Academic Year: 2024-2025 Assessment

Module Code: CO2521	**Module Title**: Information Security Management
Title of the Brief: Risk Assessment Report	**Type of assessment**: Coursework Report

Introduction

This Assessment Pack consists of a detailed assignment brief, guidance on what you need to prepare, and information on how class sessions support your ability to complete successfully. You will also find information on this page to guide you on how, where, and when to submit. If you need additional support, please make a note of the services detailed in this document.

Submission details:

Submission should be made via the Turnitin link on the Blackboard.

Assessment Deadline Date and time: **[24/02/2025, at 12:00 noon]**

Please note that this is the final time you can submit – not the time to submit! You should aim to submit your assessment in advance of the deadline. Your feedback and mark for this assessment will be provided within 15 working days.

Note: If you have any valid mitigating circumstances that mean you cannot meet an assessment submission deadline and you wish to request an extension, you will need to apply online, via MyUCLan with your evidence **prior to the deadline**. Further information on Mitigating Circumstances via this link.

We wish you all success in completing your assessment. Read this guidance carefully, and any questions, please discuss with your Module Leader.

Disclaimer: The information provided in this assessment brief is correct at time of publication. In the unlikely event that any changes are deemed necessary, they will be communicated clearly via e-mail and a new version of this assessment brief will be circulated.

Learning Outcomes

[LO1]. Select and use applicable standards and methods for information security and risk management.
[LO3]. Conduct and properly document risk assessment based on a given scenario or area.
[LO4]. Designing and developing a security assurance, governance, and risk management strategy considering and following the stakeholders' requirements.

Assignment Summary:

This assessment requires you to complete all tasks relating to the given scenarios I and II.

- By reflecting on assessment scenario (XYZ-VISA) below , write a report (maximum 2000-words) ,which includes the following:

  A discussion, in the context of cyber-security of the role of security governance and laws appropriate.

  Furthermore, evaluate approaches XYZ-VISA use to protect their business interests and mitigate risk.

- You must draw on XYZ-VISA scenario (see above section for more details) to demonstrate practical applications of hardware and software solutions to secure the XYZ-VISA and its systems, detailing the use of risk assessments, which may include:
  - Maximum of FOUR Assets' identification
  - Valuation of each Asset
  - ONE Threat Identification (per Asset)
  - ONE Vulnerability Identification (per Asset)
  - Determine Risk Likelihood
  - Determine Risk Impact
  - Identify TWO controls
  - Determine TWO post control risks

Scenario I

XYZ-VISA is a VISA application office that is responsible for managing visa application and issue, and its current IT infrastructure is depicted in Figure 1.

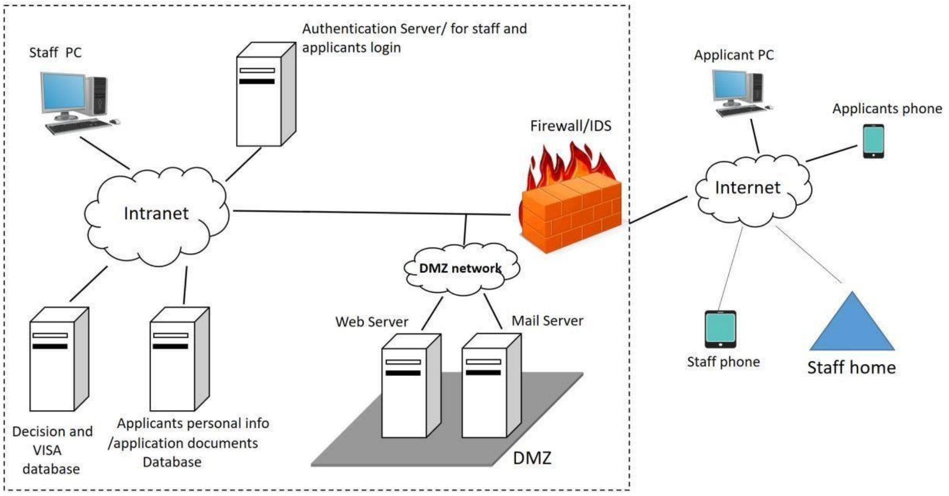
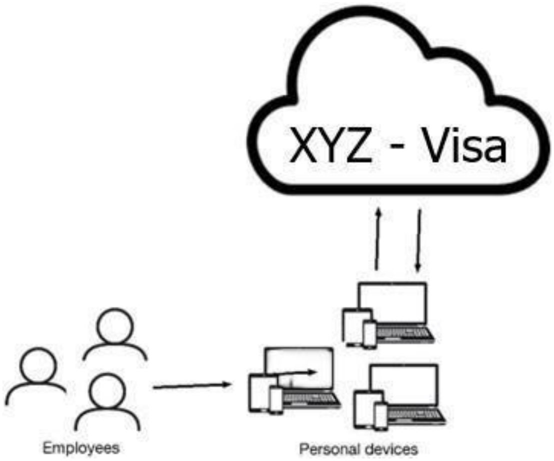

