

# CONTRIBUTE TO ORGANIZATIONAL PRIVACY AND CONTINGENCY PLANS

Wells International College  
18171 Natalia Büttner

Name of Student	Natalia Büttner	ID	18171
-----------------	-----------------	----	-------

## ASSESSMENT 1- CASE STUDY CONTENTS

Assessment 1- Case Study .....	2
Instructions .....	2
Scenario 1: identifying critical systems .....	3
Scenario 2: analysing critical areas .....	5
Scenario 3: determining system criticality .....	9
Scenario 4: identifying possible threats .....	11
Scenario 5: identifying critical systems and threats .....	12
Scenario 6: evaluating preventive and recovery options .....	15
Scenario 7: presenting a strategic recommendation .....	16
Scenario 8: reviewing procedures .....	18
Index .....	22

<https://luthiienn.github.io/copcpby18171>

## 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.

A system is critical for a commercial organisation if its failure results directly or indirectly in loss of life (for example, an air traffic control system) and/or major financial loss. When developing a disaster recovery plan (DRP) it is essential to identify critical systems and ensure they are restored as soon as possible.

Each critical system has a maximum allowable downtime beyond which its loss will severely impact the business. The shorter the period of time before losses start to occur, the more critical the system is. The size of the financial loss, relative to the financial worth of the business, is also significant. The greater the financial loss in percentage terms, the more critical the system is.

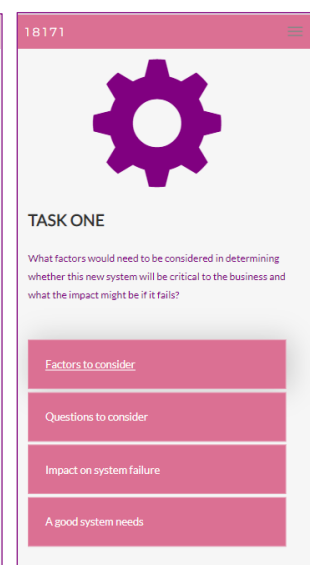
It is important to identify which systems their business relies on.

Each new system should identify its importance and a risk analysis should be undertaken early in the project.

- (loss of) life
- financial loss
- recovery plans,
- maximum allowable downtime
- which systems the business relies on
- risks, system data backups
- how much money could be saved if open online shop, is it worth it?
- etc

### Questions to consider:

- Which application software will the company use?
- What will be the recovery procedures if the system fails?



- What types of data activity will be carried out with the system? What sensitive information will the company handle on the site? e.g., customer credit card details. What are the implications of this?
- What are the resources required for the system?
- For the software application used, what would be the impact on the organisation if you could not access the data for more than one day, between 1 and 8 hours, and less than 1 hour?
- What is the maximum amount of time you could operate without access to the system? Are there any peak periods when disruption would be more or less serious?
- Are there any applications or data that must be continuously available?
- What implications will delivery have? Will delivery be 24 hours a day? And what areas will it cover and how?
- What could be the impact of the new system to the stores and traditional sales? Will it reduce store profitability? What implications could this bring?

#### Impact of system failure:

When undertaking risk analysis and disaster planning, it is usual to focus on critical systems, software and data. The very definition of a critical system is that the business depends upon it and would be severely impacted if the system were not available.

When assessing the impact on a business it is usual to consider the financial impact. Profits will suffer if customers cannot trade with the company.

If an e-commerce website is down, customers may turn to competitors.

If systems are regularly down or slow then customers may eventually go elsewhere.

If faulty systems delay payments, suppliers may stop delivering essential goods and services.

If system fails, the business might:

- lose customer
- lose data
- could be big cost
- impact on customer or supplier relationships
- impact on legal requirements
- impact on staff or morale

#### A good system needs:

- 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
- User and resource security
- System controls to stop errors in the data
- Hot sites (one option among many) to minimise the impact of a major disaster at the main site.

- Encryption, password control to stop unauthorised access to data
- Virus checking software
- User training
- Software keys
- Mirrored disks or RAID (Redundant Array of Inexpensive Disks) systems, clustered systems to allow access to data to continue even if a disk fails.
- Access rights to stop unauthorised access to data and data destruction.
- Uninterruptible power supplies (UPS), standby generator to minimise impact of power loss or spikes and surges

Comment: all bad side must be prevented

URL:

