School of Computer Science and Informatics

Coursework Submission Cover Sheet

Please use Adobe Reader to complete this form. Other applications may cause incompatibility issues.

Student Number

Module Code

Submission Date

Hours spent on this exercise

Special Provision □

(Please place an x in the box above if you have provided appropriate evidence of need to the Disability & Dyslexia Service and have requested this adjustment).

Group Submission

For group submissions, *each member of the group must submit a copy of the coversheet.* Please include the student number of the group member tasked with submitting the assignment.

Student number of submitting group member

By submitting this cover sheet you are confirming that the submission has been checked, and that the submitted files are final and complete.

Declaration

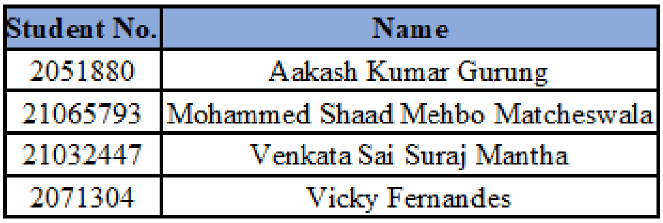
By submitting this cover sheet you are accepting the terms of the following declaration.

I hereby declare that the attached submission (or my contribution to it in the case of group submissions) is all my own work, that it has not previously been submitted for assessment and that I have not knowingly allowed it to be copied by another student. I understand that deceiving or attempting to deceive examiners by passing off the work of another writer, as one's own is plagiarism. I also understand that plagiarising another's work or knowingly allowing another student to plagiarise from my work is against the University regulations and that doing so will result in loss of marks and possible disciplinary proceedings.

Cybersecurity and Risk Management coursework group report

CMT116-1-2071304

REPORT SUBMITTED BY:



Student No.	Name
2051880	Aakash Kumar Gurung
21065793	Mohammed Shaad Mehbo Matcheswala
21032447	Venkata Sai Suraj Mantha
2071304	Vicky Fernandes

Chapter 1: Risk Assessment and risk assessment methodology

Risk assessment: A security risk assessment discovers, analyzes, and implements significant application security measures. It's also very focused with avoiding application security issues and vulnerabilities.(Security Risk Assessment. [no date])

Why do we need risk assessment? It is a decision foundation for any cybersecurity-related work that you will undertake later—starting with the idea up to incident reaction. Therefore, it helps you make educated selections instead of merely following gut impulses. It also decreases the complexity since it summarizes all the crucial components.

There are four steps involved in a risk assessment:

- Preparation: In this phase, the organization selects an assessment team and deploy an assessment plan.
- Understand: It is essential to understand the organization's operations, operating environment, and challenges before assessing.
- Assessment: Assessing the risks by categorizing (threat type, organizations functions), evaluating and grading (green, amber, red)
- Reporting: After the assessment is done, the next step is to draft a risk report, wait for the client to review it, and determine the next steps.

Risk assessment methodology:

The Facilitated Risk Analysis Procedure (FRAP) methodology is considered a relevant security risk analysis for the website. FRAP is a qualitative analysis done using an expert panel (SECURE APPLICATIONS Ltd (here)) to identify risks. The main reasons to consider FRAP as the required methodology are:

- Low cost for assessment: As we can see in the scenario, the firm under consideration is a smaller one that often focuses on limiting risks, providing excellent customer service, and decreasing expenses whenever possible.
- One system/application at a time: As we see in the scenario, they have hired a professional to perform a risk assessment on their application.
- Controls for the indicated threats are identified, and a management summary is provided.
- Assigns (green, amber, red) a simple probability and impacts each threat.(Thomas R.Peltier 2005)

Reasons why other policies are not considered:

- CRAMM: The tool must be used by skilled and trained practitioners. It mainly focuses on the IT hardware industries. (Zeki Yazar [no date])
- EBIOS RM: Security issues are rarely addressed with advice or rapid remedies.

