WELLS INTERNATIONAL COLLEGE

T. +61 2 9283 4388 | **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 Task 1

[70415] JINWOONG LEE

Name of Student	JINWOONG LEE	ID	70415

Assessment 1- Case Study

Contents

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.

1. **How much of the company's revenue is generated from online sales?**
   - If a significant portion of the company's revenue is generated from online sales, then the new system will be critical to the business. If online sales are not a significant part of the company's revenue, then the new system may not be as critical.

2. **How will the new system impact the company's ability to reach new customers?**
   - The new system could help the company reach new customers who may not be aware of the company or its products. If the new system is successful, it could help the company increase sales and grow its business.

3. **How will the new system impact the company's ability to provide customer service?**
   - The new system could help the company improve customer service by providing customers with a way to contact the company, find information about products and services, and make purchases. If the new system is successful, it could help the company improve customer satisfaction and loyalty.

4. **What are the risks associated with the new system?**
   - There are a number of risks associated with developing and implementing a new system. These risks include:
     - The system may not be able to handle the volume of traffic.
     - The system may not be secure.
     - The system may not be user-friendly.
     - The system may not be compatible with the company's existing systems.

- If the new system fails, it could have a significant impact on the company. The company could lose sales, customers, and revenue. The company could also damage its reputation.

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?**

- Frequency of backups. This will depend on the size and complexity of the website, as well as the amount of data that is being generated.
- Method of backup. There are a number of different methods that can be used to back up data, including:
  - Local backups. These backups are stored on the same device as the website. This is the simplest and most cost-effective method, but it is also the least secure.
  - Remote backups. These backups are stored on a separate device or server. This is a more secure method, but it is also more expensive.
  - Cloud-based backups. These backups are stored on a remote server that is hosted by a third-party company. This is the most secure method, but it can also be the most expensive.
- How long should data be kept in backup? (Data retention) This will depend on the laws and regulations that apply to the website, as well as the company's own policies. For example, some companies may be required to keep data for a certain period of time for tax purposes.
- Testing and recovery. It is important to test backups regularly to make sure that they can be restored successfully. This can be done by restoring a backup to a test environment and checking that all of the data is present and accessible.

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

- Human error: Human error is always a possibility when it comes to backing up data. For example, a user may accidentally delete a backup file, or they may forget to create a backup in the first place.
- Technical problems: Technical problems can also cause backup failures. For example, a power outage or a hardware failure could prevent a backup from being created or restored.
- Cyber attacks: Cyber attacks are a growing threat to businesses of all sizes. If a website is hacked, the attacker could steal sensitive data, including customer financial information.
- Data corruption: Data corruption can occur for a variety of reasons, such as a power surge, a hardware failure, or a software bug. If data corruption occurs, it can make it impossible to restore the data from a backup.

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?

   Since 50% of business is making from online within 1 year, this system is very critical for Urban Wear. If system is down:

   - Loss of sales: If customers are unable to purchase clothes online, they may go to a competitor's website instead. This can lead to lost sales and revenue for the company.
   - Damage to reputation: If customers are unable to use the website, they may become frustrated and take their business elsewhere. This can damage the company's reputation and make it more difficult to attract new customers in the future.
   - Increased costs: If the website is down for an extended period of time, the company may incur additional costs, such as lost revenue, customer support costs, and marketing costs.

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?

   The system can be down for a maximum of 30 minutes does not necessarily apply to a 24-hour trading period. The system could be down for more than 30 minutes if there is a major outage or if there is a planned maintenance window. However, the company should strive to keep the system up and running as much as possible, and they should have a plan in place to mitigate the impact of any downtime.

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.

Task 4:

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

Threat	Category
Hackers attempting to get to the data stored on the site. • Change data • Delete data • Add fake or wrong data	Extenal*
Hardware failures that stop the site operating. • Hard disk broken • Power supply down • Cable is failed to link	Internal
Denial of service attacks to bring the service down. ...	Extenal*
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. ...	Extenal
Overloaded site so response is slow. ...	Extenal
Customers falsifying information to avoid payment. ...	Extenal
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. • Earthquake, bushfire, terrorist	Extenal

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?

1. Student Data Management: The system should securely store and manage student data, including personal information, exam history, and progress tracking. This data is crucial for managing student records, generating reports, and facilitating certification processes.

2. Exam Content Management: The system should have a database or content management system to store and manage exam questions, answers, and related materials. This ensures the availability, integrity, and security of the exam content, as well as the ability to update and maintain it over time.

3. Test Administration and Scheduling: The system should support functionalities for test administration, including exam scheduling, registration, and logistics management. This area involves coordinating exam sessions, assigning testing locations, and ensuring appropriate proctoring and security measures are in place.