<https://luthienn.github.io/copcpby18171/>

## 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.

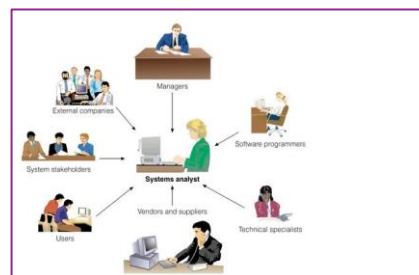
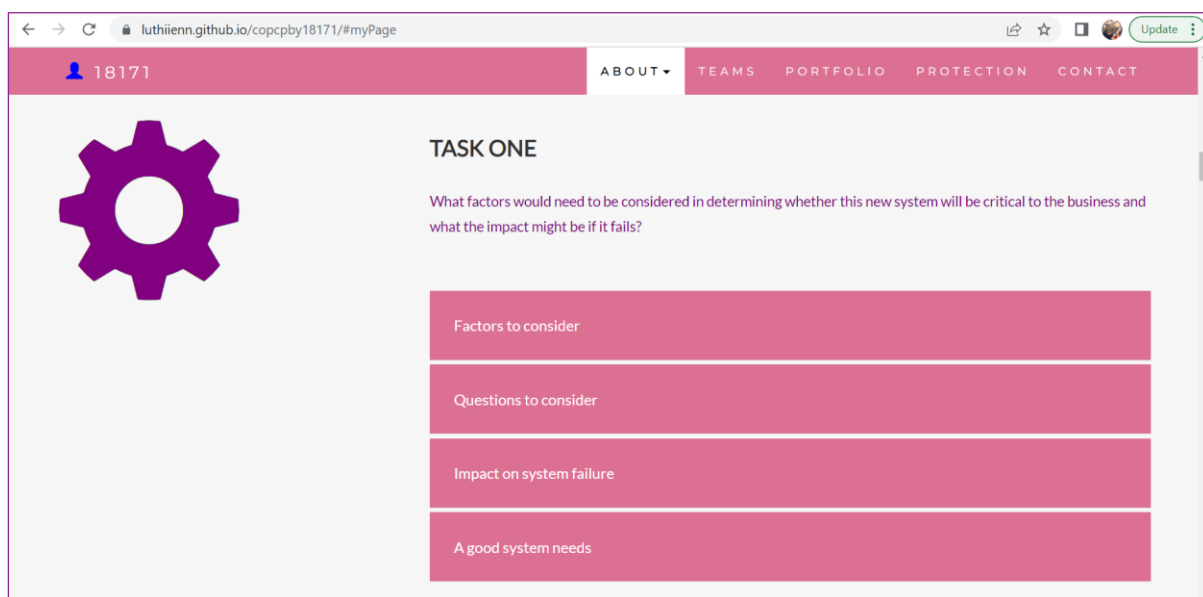
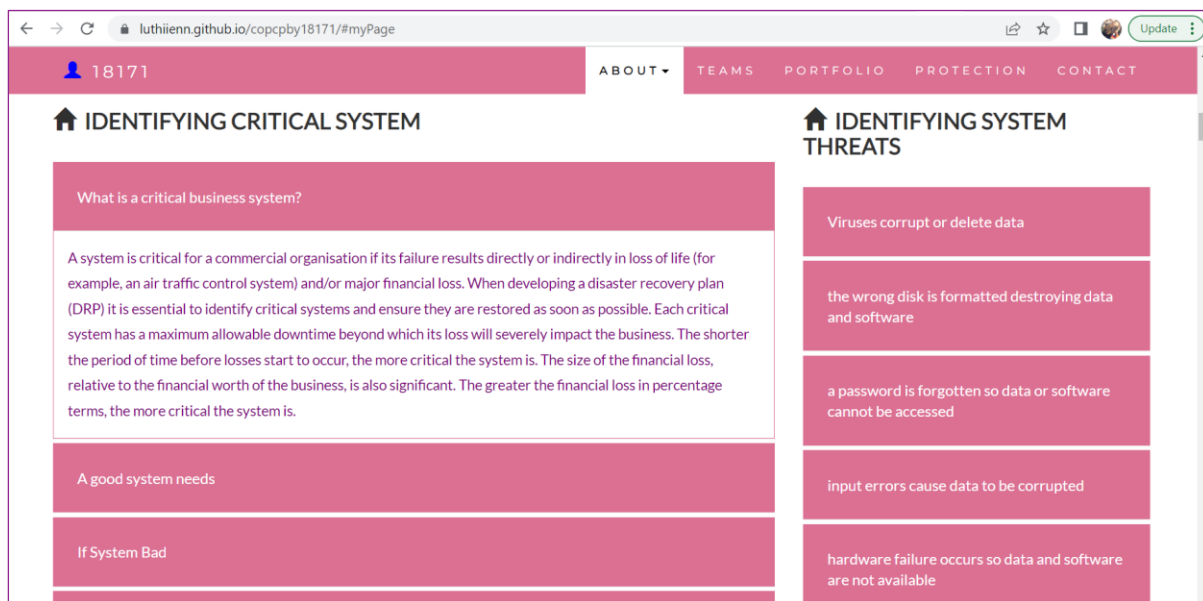


Table 1: critical areas

	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
- Use external backup devices such as tape, zip or CDs
- Nightly backups to be taken offsite: Backup procedures and the process for getting backups offsite and subsequent retrieval
- Regular backups to tapes: Tape backup unit with sufficient capacity. Tapes for the backup. Appropriate backup software.



- Backup tape unit (or zip drive or CD writer), tapes (or zip cartridges or CDs), appropriate backup software and hardware drivers

In order to recover from a disaster it is important that staff complete regular recovery and operational procedures.

Example:

-All client files must be stored on the file server. Only files of a temporary or personal nature should be kept on the local hard disk.

-Every evening, a full backup of the file server is to be completed. Instructions for carrying out the backup are provided in the folder next to the backup tapes in the storage room. The tape rotation scheme is also documented.

-The backup takes several hours and will run automatically overnight. First thing each morning the IT administrator will check the backup report to ensure that it finished correctly.

-The tape will then be stored in the fireproof safe until 4 pm. At that time a courier will collect the tape from the off-site storage agent. Full procedures for recording the dispatch of these tapes are available.

-If the IT administrator is away from the office, the chief financial officer will arrange for someone else to carry out their task.

-Every quarter backups are verified to ensure the backup tapes are readable and data can be recovered

Recovery procedures are put in place to ensure that the system can be quickly restored after the event occurs. For example, the use of a hot-site (one that has a computer system already set up and ready to use) allows for speedy recovery after a fire has gutted the building. This process may also be termed a contingency. In fact DRP is sometimes referred to as contingency planning.

#### Cost of recovery and prevention options

There are many options available to prevent risk from occurring. Some of these are based on policies or standards and may involve no additional cost. However, some options, such as a hot site, can be very expensive.

When deciding which options to adopt, you need to weigh the possible cost of the risk event against the cost of the recovery or prevention option (single incident cost). A simple formula can be used to calculate how much money to allocate to a recovery or prevention measure for the known value of an asset.

Loss= Single Incident Cost X Rate of Threat Occurrence

While a typical small business can still suffer a relatively large loss in the case of critical system failure, it will probably not choose to create a backup site because of the high cost.

