**T.** +61 2 9283 4388 | **F.** +61 2 9283 0748 | **E.** info@wic.nsw.edu.au
Lower Ground, 101 Sussex St., Sydney NSW 2000 Australia | www.wic.nsw.edu.au

**ABN:** 19 080 559 600 | **CRICOS CODE:** 01856K | **RTO:** 90501

# Assessment 1 – Role Play

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.

## 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** | 10% | | | |
| **From other data files** | 10% | | | |
| **From irrecoverable sources such a telephone calls** | 80% | | | |
| **Developed at the workstation such as report writing** | | | | |
| **Other—specify** | | | | |

### *Task 2:*

1. What issues need to be considered for backup and restoration of data?
2. What problems can occur with backing up online transactions?

## 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 | | |
| **Impact on profitability** | X | | |
| **Impact on customer or supplier relations** | 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.
- ❑ Are there any applications or data that you believe must be continuously available?
  - No—subject to no more than 30 minutes downtime

### *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?

## 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. | |
| Hardware failures that stop the site operating. | |
| Denial of service attacks to bring the service down. | |
| Data destruction by any means such as a user deleting a file. | |
| Misuse of information by internal staff. | |
| Power problems so site is down. | |
| Overloaded site so response is slow. | |
| Customers falsifying information to avoid payment. | |
| Incorrect information such as wrong prices so customers pay too little. | |
| Incorrect information such as wrong quantity in stock so customers have to wait for delivery. | |
| Major disaster so site is down. | |

### *Task 4:*

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

## 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:*

1. What are the critical data and software areas for this system?
2. What are the potential threats to the system and testing facility?

## 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 | | | |
| Hardware problems that stop system operating | | | |
| Credit card fraud. With the short time frame the student could be tested before any credit card discrepancy was identified. | | | |
| Student not turning up and exam lapses so $50 is lost. | | | |
| ISDN links broken delaying download of exams | | | |
| Hackers who may try to access test data or student data | | | |
| Internal unauthorised access to test data or student data | | | |
| Theft or misappropriation of test certificates | | | |

## 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.

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
2. Threats to be safeguarded against
3. Cost benefit analysis (Assume 50% would go elsewhere if the system is down)
4. How RAID supports the business

## 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.

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