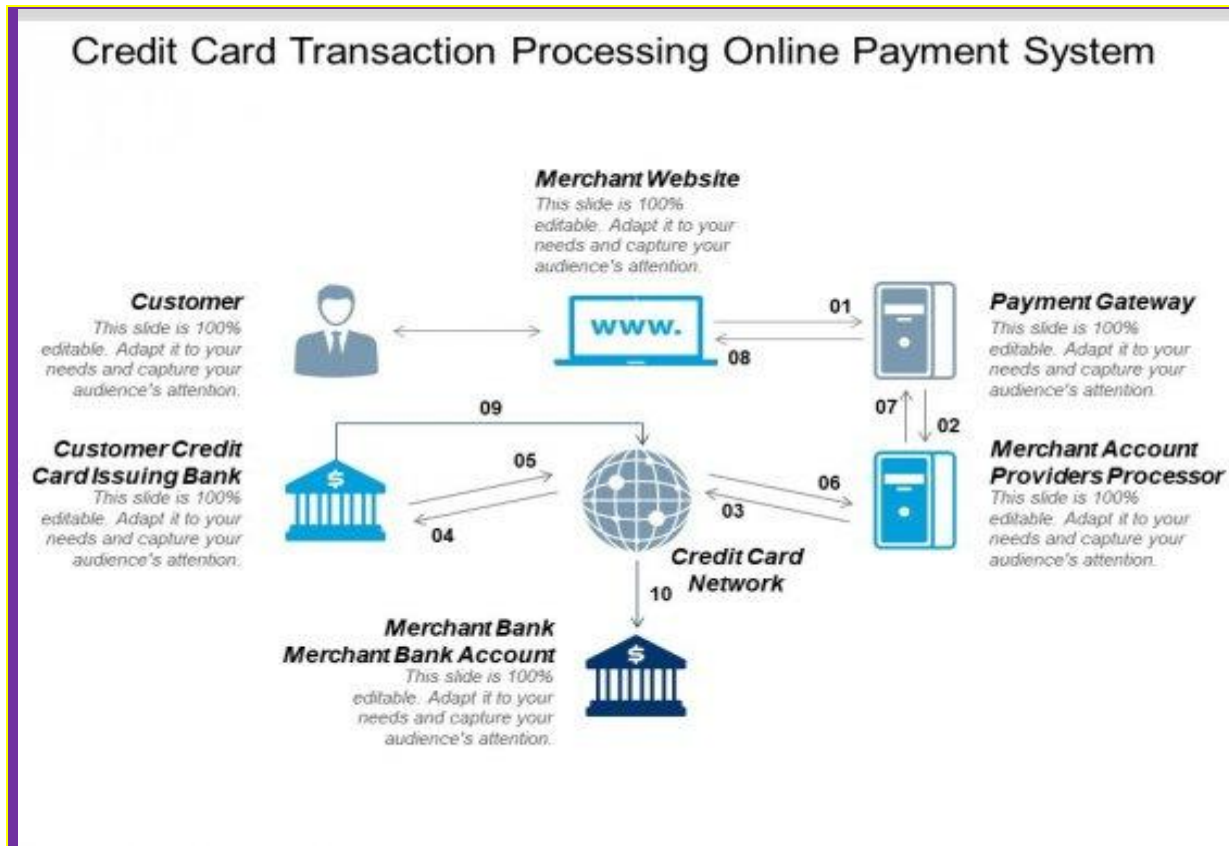
1. What issues need to be considered for backup and restoration of data?

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

2. 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
- ...





You comment: The purpose of a backup is to make a copy of your data that you can recover from if your primary data is lost. Primary data failures may come from hardware or software issues, data corruption, or a human error like a malicious attack (virus or malware), data deletion accident, or other human-caused event.