Staff PC
Authentication Server/ for staff and applicants login
Firewall/IDS
Intranet
DMZ network
Web Server
Mail Server
Decision and VISA database
Applicants personal info /application documents Database
DMZ
Applicant PC
Applicants phone
Internet
Staff phone
Staff home

Figure 1. The IT infrastructure of XYZ-VISA

The IT infrastructure comprises of the following.

- Staff PCs running Windows 10. Staff use their PCs to check the application documents and login into their staff accounts to create the decision documents.
- A Microsoft SQL server database engine that stores all information about staff and applications.
- Authentication of both staff and applicants accounts is via a Kerberos service.
- A machine running a Microsoft Exchange Server that stores all emails and attached files.
- A machine running Microsoft Internet Information Service (IIS) web server hosting the website (designed with ASP.NET) of XYZ-VISA. This service is used for hosting the website of XYZ-VISA on which people can browse for application information and apply online, as well as checking their application status/decision.
- For enhanced security, there is a D-Link DIR-878 firewall with firmware 1.12A1 installed to monitor and filter traffic/activity.
- After some attack incidents, the VISA office realized that a risk assessment is required and improve its IT infrastructure with security controls.

Scenario II



After an initial security assessment, it was found that the XYZ-VISA has no bring-your-own-device (BYOD) policy. BYOD practice allows employees of an organization to use their personal devices for work purposes and according to your Security Officer, unrecognised employees' assets were the primary infiltration points. Figure 2 shows some of the BYOD devices accessing the company's resources.

Assessment Tasks

Using the fictitious IT Infrastructure of XYZ-VISA given in Figure 1, write a report including the following:

- Discussion on the context of cyber-security and the roles of security governance. Furthermore, evaluate approaches XYZ-VISA use to protect their business interests and mitigate risk.
- Demonstration of the practical applications of hardware and software solutions to secure the XYZ-VISA and its systems, detailing the use of risk assessments, which may include:
  - Assets’ identification
  - Threat identification per asset
  - Vulnerability identification per asset
  - Finding and discussing recent Common Vulnerabilities and Exposures (CVE) for all previously identified assets.
  - Security control strategies

Employees would like to be able to work with their personal devices and XYZ-VISA wants to allow this. Based on scenario 2 including in your report the following.

  - Identify ONE security control strategy to reduce future risk
  - Elaborate on how you will implement or deploy the strategy in (1)

- What other technologies can help to protect the information to not discontinue BYOD at XYZ-VISA?

The **2000-**words risk assessment report should be submitted as a .docx to the appropriate assignment submission link through Blackboard. All references and in-text citations in the report should follow the Harvard style of referencing.

Marking Scheme

For Grade Bands 70-100 (1st)

- The report has clearly defined sections and the structure is excellent.
- The student has identified at least FOUR weaknesses in the given infrastructure that put the assets at risk.
- The report includes and discusses at least THREE applicable standards that are consistent with laws and regulations.
- Identification and description of at least FOUR assets (logical and physical) and associated threats.
- Identification and description of at least ONE strongly related vulnerability per identified asset.
- Description of at least FOUR known and matching patched or unpatched CVEs alongside the CVE numbers (in MITRE or NVD databases) that pose risks to identified assets.
- Justification for high or low CVSS scores assigned to the identified CVEs.
- Identification and discussion of at least THREE security controls to mitigate the security problems with the infrastructure.
- Identification and excellent description of appropriate security controls for allowing BYOD
- At least FIVE examples of supporting technologies that can add security to BYOD
- All tasks have not exceeded their word limits margins beyond +10%
- At least 10 excellent scientific references are provided, and all listed references are cited.
- The report is written in English with excellent grammar and spelling.