- CORAS: The implementation requires deeper knowledge in various fields, and the effectiveness is not included.
- OCTAVE: It primarily focuses on risk minimization and acceptance rather than risk avoidance. (Wissam Abbass ; Amine Baina ; Mostafa Bellafkih [no date])

Chapter 2: Qualitative Risk Analysis

As discussed in chapter 1, FRAP methodology was selected, and according to FRAP, the risks must be classified in red, amber, and green. Table 1 takes several possibilities that were taken into consideration based on the identification of threats, risks and impact, and the Likelihood:

Threats	**Risks**	**Impact**	**Likelihood**	**Result**: **Impact + Likelihood**
SQL injection	Data modification Data loss Repudiation issues Gaining unauthorized access to the system	High	High	Red
Cross-site scripting	Data theft Malware deployment Users credentials could be stolen Data exfiltration	High	High	Red
Remote code execution	Executing a malware script on the organization, e.g., trojan, worm, virus, etc. Data extraction Data breach Data modification	High	High	Red
Malware	Data corruption Ransomware Data breach Data modification	High	Medium	Red

Insider threats	Upload malware through USB Data leaks Risk to confidential data of the organization	High	High	Red

Table 1: Risk classification

Chapter 3: Risk Handling

1. Data Loss:

Data loss refers to the loss or destruction of vital or personal data kept on a computer or network as a result of an attack or human error. Many assaults, including SQL injection, ransomware, denial of service, and others, might result in data loss in our scenarios.

To protect this data, the organisation must first understand and decide where the data will be stored; cloud storage, databases, and hard drives are a few examples, as is strong encryption of the storage, having an access control list to control who can access the sensitive data based on their roles, and hardening of systems and networks.

2. Insider threats:

Insiders are typically unhappy or former workers who have some level of access to organisational resources and may frequently inflict major harm to a company due to their privileged access, awareness of flaws, and knowledge of lucrative targets. As a result, they often turn to social engineering, threats, or spreading rumours in order to encourage other employees to undermine the organisation and prevent it from conducting business.(Blackwell 2009)

To ensure these do not occur, the company can increase the probability or perception of detection by putting up fake alarms or empty cameras, giving itself security through obscurity. There can be clear policies to ensure that if any employee tries to harm, there will be severe consequences even legal measures will be taken against them.

3. Financial loss:

Financial losses are harmful to an organization's wealth, and this comprises organizational losses such as increased expenses or decreased income as a result of the threat and compensation and legal bills incurred as a result of the threat.

To prevent financial loss, the company needs to have better security measures based on its business model and choose security policies that ensure that the damage to their environment is reduced to the lowest, saving costs of damage and legal costs.

4. Reputational loss:

Reputation losses relate to people's loss of trust and poorer opinion of a corporation as a result of a threat.This might be caused to service unreliability, which makes consumers unwilling to continue doing business, or employee or customer information being stolen and leaked, which causes them to lose faith in the company's capacity to keep and safeguard their data.

The company can employ strong security measures to guarantee that it is not attacked, and if it is, it must be able to recover with little harm. Implementing a zero-trust network design, in which the company trusts no one and allows no one onto the network without prior clearance and access to just desired information, might be a terrific solution.

5. Loss of Availability:

Availability guarantees that users access systems, apps, and data when they need it. The most typical assaults that influence availability are denial-of-service attacks, in which an attacker denies access to information, systems, devices, or other network resources.