4. Exam Delivery and Assessment: The software should enable the secure and reliable delivery of exams to students. This may involve features such as randomized question selection, time limits, and monitoring tools to prevent cheating. The system should also provide automated assessment and grading mechanisms to evaluate student performance accurately.

5. Certification and Credentialing: The system should support the management of certifications and credentials obtained by students. This includes tracking completed exams, issuing certificates, and providing verification mechanisms for potential employers or other institutions.

6. Integration with Vendor Systems: Since the tests will include vendor exams like Microsoft MCSE or Novell CNA, the system should integrate with the respective vendor systems to access exam content, synchronize certifications, and validate exam results.

7. Security and Data Privacy: Given the sensitive nature of student data and exam content, strong security measures should be implemented, including encryption, access controls, and regular security audits. Compliance with data privacy regulations, such as GDPR or CCPA, should also be ensured.

8. Reporting and Analytics: The system should have reporting and analytics capabilities to generate insights into student performance, exam results, and overall system usage. This data can help identify areas for improvement, track trends, and support decision-making processes.

9. Scalability and Reliability: The software should be designed to handle a large number of students and exams simultaneously, ensuring system availability, responsiveness, and scalability. Measures such as load balancing, fault tolerance, and redundancy should be considered to minimize downtime and ensure a smooth testing experience.

10. User Interface and Experience: The system should have a user-friendly interface for both administrators and students, allowing them to easily navigate through the system, access exam materials, and manage their accounts. Intuitive design and responsive interfaces can enhance the overall user experience.

What are the potential threats to the system and testing facility?

1. Security Breaches: As the system involves handling sensitive student information, including personal data and exam results, there is a risk of unauthorized access, data breaches, or hacking attempts. This could lead to the compromise of student records, financial information, or tampering with exam results.

2. Vendor System Integration Issues: The reliance on ISDN links with multiple vendors introduces the risk of connectivity issues or compatibility problems. Any disruptions or failures in these links could impact the ability to download tests or transmit student information, leading to delays or system downtime.

3. Unauthorized Access to Tests: The absence of physical storage of tests at the test centers could make the system vulnerable to unauthorized access. Attackers may attempt to gain access to the server or manipulate the test content, potentially compromising the integrity and security of the exams.

4. System Availability and Reliability: The proposed operating hours from 5 am to 11 pm, seven days a week, put significant demands on the system's availability and reliability. Any system outages, hardware failures, or software glitches could disrupt the testing process and lead to dissatisfaction among students.

5. Lack of Test Utilization: The requirement to pay for the tests upfront, regardless of whether they are used or not, introduces a financial risk. If tests go unused due to unforeseen circumstances, technical issues, or insufficient demand, it could result in financial losses for the test centers.

6. Compliance and Contractual Obligations: Test centers must adhere to strict contract obligations with vendors. Failure to comply with these obligations, such as timely transmission of student information or maintaining the required stock of certificates, may result in penalties, contract termination, or denial of test facility access.

7. Fraud and Cheating: The system needs robust measures to prevent fraud and cheating during the testing process. Without adequate security measures, students may attempt to impersonate others, manipulate exam results, or use unauthorized resources during the tests, compromising the integrity of the certification process.

8. System Scalability: The ability to process 20 students per hour may pose scalability challenges during peak periods of high demand. If the system cannot handle the volume of student registrations or experiences performance issues under heavy loads, it could result in delays and dissatisfaction among students.

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.

Threat	Options	Cost (1-5)	Business requirement (1-5)
Disasters that stop the centre operating such as fire, flood, earthquake	Implement an off-site backup and disaster recovery plan to ensure data and system availability in case of physical damage to the center.	5	4
Hardware problems that stop system operating	Have spare hardware components available for quick replacements if needed.	4	5
Credit card fraud. With the short time frame the student could be tested before any credit card discrepancy was identified.	Implement robust security measures to protect credit card transactions, including encryption and secure payment gateways.	3	5
Student not turning up and exam lapses so $50 is lost.	Clearly communicate the cancellation and rescheduling policies to students to minimize no-shows.	1	3
ISDN links broken delaying download of exams	Have backup plans in place, such as alternative connectivity options, to ensure timely exam downloads even in the event of link failures.	2	4
Hackers who may try to access test data or student data	Implement strong security measures, such as firewalls, intrusion detection systems, and encryption, to protect against external threats.	3	5
Internal unauthorised access to test data or student data	Enforce strong password policies and user account management practices.	1	5
Theft or misappropriation of test certificates	Implement physical security measures, such as secure storage areas, surveillance systems, and restricted access to test certificates.	3	4

Scenario 7: presenting a strategic recommendation

After completing the risk analysis for the 4phones e-commerce project, you believe that RAID (Redundant Array of Inexpensive Disks) should be used in the server to prevent hardware failure. You also wrote a report that justifies your decision.