Scenario 3: determining system criticality

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

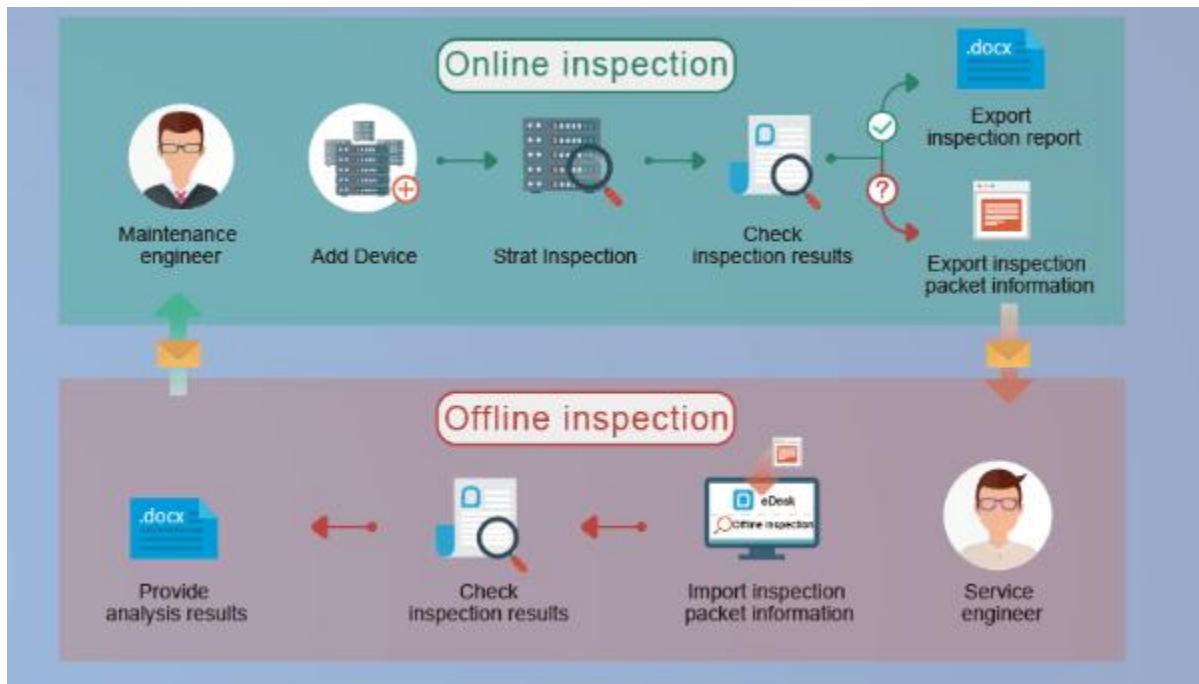
Table: Analysing critical areas: impact of system down for less than 1 hour.

	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: reducing the possibility of human error and enabling businesses to bring everything under one roof

...

Task 3:

1. How critical is this system to the organisation? Why?
 - online banking systems, traffic control systems and communication systems are mission-critical computing systems that result in business loss if they fail.
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?

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.

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. <ul style="list-style-type: none"> Change data Delete data Add fake or wrong data 	Ex*
Hardware failures that stop the site operating. <ul style="list-style-type: none"> Hard disk broken Power supply down Cable is failed to link 	in
Denial of service attacks to bring the service down. <ul style="list-style-type: none"> Flooding Services Crashing Services 	ex*
Data destruction by any means such as a user deleting a file. <ul style="list-style-type: none"> Overwriting Deguuasing Physical Destruction 	in*
Misuse of information by internal staff. <ul style="list-style-type: none"> misuse of email manipulation of a computerised accounting system insertion of malicious code 	in
Power problems so site is down. <ul style="list-style-type: none"> Server Overload Malicious Cyber attack 	ex*
Overloaded site so response is slow. <ul style="list-style-type: none"> there is a communication problem between the target server and the client 	ex
Customers falsifying information to avoid payment. <ul style="list-style-type: none"> Farud Scammers 	ex*
Incorrect information such as wrong prices so customers pay too little. <ul style="list-style-type: none"> when an advertised price is different from the actual price the seller intends to charge you for the product. 	in
Incorrect information such as wrong quantity in stock so customers have to wait for delivery. <ul style="list-style-type: none"> avoid false information. 	in
Major disaster so site is down. <ul style="list-style-type: none"> Earthquake bushfire terrorist 	Ex*

Task 4:

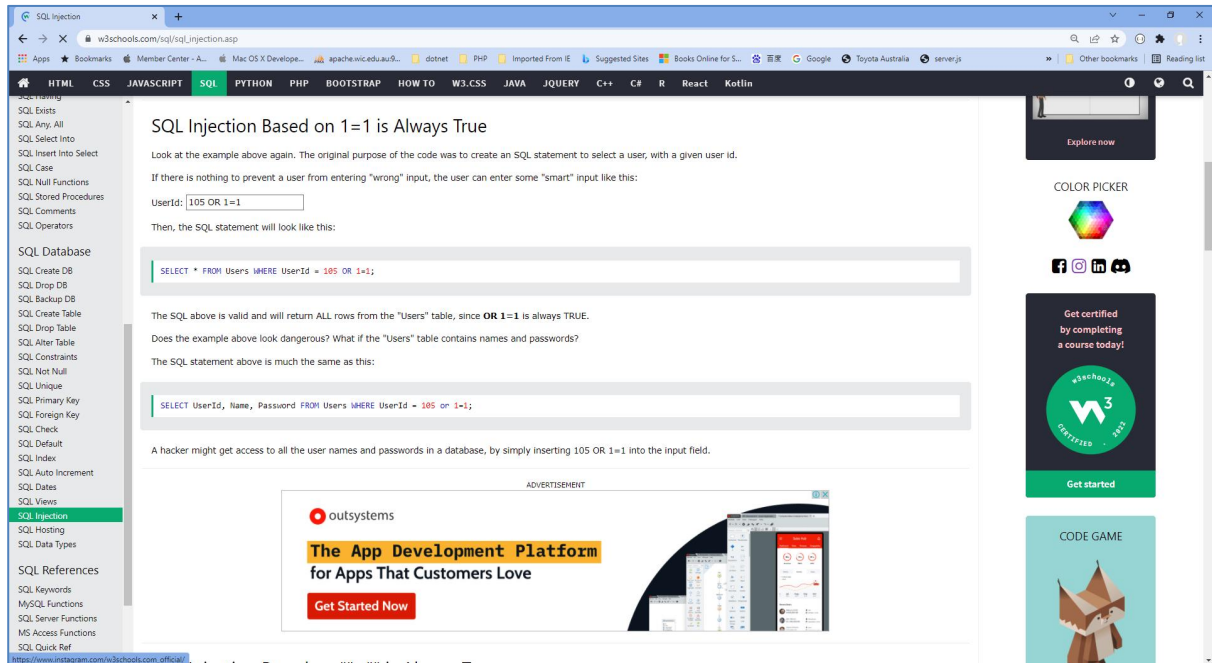
Identify whether they are internal or external and flag with an * any threats that are also security threats.

Example:

Contribute to organizational privacy and contingency plans - Assessment Task 1 **LAST UPDATED:** December 2015, Version No. 3.0

SQL injection:

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



Your comment:SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed.

...

If you do not know about this, 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.

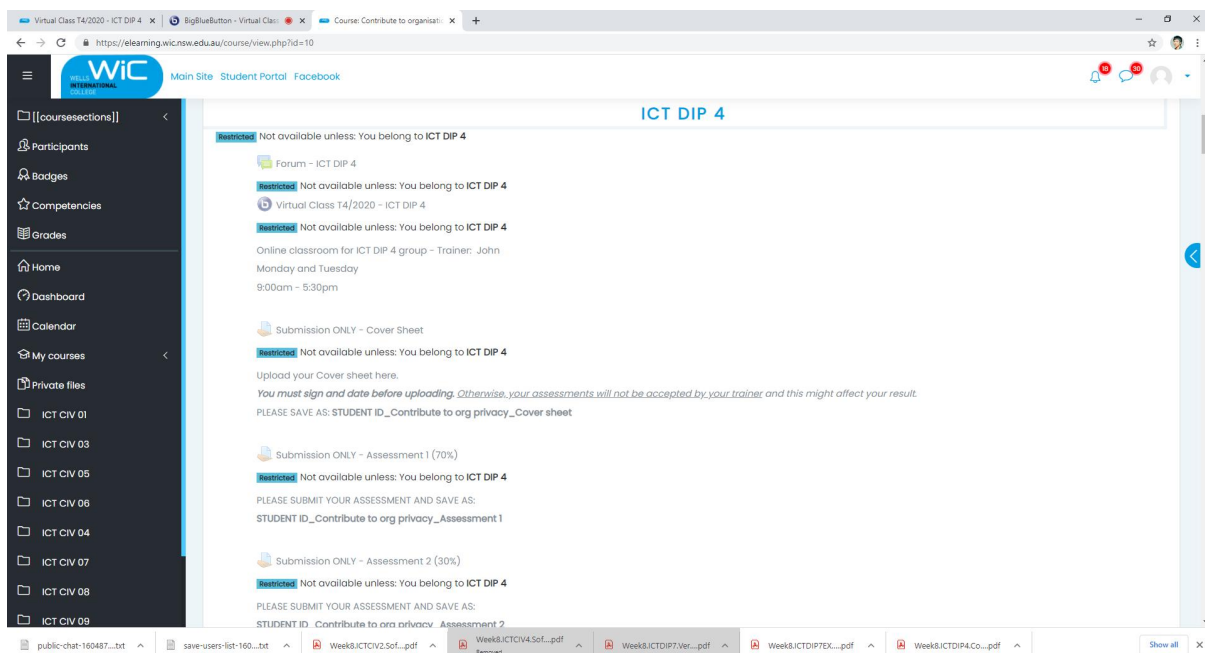
The following are extracts from the business case and other project documentation that has been developed for this project.