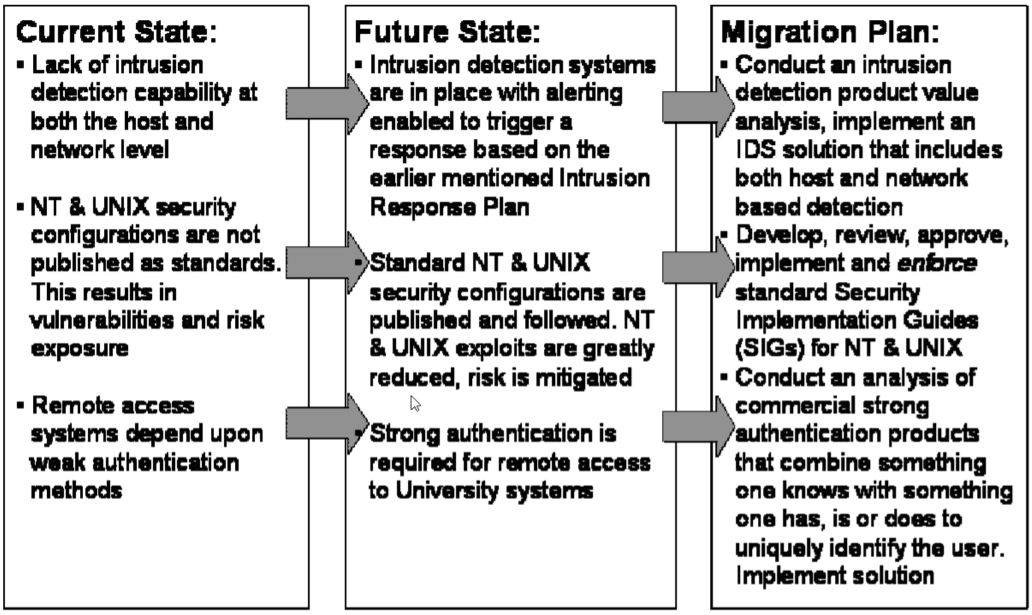
The company may avoid Denial-of-service attacks by developing a DoS response strategy, enhancing network security, restricting network broadcasting, utilizing cloud-based protection, and implementing continuous monitoring.

Chapter 4: Information Security Policy for implementation of risk mitigation strategy

The security policy defines and instructs the organization through a documented set of procedures to handle the potential security risks per the business's risk appetite. Often, organizations tend to make incorrect assumptions that developing a successful information security policy requires a knowledgeable person to compose a document by sitting in a room isolated from the rest of the organization. This approach creates a sense of divide between employees and the security policy as it will lead to great levels of resistance who must abide by the policies defined by the organization (Susan Moore)

The creation of an information security policy undergoes various phases, which can be listed as follows:

1. **Origination Phase**: The organization's security objectives and how these objectives will be met need to be understood. The key deliverables in this phase are the security policy scope document and end-users affected by the security policy.
2. **Gap analysis:** The organization needs to understand its current security posture by conducting employee interviews, documenting its analysis, conducting open discussions with its stakeholders, and utilizing appropriate tools to generate a snapshot of the overall security status. Figure 1 illustrate the gap analysis as follows:



Current State:
- Lack of intrusion detection capability at both the host and network level
- NT & UNIX security configurations are not published as standards. This results in vulnerabilities and risk exposure
- Remote access systems depend upon weak authentication methods

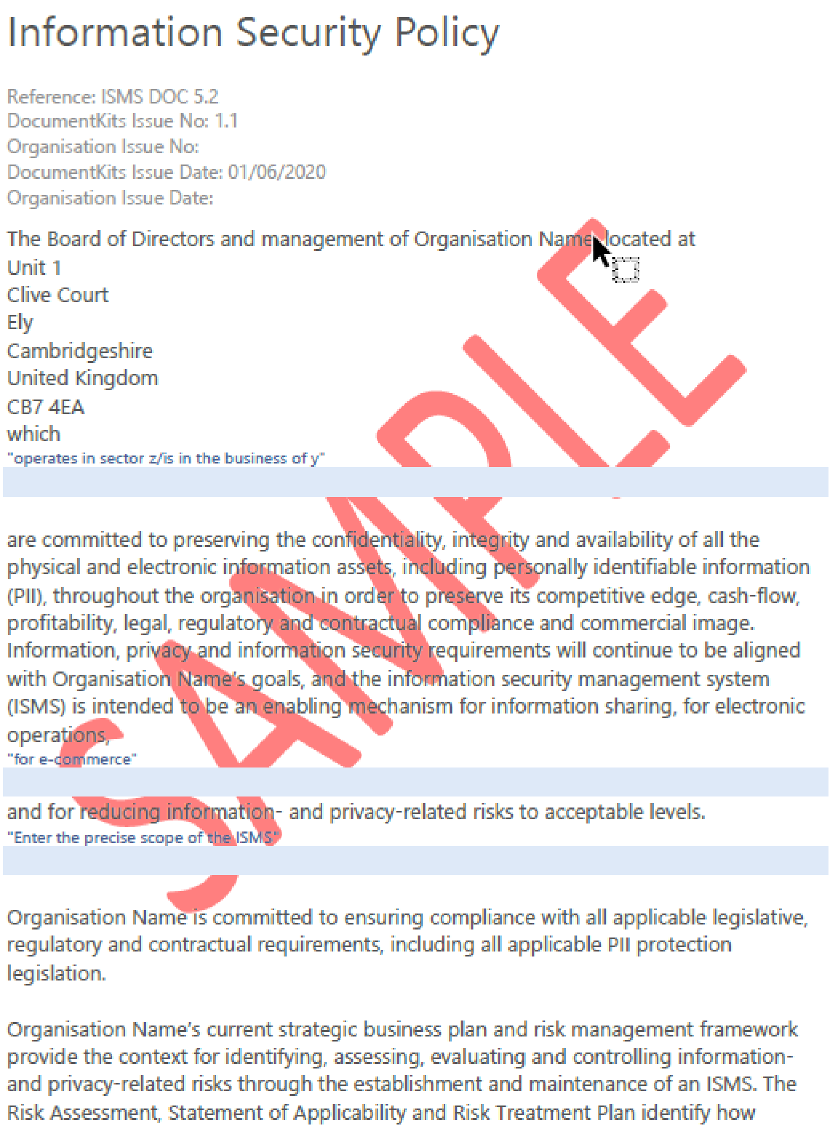
Future State:
- Intrusion detection systems are in place with alerting enabled to trigger a response based on the earlier mentioned Intrusion Response Plan
- Standard NT & UNIX security configurations are published and followed. NT & UNIX exploits are greatly reduced, risk is mitigated
- Strong authentication is required for remote access to University systems