## 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
- The following are some potential downsides of cloud backup:

- Cost accumulations: Although a small amount of data is cheap, a lot of data stored over a long period of time steadily increases costs. A company must pay for its data backup storage every month. It's critical to keep a close eye on cloud backup expenses.
- Latency: The cloud can have latency, especially if many users are trying to access the same data or cloud or if an organization is trying to get a large volume of data out of the cloud. This is where a retention policy becomes key; when backed-up data keeps growing, it can become hard to keep a handle on it all, which can delay recovery time.
- Security issues: Some organizations are still worried about the safety of keeping data in the cloud. Confirm that a cloud backup product has the necessary security elements, such as end-to-end encryption. In addition, just because a backup is in the cloud, that doesn't mean it's safe from cyber attacks, so be wary of a false sense of security.
- Slow, costly restores. Restoring data out of the cloud can be a time-consuming and costly process, especially when it involves large volumes. Data egress fees can quickly make restorations expensive.

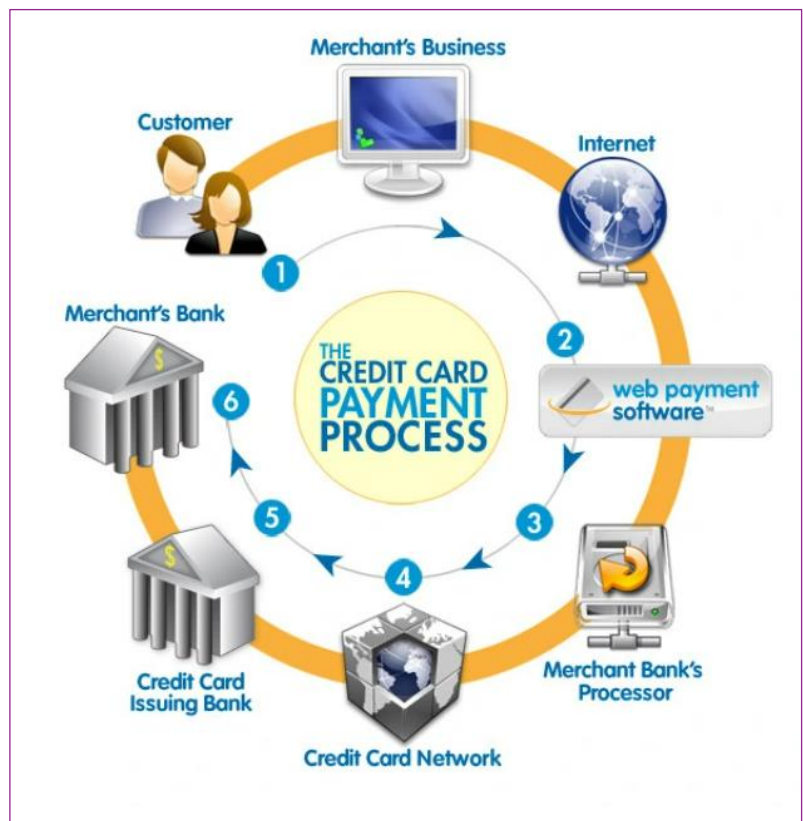
Payment processing or credit card processing is in essence the automation of electronic payment transactions between the merchant and the customer.

#### Prerequisites for Credit Card Online Processing:

- An ecommerce website
- A secure payment gateway
- An online merchant account

#### Credit Card Online Processing: The Process

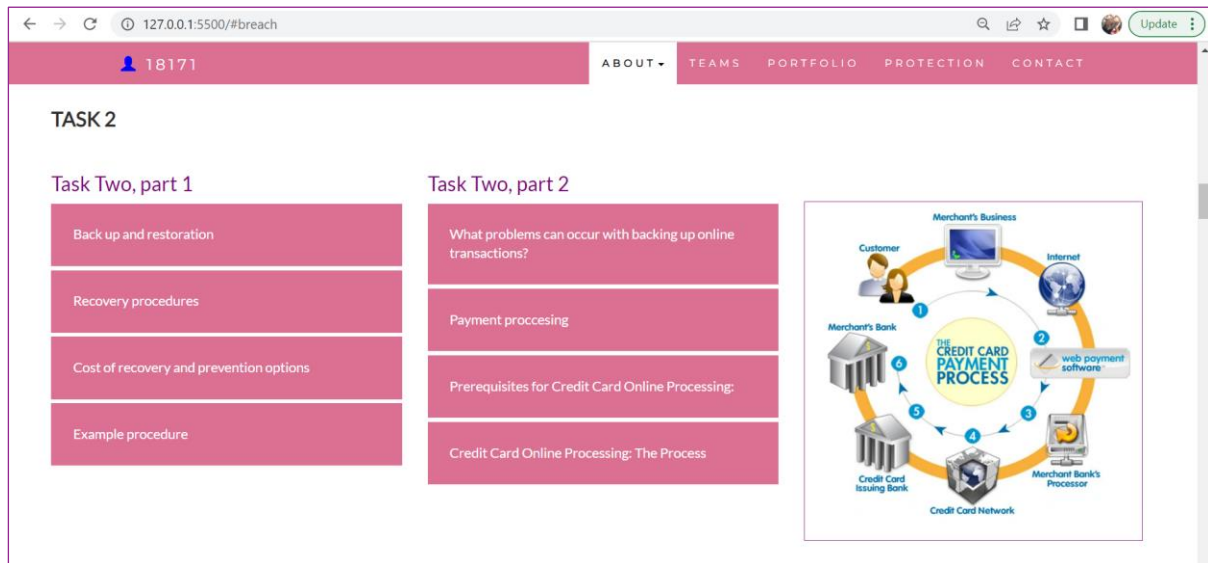
- Merchants receives credit card details from customers through their website
- The card details are then sent to the issuing bank
- Issuing bank approves or disapproves the transaction depending on the availability of the fund in card holder's account
- If approved, the approval is received by the processor
- The amount is then debited from the customer's account and transferred to the merchant's bank account





- Once the whole transaction protocol is clear the funds can be then transferred from the merchant's account into its regular bank account.

The whole transaction process involve two important stages i.e. authorization and settlement. It becomes essential to know the process as each stage incurs some fees, and a minor technical error or partial failure can culminate in increased costs at business end as credit card sales may not be deposited.