For Grade Bands 60-69 (Upper 2nd)

- The report has mostly clearly defined sections and is well structured.
- The student has identified at least THREE weaknesses in the given infrastructure that put the assets at risk
- The report includes and discusses at least TWO applicable standards that are consistent with laws and regulations.
- Identification and description of at least FOUR assets (logical and physical) and associated threats
- Identification of at least ONE related vulnerability per identified asset.
- Description of TWO known and matching patched or unpatched CVEs alongside the CVE numbers (in MITRE or NVD databases) that pose risks to identified assets.
- Identification and discussion of at least TWO security controls to mitigate the security problems with the infrastructure.
- Identification and a good description of appropriate security controls for allowing BYOD.
- At least THREE examples of supporting technologies that can add security to BYOD.
- All tasks have not exceeded word limits margins beyond +10%
- At least 10 good references are provided, and all listed references are cited.
- The report is written in English with good grammar and spelling.

For Grade Bands 50-59 (Lower 2nd)

- The report has sections, and a reasonable attempt has been made at a cohesive

structure.
- The student has identified at least TWO weaknesses in the given infrastructure that put the assets at risk.
- The report lists standards (but not relevant to the given scenario) that are consistent with laws and regulations.
- Identification of at least THREE assets (logical or physical) and associated threats.
- List of some vulnerabilities partly related to the identified asset.
- List of at least ONE known patched or unpatched CVE with numbers (in MITRE or NVD databases) but not correctly linked to the appropriate assets.
- Identification and discussion of at least TWO security controls to mitigate the security problems with the infrastructure.
- Identification or description of any security controls for allowing BYOD.
- At least ONE example of supporting technologies that can add security to BYOD.
- At least 10 references are provided but some of them are not cited correctly.
- The report is written in English but there could be some grammatical or spelling errors.

For Grade Bands 40-49 (3rd)

- The report is readable and organised.
- The student has identified some weaknesses in the given infrastructure that put the assets at risk.
- The report lists standards (but not relevant to the given scenario) that are mostly consistent with applicable laws and regulations.
- Identification of at least TWO assets (logical or physical).
- A general list of some vulnerabilities is provided.
- List at least ONE known patched or unpatched CVE (in MITRE or NVD databases) but not correctly linked to the appropriate assets.
- Identification and discussion of at least TWO security controls to mitigate the security problems with the infrastructure.
- Identification of security controls for allowing BYOD, the control may be unrelated to the given scenario.
- At least ONE example of supporting technologies that can add security to BYOD.
- Some references are provided.
- The report is written in English but there could be several noticeable grammatical or spelling errors.

For Fail Grade Bands (0-39)

- The report is of poor quality with little link made to the project.
- The student has identified no weaknesses relating to the given infrastructure that put the assets at risk or those provided are not sufficiently detailed to show insight into these scenarios.
- The report lists no legal or regulatory frameworks or standards that are appropriate or lacks explanation in what is discussed in this matter.
- No security controls identified or discussed to mitigate the security problems with the infrastructure.
- No security controls for allowing BYOD provided or all controls supplied are unrelated to the given scenario.
- Only 5 or less relevant references are provided.
- The writing is difficult to follow and is not in an appropriate voice for the audience, with spelling and grammar errors.
- Submissions in this class demonstrate little knowledge of relevant material and the

treatment of topics is superficial, mostly regurgitated, and does not meet the requirements for the 40% pass mark stated above.

For Grade Bands 40-49 (3rd)

- The report is readable and organised.
- The student has identified some weaknesses in the given infrastructure that put the assets at risk.
- The report lists standards (but not relevant to the given scenario) that are mostly consistent with applicable laws and regulations.
- Identification of at least TWO assets (logical or physical).
- A general list of some vulnerabilities is provided.
- List at least ONE known patched or unpatched CVE (in MITRE or NVD databases) but not correctly linked to the appropriate assets.
- Identification and discussion of at least TWO security controls to mitigate the security problems with the infrastructure.
- Identification of security controls for allowing BYOD, the control may be unrelated to the given scenario.
- At least ONE example of supporting technologies that can add security to BYOD.
- Some references are provided.
- The report is written in English but there could be several noticeable grammatical or spelling errors.

For Grade Bands 50-59 (Lower 2nd)

- The report has sections, and a reasonable attempt has been made at a cohesive structure.
- The student has identified at least TWO weaknesses in the given infrastructure that put the assets at risk.
- The report lists standards (but not relevant to the given scenario) that are consistent with laws and regulations.
- Identification of at least THREE assets (logical or physical) and associated threats.
- List of some vulnerabilities partly related to the identified asset.
- List of at least ONE known patched or unpatched CVE with numbers (in MITRE or NVD databases) but not correctly linked to the appropriate assets.
- Identification and discussion of at least TWO security controls to mitigate the security problems with the infrastructure.
- Identification or description of any security controls for allowing BYOD.
- At least ONE example of supporting technologies that can add security to BYOD.
- At least 10 references are provided but some of them are not cited correctly.
- The report is written in English but there could be some grammatical or spelling errors.