Migration Plan:
- Conduct an intrusion detection product value analysis, implement an IDS solution that includes both host and network based detection
- Develop, review, approve, implement and *enforce* standard Security Implementation Guides (SIGs) for NT & UNIX
- Conduct an analysis of commercial strong authentication products that combine something one knows with something one has, is or does to uniquely identify the user. Implement solution

Figure 1: Gap analysis

3. **Define the security policy:** In this phase, the future state of the organization's security program post-implementation of the security policy will be defined. The policy should be built by taking references from the National Institute of Standards and Technology (NIST) standard, the National Security Agency, the National

Computer Security Centre, and other prominent resources. Figure 2 is an extract from an information security policy sample document:



Information Security Policy

Reference: ISMS DOC 5.2
DocumentKits Issue No: 1.1
Organisation Issue No:
DocumentKits Issue Date: 01/06/2020
Organisation Issue Date:

The Board of Directors and management of Organisation Name located at
Unit 1
Clive Court
Ely
Cambridgeshire
United Kingdom
CB7 4EA
which
"operates in sector z/is in the business of y"

are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets, including personally identifiable information (PII), throughout the organisation in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image. Information, privacy and information security requirements will continue to be aligned with Organisation Name's goals, and the information security management system (ISMS) is intended to be an enabling mechanism for information sharing, for electronic operations,
"for e-commerce"

and for reducing information- and privacy-related risks to acceptable levels.
"Enter the precise scope of the ISMS"

Organisation Name is committed to ensuring compliance with all applicable legislative, regulatory and contractual requirements, including all applicable PII protection legislation.

Organisation Name's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information- and privacy-related risks through the establishment and maintenance of an ISMS. The Risk Assessment, Statement of Applicability and Risk Treatment Plan identify how

Figure 2: Information Security Policy sample template (ISO 27001 Toolkit)

4. **Assign roles and responsibilities**: The policy should define the roles and assign responsibilities to the security team and system users and of system and data owners who process and transmit sensitive information to understand their part in achieving organizational security. Also, the policy should consider the stakeholders who would be affected by this policy. Figure 3 illustrates the information security policy stakeholders:

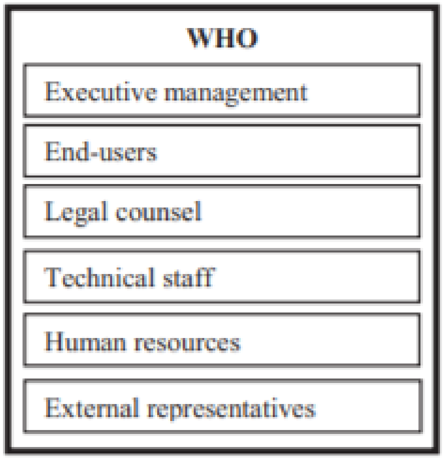


Figure 3: Information Security policy stakeholders (Flowerday and Tuyikeze 2016)