The screenshot shows a web application interface for 'TASK 2'. The top navigation bar includes links for 'ABOUT', 'TEAMS', 'PORTFOLIO', 'PROTECTION', and 'CONTACT'. The main content area is divided into two columns: 'Task Two, part 1' and 'Task Two, part 2'. 'Task Two, part 1' lists four items: 'Back up and restoration', 'Recovery procedures', 'Cost of recovery and prevention options', and 'Example procedure'. 'Task Two, part 2' lists four items: 'What problems can occur with backing up online transactions?', 'Payment processing', 'Prerequisites for Credit Card Online Processing:', and 'Credit Card Online Processing: The Process'. To the right of these columns is a diagram titled 'THE CREDIT CARD PAYMENT PROCESS' showing the flow from 'Customer' to 'Merchant's Business' to 'Internet' to 'web payment software' to 'Merchant Bank's Processor' to 'Credit Card Network' to 'Credit Card Issuing Bank' to 'Merchant's Bank' and back to 'Customer'.

### SCENARIO 3: DETERMINING SYSTEM CRITICALITY

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

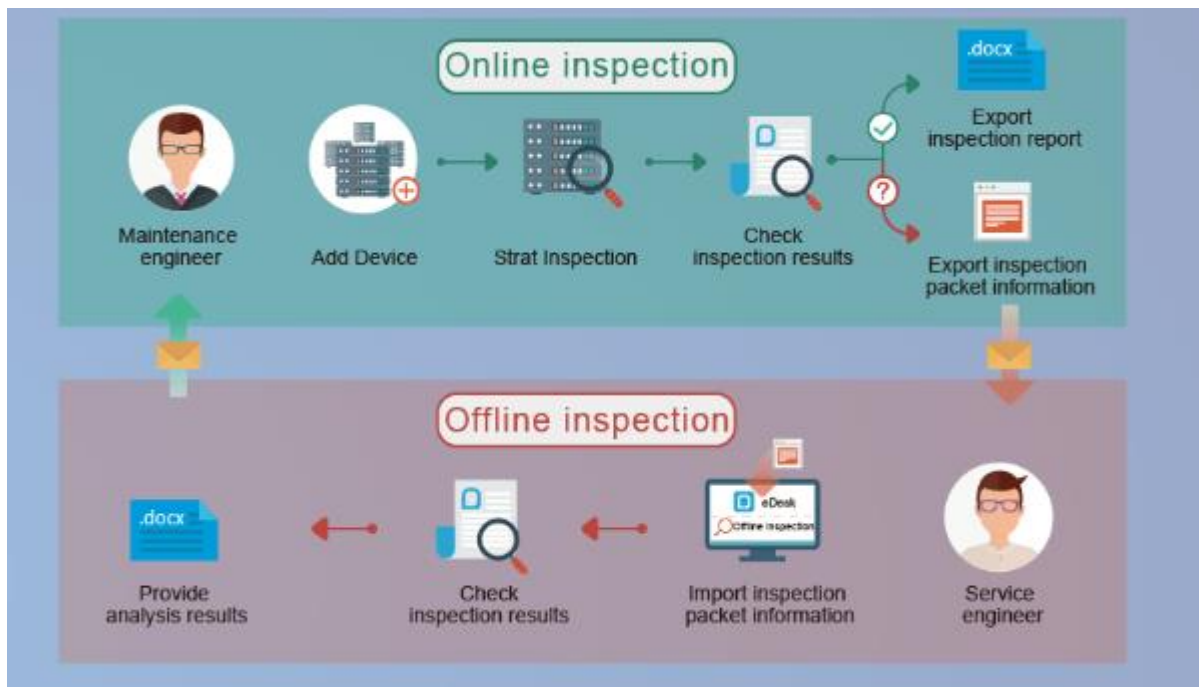
Table: Analysing critical areas: impact of system down for less than 1 hour.

	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



The inspection function helps maintenance engineers check network devices to ensure normal operations of the enterprise network.

Online inspection: Maintenance engineers use the online inspection function to check health of network devices, export inspection reports, and provide the reports to field service engineers to help them optimize the network.

Offline inspection: If maintenance engineers experience difficulties in solving network problems based on inspection results, they can export package information collected during the inspection and provide it to service engineers for offline inspection. Service engineers then import the package information, perform inspection, and analyse the inspection results.

### TASK 3:

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

The system is critical to the organisation.

Reasons:

- after analysing the critical areas, if the system is down for less than 1 hour it will have a very costly and serious impact on cash flow, profitability, customer and supplier relationships.

And the maximum allowable downtime is only 30 minutes.

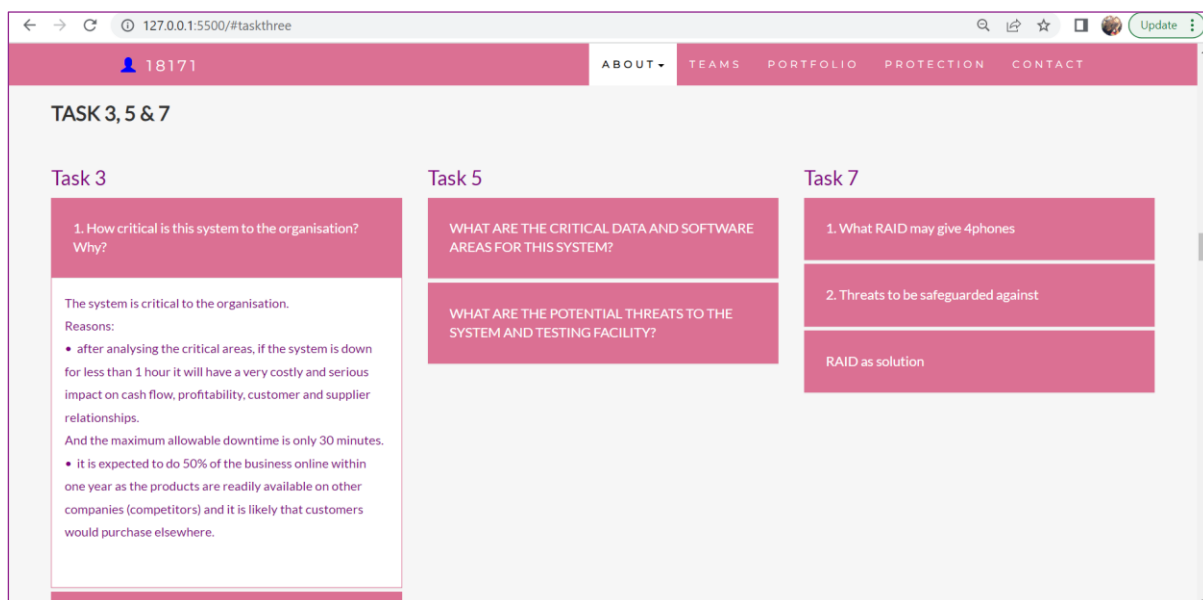
- it is expected to do 50% of the business online within one year as the products are readily available on other companies (competitors) and it is likely that customers would purchase elsewhere.