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

You covered the following matters in your report:

- ❑ The use of RAID will protect against the failure of a single disk in the server. Since disks are electromechanical devices, they are the most susceptible component to wear and tear and subsequent breakdown. They also store the data that may be difficult or impossible to recover depending upon when the breakdown occurs. They will not protect against other hardware failures such as power failures or major disasters such as fire.
- ❑ The server has been identified as a critical component in the system and its loss could cause considerable problems and loss of revenue and profit.
- ❑ All parts of the system will be impacted by the loss of disks in the server. The cost to the business of losing the server disks for a day could be $100,000. (Orders placed on the web $100,000 per day)
- ❑ The only current facility to cope with such an event is to restore from backup. This takes four hours during which time we would not be able to operate the system. In addition, the backup tapes could be on average 12 hours old and so will not have current information.
- ❑ While we will eventually have a high-speed link to a backup site, the use of RAID provides a cost-effective solution until this link is established in 10 months' time.
- ❑ The cost of a RAID system would be in the region of $12,000. We will also gain an improvement in the performance of disk access in the region of 10%.
- ❑ If this recommendation is approved, we can order the RAID components and have it installed and operating within a week.

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

    - Improved Data Reliability: RAID (Redundant Array of Independent Disks) provides redundancy by distributing data across multiple drives. This redundancy ensures that if one drive fails, the data can still be accessed and the system remains operational, minimizing the risk of data loss.
    - Enhanced Performance: Certain RAID configurations, such as RAID 0 or RAID 10, can improve read and write speeds by striping data across multiple drives. This can result in faster data access and improved system performance, benefiting the overall user experience on the 4phones e-commerce platform.
    - Scalability and Capacity: RAID allows for the expansion of storage capacity by adding additional drives to the array. This flexibility enables 4phones to accommodate growing data storage needs and support future business growth without significant disruptions.

2. Threats to be safeguarded against
    - Hard Drive Failures: RAID helps safeguard against hard drive failures by distributing data across multiple drives. In the event of a drive failure, the system can continue to function without interruption, ensuring that 4phones' operations can proceed smoothly.

    - Data Loss: By providing redundancy, RAID protects against data loss. In case of drive failure, the data can be reconstructed or accessed from the remaining drives in the array, reducing the risk of critical data being permanently lost and minimizing potential business disruptions.

3. Cost benefit analysis (Assume 50% would go elsewhere if the system is down)
    a. Orders placed on the web = $100,000 per day
    b. Assume 50% would go elsewhere if our system down
    c. Loss = $50,000
    d. RAID costs only $12,000

4. How RAID supports the business
    - Business Continuity: RAID provides a critical layer of protection against hardware failures, ensuring that the 4phones e-commerce platform remains operational even if individual drives fail. This helps maintain business continuity, minimizes disruptions, and ensures that customers can continue to access the platform without interruptions.

    - Data Integrity and Availability: By distributing data across multiple drives, RAID helps maintain data integrity and availability. The redundancy offered by RAID protects against data loss, provides faster data access, and ensures that customer data and transactions remain secure and accessible.

    - Scalability and Flexibility: RAID allows for the expansion of storage capacity as the business grows. This scalability enables 4phones to accommodate increasing data storage requirements, support a larger customer base, and handle future business growth without significant infrastructure changes or disruptions.

    - Cost Savings: Implementing RAID can help reduce costs associated with data recovery, system downtime, and potential revenue loss. By minimizing the risk of hardware failures and offering easier data restoration, RAID can contribute to cost savings in terms of data recovery services, customer retention, and revenue generation.

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.

    - All software loaded on the network must be checked for virus contamination before it is installed. This includes shrink-wrapped (brand new) software. The virus checking program selected should be regularly updated to protect against new viruses.
    - Users must run a virus scan on all incoming and outgoing e-mail messages. This includes attachments and any other files that are sent or received.
    - Users must not open attachments or click on links in e-mail messages from unknown senders. These messages may contain viruses or other malicious software.
    - Users must not download software from the Internet unless they are sure that the source is legitimate. Downloaded software may be infected with viruses or other malicious software.
    - Users must create regular backups of their data. This will help to protect against data loss in the event of a virus attack.

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

    - Antivirus software: Antivirus software is essential for protecting against viruses. It should be updated regularly to protect against new viruses.
    - Firewall: A firewall can help to protect against unauthorized access to the network.
    - Data backup solution: A data backup solution can help to protect against data loss in the event of a virus attack. (i.e. cloud services or SSD)