5. **Maintaining the implemented security policy**: After the security policy is implemented, the organization needs to maintain it to ensure that it reflects the overall security posture. Also, the policy should have provisions and change management procedures for making any change requests, evaluating the existing policy, and granting exceptions on a risk-based approach to the implemented policy. (Walton 2002)

Information Security Policy

Overview:

The policy was designed to ensure the confidentiality, integrity, and availability of the organization's data while also raising awareness of the necessity of cybersecurity. This policy also governs the use of authorized technologies, such as email, computing devices, and smartphones, that do not jeopardize the organization's overall security posture.

All personnel on whom this policy is implemented had their opinions taken into account. Furthermore, all workers are fully aware of and understand the obligations of this information security policy.

Acceptable Use:

By complying with this policy, employees agree to do the following:

1. Perform regular anti-virus and anti-malware scans for their systems. Also, users should ensure that they are applying all the available security updates for their operating system to keep their systems up to date with the latest security patches.
2. Use a screen lock or lock their systems when not in use to protect data confidentiality.
3. Run spyware blockers/removers on their systems regularly.

4. Utilize OneDrive as the only file-sharing technology and refrain from other insecure P2P (Peer-to-Peer) file sharing methods.
5. Use of strong passwords for employee accounts.

Unacceptable Use:

Employees should refrain from the following:

1. Use of corporate IT resources such as corporate network or office devices for downloading, creating, storing, and circulation any obscene, abusive, or offensive content as it could be a potential source of malware and could be a violation of the law.
2. Performing unauthorized attempts to access corporate systems that one is not entitled to access.
3. Carrying and plugging in personal storage devices such as USB sticks into the organization's systems.
4. Employees shall refrain from interacting with any suspicious emails and should not click on any links that seem to be malicious.
5. Users shouldn't use any technology or software not pre-installed on corporate devices.

Consequences of Breach:

In the event of any data breach, if any employee discovers the breach, they should immediately report the incident by raising any incident request to their reporting manager. However, if an employee willfully did the breach, then the organization reserves the right to do the following:

1. Restrict or terminate the user's access to the corporate system and network.
2. Withdraw or remove any content that the concerned user publishes.
3. If the breach occurred is of a serious nature that can damage the company's reputation, then the organization shall report the matter to law enforcement agencies for any legal action to be taken. (IT Acceptable Use Policy)

Once the policy is approved, it will include information on the security objectives and guide employees to aid in achieving business, contractual and compliance requirements (Prachi).

Appendix

Minutes of Meeting:

Date: 15th November 2021

Time: 1 hour

Invitees:

- Aakash Kumar Gurung
- Mohammed Shaad Mehboob Matcheswala
- Muzammil Mohammadikb Tirmizi
- Venkata Sai Suraj Mantha
- Vicky Fernandes

Participants Attended:

- Aakash Kumar Gurung
- Mohammed Shaad Mehboob Matcheswala
- Venkata Sai Suraj Mantha
- Muzammil Mohammadikb Tirmizi
- Vicky Fernandes

Discussion points:

- A formal introduction of team members after group formation.
- Reading and understanding of the problem statement for group coursework activity.

Action items:

- All group members agreed to research various risk assessment methodologies and propose at least one methodology that would be unique from the other group members and its advantages and disadvantages.

Date: 22nd November 2021

Time: 3 hours

Invitees:

- Aakash Kumar Gurung
- Mohammed Shaad Mehboob Matcheswala
- Muzammil Mohammadikb Tirmizi
- Venkata Sai Suraj Mantha
- Vicky Fernandes

Participants Attended:

- Aakash Kumar Gurung
- Mohammed Shaad Mehboob Matcheswala
- Venkata Sai Suraj Mantha
- Vicky Fernandes

Discussion points:

- All group members proposed the risk assessment methodology that they have researched.
- Aakash suggested the Octave-S methodology as the company in the given scenario is small.
- Shaad suggested ISO27001 could be the appropriate methodology. However, Vicky argued that it would be difficult to implement ISO27005 for the given organization that mainly functions offline and has only recently decided to start an online book purchasing store.
- Suraj proposed FRAP (Facilitated Risk Analysis Process) methodology since the number of employees in the organization could be minimized, and the policies implemented due to FRAP could be easily implemented.