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.

It is difficult to say if this figure applies to a 24-hour trading period but the maximum time the system can be down may vary depending on the (low/high) activity.



**TASK 3, 5 & 7**

**Task 3**

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

The system is critical to the organisation.

Reasons:

- after analysing the critical areas, if the system is down for less than 1 hour it will have a very costly and serious impact on cash flow, profitability, customer and supplier relationships.
- And the maximum allowable downtime is only 30 minutes.
- it is expected to do 50% of the business online within one year as the products are readily available on other companies (competitors) and it is likely that customers would purchase elsewhere.

**Task 5**

WHAT ARE THE CRITICAL DATA AND SOFTWARE AREAS FOR THIS SYSTEM?

WHAT ARE THE POTENTIAL THREATS TO THE SYSTEM AND TESTING FACILITY?

**Task 7**

1. What RAID may give 4phones

2. Threats to be safeguarded against

RAID as solution

#### 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"> <li>• Change data</li> <li>• Delete data</li> <li>• Add fake or wrong data</li> </ul>	External*
Hardware failures that stop the site operating.	Internal

<ul style="list-style-type: none"> <li>• Hard disk broken</li> <li>• Power supply down</li> <li>• Cable is failed to link</li> </ul>	
Denial of service attacks to bring the service down. ...	External
Data destruction by any means such as a user deleting a file. ...	Internal
Misuse of information by internal staff. ...	Internal
Power problems so site is down. ...	External
Overloaded site so response is slow. ...	External
Customers falsifying information to avoid payment. ...	External
Incorrect information such as wrong prices so customers pay too little. ...	Internal
Incorrect information such as wrong quantity in stock so customers have to wait for delivery. ...	Internal
Major disaster so site is down. <ul style="list-style-type: none"> <li>• Earthquake, bushfire, terrorist</li> <li>• ...</li> </ul>	External*

#### TASK 4:

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

There are many ways to categorise threats. One way is to consider whether the source of the threat is internal or external.

It is important to consider possible threats to the system. A risk analysis will help determine these.

An organisation undertakes an IT risk analysis to identify: how dependent it is on IT systems, what could go wrong with these systems, what system assets they might lose, what can be done about it

IT systems can comprise many parts including: hardware, software, networks, data, technical skills, projects.

#### 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?

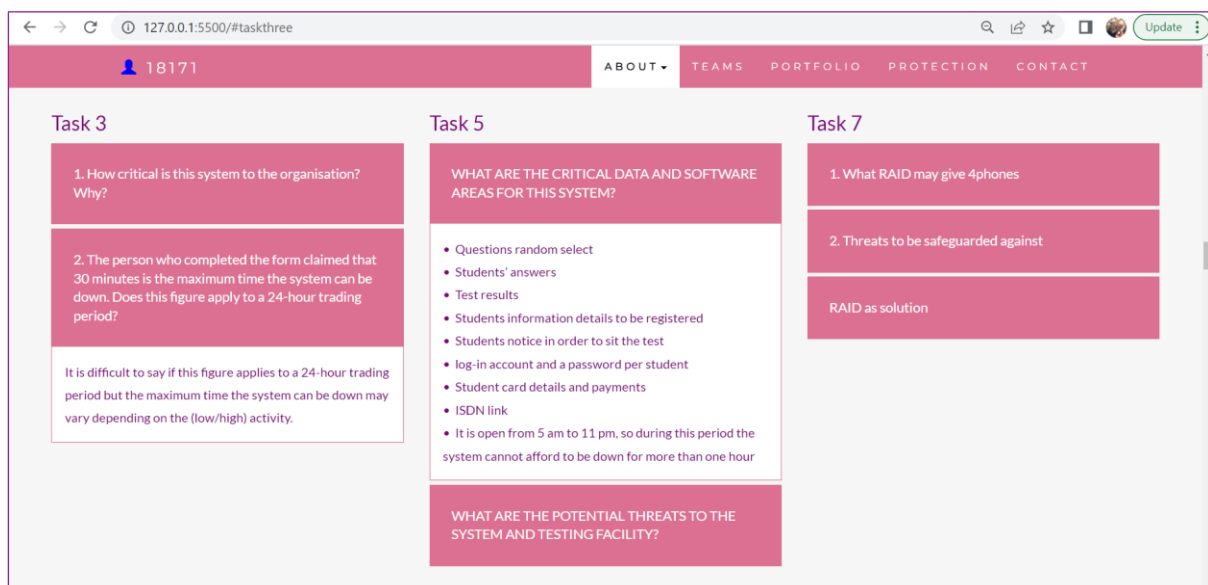
---

- Questions random select
- Students' answers
- Test results
- Students information details to be registered

- Students notice in order to sit the test
- log-in account and a password per student
- Student card details and payments
- ISDN link
- It is open from 5 am to 11 pm, so during this period the system cannot afford to be down for more than one hour

#### WHAT ARE THE POTENTIAL THREATS TO THE SYSTEM AND TESTING FACILITY?

- Hack the question
- Get answer key
- System is going down
- Problems with the ISDN links and/or download of exams
- Viruses corrupt or delete data
- Hardware failure occurs so data and software are not available
- Data and software files are deleted
- Theft of data and loss of confidential information especially customer details transmitted over the Internet or wide area network connection.
- Breakdowns of Internet or wide area network connection or failure of critical systems hardware
- Fire or earthquake which renders the system inaccessible.
- Flooding which renders the system inaccessible. Water from sprinklers or sewer lines can cause flooding of offices.
- Hack customers credit card details
- Power problems make the system inaccessible. Power spikes or outages can disrupt critical systems.