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.



The screenshot shows the WIC Student Portal interface for the ICT DIP 4 course. The left sidebar contains navigation links: Participants, Badges, Competencies, Grades, Home, Dashboard, Calendar, My courses, Private files, and a list of ICT CIV modules (01 to 09). The main content area is titled 'ICT DIP 4' and displays several sections, each with a 'Restricted' warning: 'Not available unless: You belong to ICT DIP 4'. These sections include:

- Forum - ICT DIP 4
- Virtual Class T4/2020 - ICT DIP 4
- Online classroom for ICT DIP 4 group - Trainer: John Monday and Tuesday 9:00am - 5:30pm
- Submission ONLY - Cover Sheet
- Submission ONLY - Assessment 1 (70%)
- Submission ONLY - Assessment 2 (30%)

 Each section includes instructions on how to upload or submit work, such as 'Upload your Cover sheet here' and 'PLEASE SUBMIT YOUR ASSESSMENT AND SAVE AS: STUDENT ID_Contribute to org privacy_Cover sheet'. The bottom of the screen shows a file explorer with various PDF documents related to the course.

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: Cyber attacks on critical healthcare infrastructure reveal just how much damage weak security systems can cause in people's lives.

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.	Notify Your Credit Card Issuer. Immediately contact your credit card issuer of the fraudulent transaction	5	3
Student not turning up and exam lapses so \$50 is lost.	Check your account	4	5
ISDN links broken delaying download of exams	check the cabling between the modem and the access server or router	5	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	Data breach	5	4
Theft or misappropriation of test certificates	Fraud Detection	5	4

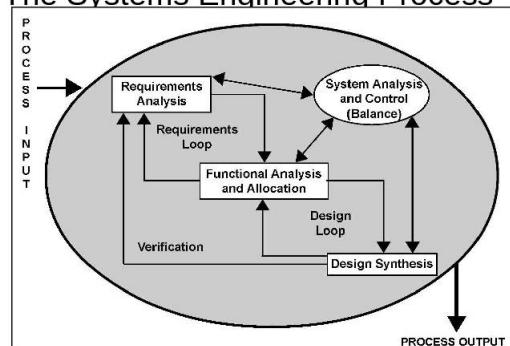
Comment: ...

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.



The Systems Engineering Process



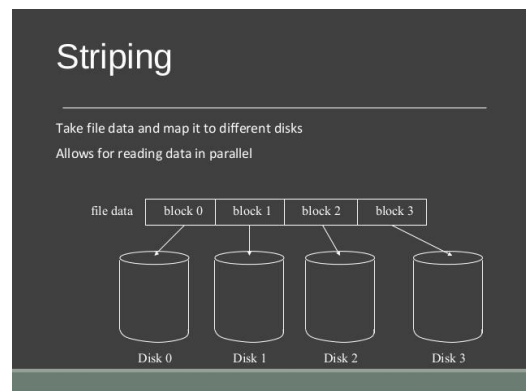
RAID (redundant **array of independent disks**) is a data storage virtualization technology that combines multiple physical **disk** drive components into a single logical unit for the purposes of data **redundancy**, performance improvement, or both.

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.

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
2. 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.

3. 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

...

4. 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: ...

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.



2. 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:

Hard Disk Drive (HDD)	Solid State Drive (SSD)
	
Capacity, price, general use	Speed, reliability, high-performance use

Capacity	Speed(read/write)	Price
1TB	Read 80MB/s Write 160MB/s,	\$59
2TB	Read 540/mbs Write 500. MB/s	\$79
4TB	Read 145MB/s Write153MB/s	\$129
8TB	Read 188.02MB/s Write 187.21MB/s	\$179
SSD 1TB	Read speed 3,500 MBps max. Write speed 2,500 MBps max.	\$339
SSD 2TB	Read 5000 MB/s Write 4400 MB/s	\$619

<https://wellsjohn220.github.io/copcp/#taskeight>

Below these is my web contents support.

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