Note that the marking will follow the banded grades scheme that is in use across the university. The scheme is reproduced below for your information:

Band	**Numerical equivalent**
Exceptional 1st	100
Very High 1st	94
High	87
Mid 1st	80
Low 1st	74
High 2.1	68
Mid 2.1	65
Low 2.1	62
High 2.2	58
Mid 2.2	55
Low 2.2	52
High 3rd	48
Mid 3rd	45
Low 3rd	42
Marginal Fail	35
Mid Fail	30
Low Fail	25
Fail	10
Non- submission/Penalty/No Academic Merit	0

Additional Support available:

All links are available through the online Student Hub

1. Our **Library resources** link can be found in the library area of the Student Hub or via your subject librarian at SubjectLibrarians@uclan.ac.uk.

2. Support with your academic skills development (academic writing, critical thinking and referencing) is available through **WISER** on the Study Skills section of the Student Hub.

3. For help with Turnitin, see Blackboard and Turnitin Support on the Student Hub

4. If you have a disability, specific learning difficulty, long-term health, or mental health condition, and not yet advised us, or would like to review your support, **Inclusive Support** can assist with reasonable adjustments and support. To find out more, you can visit the Inclusive Support page of the Student Hub.

5. For mental health and wellbeing support, please complete our online referral form, or email wellbeing@uclan.ac.uk. You can also call 01772 893020, attend a drop-in, or visit our UCLan **Wellbeing Service** Student Hub pages for more information.

6. For any other support query, please contact **Student Support** viastudentsupport@uclan.ac.uk.

7. For consideration of Academic Integrity, please refer to detailed guidelines in our policy document . All assessed work should be genuinely your own work, and all resources fully cited.

8. For advice on the use of Artificial Intelligence, please refer to Categories of AI tools guidance. **For this assignment, you are not permitted to use any category of AI tools.**

Preparing for your assignment.

Refer to the Module Information Pack to understand the Learning Outcomes and Marking Criteria.

Ensure that your submission is in MS Word format (.doc or docx)

Make sure you attach the Coursework Cover Sheet to your submission.

Additional criteria:

Late submissions: Except where an extension of the hand-in deadline date has been approved, work that is handed in within 5 working days late will receive a maximum mark of 40%. Work handed in later than this will receive 0%.

Academic Malpractice: The consequences of academic malpractice in assessments are serious. This includes plagiarism, collusion and allowing other students to access your work. This will not be tolerated. Details surrounding the coursework regulations can be found in the University's Academic Regulations.

Extenuating circumstances and extension

Extensions are granted when there are serious and exceptional factors outside your control. Everyday occurrences such as colds and hay fever do not normally qualify for extensions. Where possible, requests for extensions should be made before the hand-in date. Information about how to submit: https://www.uclan.ac.uk/students/support/extensions.php

Unfair Means to Enhance Performance

The University operates an electronic plagiarism detection service (Turnitin) where your work will be automatically uploaded, stored, and cross-referenced against other material. You should be aware that the software searches the World Wide Web, extensive databases of reference material and work submitted by members of the same class to identify duplication.

To avoid accusations of plagiarism, give an in-text citation and provide bibliographic details of any source used in the references list. Remember that you can reuse ideas from different sources but not literal text.

Plagiarism is not acceptable, and you will face consequences when it is detected by Turnitin. For detailed information on the procedures relating to plagiarism, please seethe current version of the University Academic Regulations.

Reassessed Work

Reassessment in written examinations and coursework is at the discretion of the Course Assessment Board and is dealt with strictly in accordance with university policy and procedures. Revision classes for referrals will take place during ’reassessment revision, appeals and guidance week’ as marked on the academic calendar.

The mark for the reassessed module is subject to a maximum of 50%. This is not the case when you got EC approved.

Please see the UCLAN Academic Regulations and Assessment Handbook for information and penalties related to “unfair means to enhance performance.

Feedback Guidance:

Reflecting on Feedback: how to improve.

From the feedback you receive, you should understand:

❑ The grade you achieved.

❑ The best features of your work.

❑ Areas you may not have fully understood.

❑ Areas you are doing well but could develop your understanding.

❑ What you can do to improve in the future - feedforward.

Use the WISER: Academic Skills Development service. WISER can review feedback and help you understand your feedback. You can also use the WISER Feedback Glossary

Next Steps:

❑ List the steps you have taken to respond to previous feedback.

❑ Summarise your achievements

❑ Evaluate where you need to improve here (keep handy for future work):