The screenshot shows a web application with a navigation bar at the top containing links: ABOUT, TEAMS, PORTFOLIO, PROTECTION, and CONTACT. The main content area is divided into three columns, each representing a task.

**Task 3**

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

It is difficult to say if this figure applies to a 24-hour trading period but the maximum time the system can be down may vary depending on the (low/high) activity.

**Task 5**

WHAT ARE THE CRITICAL DATA AND SOFTWARE AREAS FOR THIS SYSTEM?

- Questions random select
- Students' answers
- Test results
- Students information details to be registered
- Students notice in order to sit the test
- log-in account and a password per student
- Student card details and payments
- ISDN link
- It is open from 5 am to 11 pm, so during this period the system cannot afford to be down for more than one hour

WHAT ARE THE POTENTIAL THREATS TO THE SYSTEM AND TESTING FACILITY?

**Task 7**

- 1. What RAID may give 4phones
- 2. Threats to be safeguarded against

RAID as solution

## 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	3
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.	Keep students ID during test, verify identity before taking exam Insurance to cover fraud	1 3	5
Student not turning up and exam lapses so \$50 is lost.	Charge the \$50 as a cancellation fee at time of booking	1	3
ISDN links broken delaying download of exams	Alternate links	4	5
Hackers who may try to access test data or student data	Fire wall, virus checking software	1	5
Internal unauthorised access to test data or student data	Encryption, password control	1	5
Theft or misappropriation of test certificates	Secure system for certificates	1	5

There are two main strategies for dealing with risk (apart from ignoring it in the hope it will go away): prevent or recover. Both options have the objective of minimising the impact of the risk event.

With prevention you attempt to decrease the probability (maybe even to 0) of the event occurring or causing damage. Many events can never be totally eliminated but their impact may be minimised.

For example, an extensive sprinkler system will ensure that any outbreak of fire does minimal damage. It is almost impossible to totally prevent a fire from occurring in the first place but this is still considered a preventative action. This type of activity may also be termed risk minimisation.

## 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.

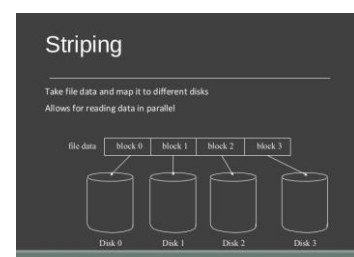
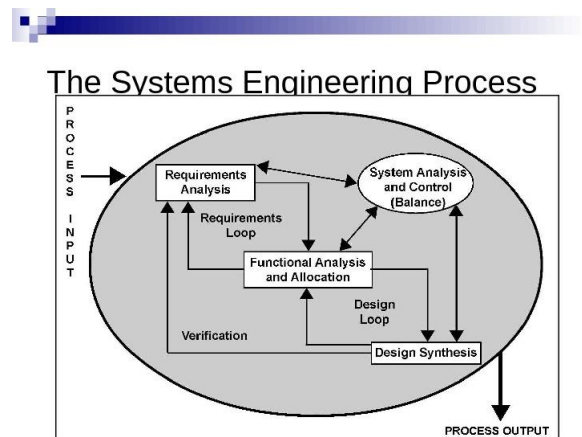
RAID (redundant **array of independent disks**) is a data storage virtualization technology that combines multiple physical **disk** drive components into a single logical unit for the purposes of data **redundancy**, performance improvement, or both.

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.

### 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
- Protection against the failure of a single disk in the server
- A cost-effective solution until eventually have a high-speed link to a backup site in 10 months' time.
- Improvement in the performance of disk access in the region of 10%.

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)

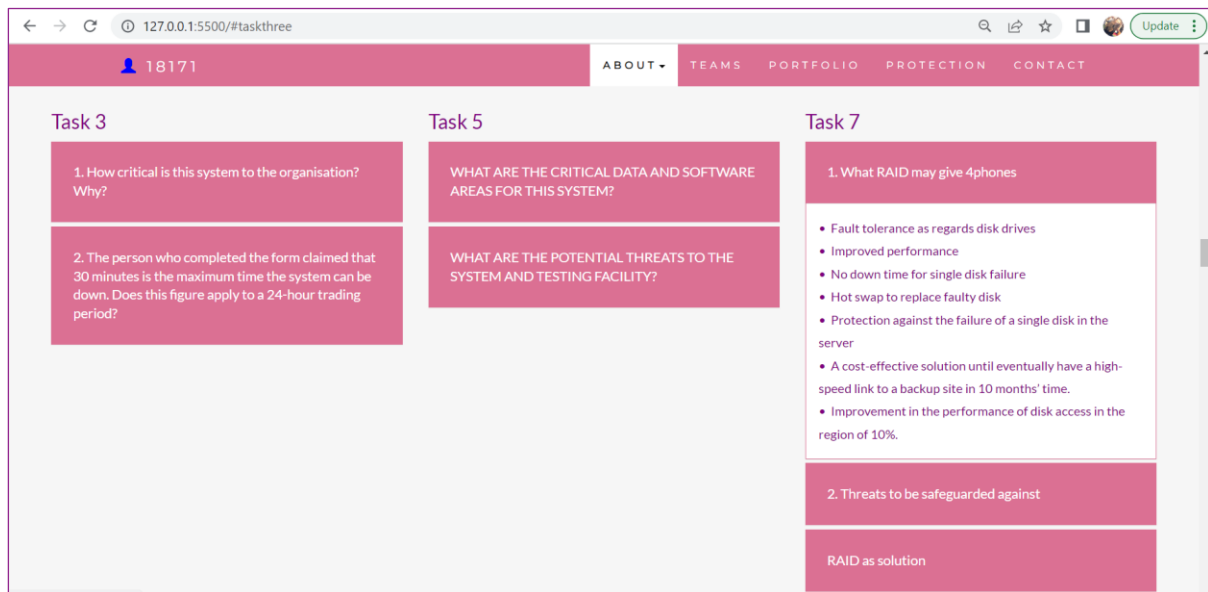
- Orders placed on the web = \$100,000 per day
- Assume 50% would go elsewhere if our system down
- Loss = \$50,000
- RAID costs only \$12,000

The cost of RAID is very low compared to the possible losses so it is very convenient.

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

RAID is a good solution for many reasons. It will provide protection against the failure of a single disk in the server and it is a cost-effective solution until eventually have a high-speed link to a backup site in 10 months' time. It will also improve the performance of disk access in the region of 10%. The cost of RAID is very low compared to the possible losses.



18171

ABOUT TEAMS PORTFOLIO PROTECTION CONTACT

### Task 3

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

### Task 5

WHAT ARE THE CRITICAL DATA AND SOFTWARE AREAS FOR THIS SYSTEM?

WHAT ARE THE POTENTIAL THREATS TO THE SYSTEM AND TESTING FACILITY?

### Task 7

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
  - Protection against the failure of a single disk in the server
  - A cost-effective solution until eventually have a high-speed link to a backup site in 10 months' time.
  - Improvement in the performance of disk access in the region of 10%.
2. Threats to be safeguarded against

RAID as solution

## 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

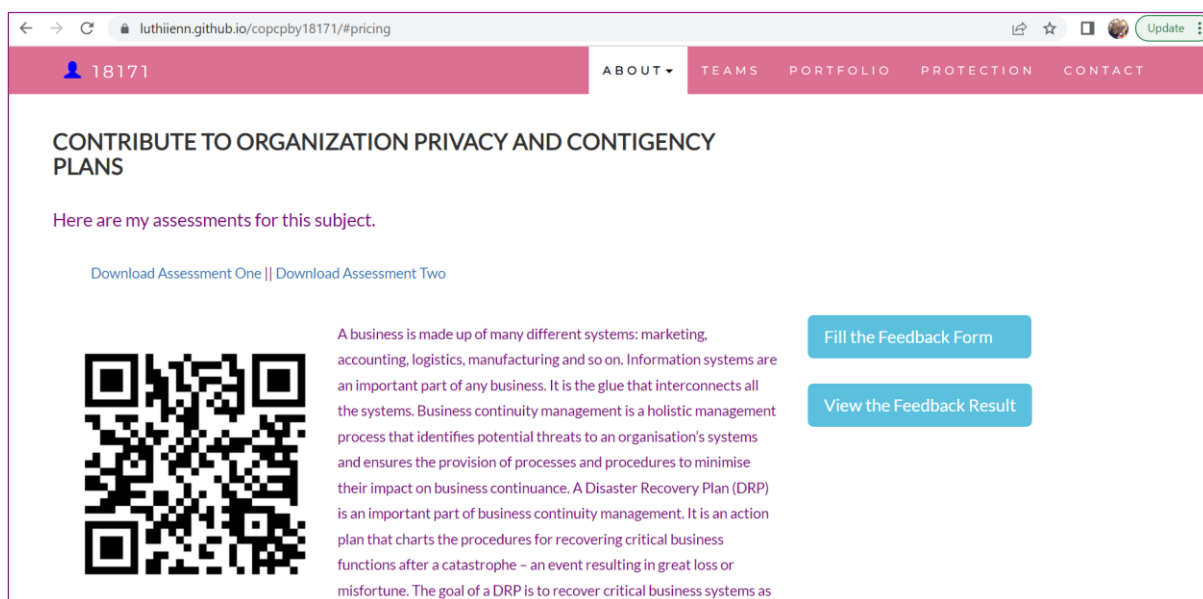
The current tape unit is too slow and does not have the capacity to store a full back up on a single tape. Typical hardware specifications and costs are:

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

Capacity	Speed(read/write)	Price
1TB	...	\$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? ...

Below these is my web contents support:

<https://luthiienn.github.io/copcpby18171/#myPage>




← → ↻ luthienn.github.io/copcpby18171/#pricing

18171 ABOUT TEAMS PORTFOLIO PROTECTION CONTACT

## CONTRIBUTE TO ORGANIZATION PRIVACY AND CONTINGENCY PLANS

Here are my assessments for this subject.

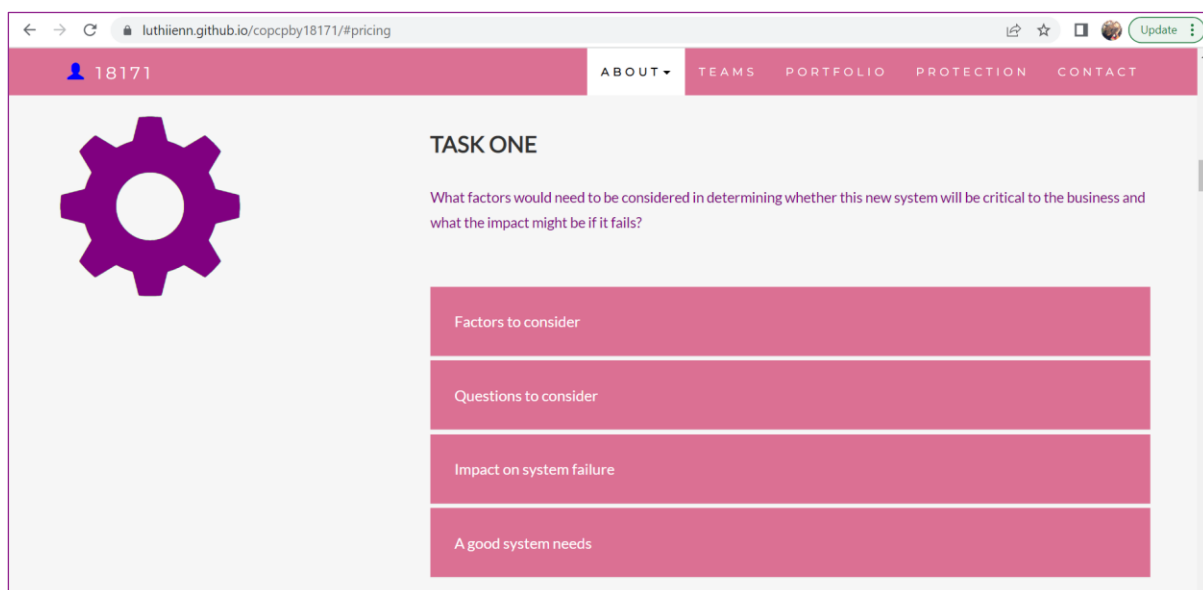
[Download Assessment One](#) || [Download Assessment Two](#)



A business is made up of many different systems: marketing, accounting, logistics, manufacturing and so on. Information systems are an important part of any business. It is the glue that interconnects all the systems. Business continuity management is a holistic management process that identifies potential threats to an organisation's systems and ensures the provision of processes and procedures to minimise their impact on business continuance. A Disaster Recovery Plan (DRP) is an important part of business continuity management. It is an action plan that charts the procedures for recovering critical business functions after a catastrophe – an event resulting in great loss or misfortune. The goal of a DRP is to recover critical business systems as


[Fill the Feedback Form](#)

[View the Feedback Result](#)



← → ↻ luthienn.github.io/copcpby18171/#pricing

18171 ABOUT TEAMS PORTFOLIO PROTECTION CONTACT



## TASK ONE

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?

- Factors to consider
- Questions to consider
- Impact on system failure
- A good system needs

← → ↻ luthienn.github.io/copcby18171/#pricing

18171 ABOUT TEAMS PORTFOLIO PROTECTION CONTACT

## TASK 2

### Task Two, part 1

- Back up and restoration
- Recovery procedures
- Cost of recovery and prevention options
- Example procedure

### Task Two, part 2

- What problems can occur with backing up online transactions?
- Payment processing
- Prerequisites for Credit Card Online Processing:
- Credit Card Online Processing: The Process



← → ↻ 127.0.0.1:5500/#taskthree

18171 ABOUT TEAMS PORTFOLIO PROTECTION CONTACT

### Task 3

- How critical is this system to the organisation? Why?
- 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?

It is difficult to say if this figure applies to a 24-hour trading period but the maximum time the system can be down may vary depending on the (low/high) activity.

### Task 5

WHAT ARE THE CRITICAL DATA AND SOFTWARE AREAS FOR THIS SYSTEM?

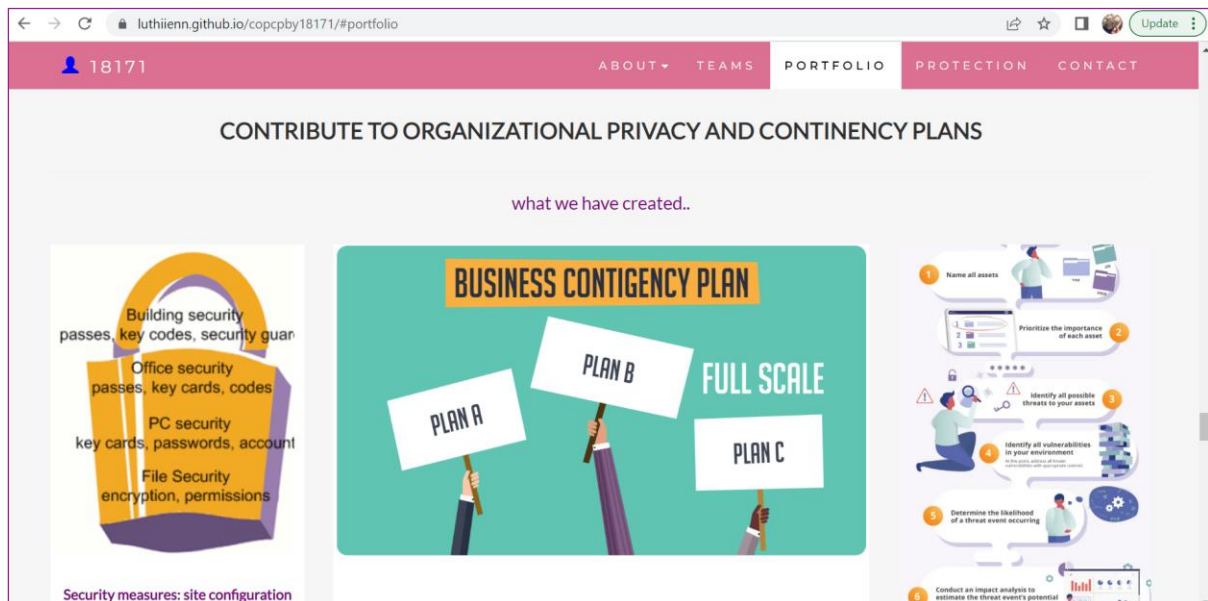
- Questions random select
- Students' answers
- Test results
- Students information details to be registered
- Students notice in order to sit the test
- log-in account and a password per student
- Student card details and payments
- ISDN link
- It is open from 5 am to 11 pm, so during this period the system cannot afford to be down for more than one hour

WHAT ARE THE POTENTIAL THREATS TO THE SYSTEM AND TESTING FACILITY?

### Task 7

- What RAID may give 4phones
- Threats to be safeguarded against

RAID as solution



## 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