Action items:

- All group members considered each other's feedback and confirmed the methodology for the coursework in the next meeting.

The team tried to contact Muzammil as he was absent to check whether there were any challenges in attending these sessions. Unfortunately, there was no response from his end.

Date: 28th November 2021

Time: 2 hours

Invitees:

- Aakash Kumar Gurung
- Mohammed Shaad Mehboob Matcheswala
- Muzammil Mohammadikb Tirmizi
- Venkata Sai Suraj Mantha
- Vicky Fernandes

Participants Attended:

- Aakash Kumar Gurung
- Mohammed Shaad Mehboob Matcheswala
- Venkata Sai Suraj Mantha
- Vicky Fernandes

Discussion points:

- Team members finalized that FRAP methodology is to be used for the coursework.
- All members agreed that they needed to perform data collection better to understand the methodology and its application to the scenario.

Action items:

- Read the methodology, documents, and related articles.

Date: 4th December 2021

Time: 3 hours

Invitees:

- Aakash Kumar Gurung
- Mohammed Shaad Mehboob Matches Wala
- Muzammil Mohammadikb Tirmizi
- Venkata Sai Suraj Mantha
- Vicky Fernandes

Participants Attended:

- Aakash Kumar Gurung
- Mohammed Shaad Mehboob Matches Wala
- Venkata Sai Suraj Mantha
- Vicky Fernandes

Discussion points:

- Discussion of concepts of FRAP methodology.
- Coursework was divided into four major sections, and each section was distributed among team members.
- Muzammil was not present for this meeting. However, it was decided that he could work on the risk assessment requirement question to build the pace for the rest of the coursework data. The same was communicated to him as well.

Action items:

- List down various risks, threats as per each group members understanding and presenting in the following meeting.

Date: 17th December 2021

Time: 3 hours

Invitees:

- Aakash Kumar Gurung

- Mohammed Shaad Mehboob Matches Wala
- Muzammil Mohammadikb Tirmizi
- Venkata Sai Suraj Mantha
- Vicky Fernandes

Participants Attended:

- Aakash Kumar Gurung
- Mohammed Shaad Mehboob Matches Wala
- Venkata Sai Suraj Mantha
- Vicky Fernandes

Discussion points:

- Shaad identified that SQL injection, Cross-site scripting (XSS) and remote code execution could be major threats for the organization.
- Suraj and Aakash identified Phishing, Malvertising and Man-in-the-middle attacks as some of the big threats.
- Vicky suggested that DDoS and password attacks can also be applicable.
- Also, the threats and the top risks were identified, and the information security policy was drafted during this session.

Date: 3rd January 2021

Time: 1 hour

Invitees:

- Aakash Kumar Gurung
- Mohammed Shaad Mehboob Matcheswala
- Muzammil Mohammadikb Tirmizi
- Venkata Sai Suraj Mantha
- Vicky Fernandes

Participants Attended:

- Aakash Kumar Gurung
- Mohammed Shaad Mehboob Matcheswala
- Venkata Sai Suraj Mantha
- Vicky Fernandes

Discussion points:

- Status update session to check the ongoing progress of group work.

The team tried contacting Muzammil to check the update from his end but received no response.

Date: 10th January 2021

Time: 2 hours

Invitees:

- Aakash Kumar Gurung
- Mohammed Shaad Mehboob Matcheswala
- Muzammil Mohammadikb Tirmizi
- Venkata Sai Suraj Mantha
- Vicky Fernandes

Participants Attended:

- Aakash Kumar Gurung
- Mohammed Shaad Mehboob Matcheswala
- Venkata Sai Suraj Mantha
- Vicky Fernandes

Discussion points:

- Status update sessions to check the ongoing progress of group work and any challenges during the activity were also discussed.

Date: 14th January 2021

Time: 2 hours

Invitees:

- Aakash Kumar Gurung
- Mohammed Shaad Mehboob Matcheswala
- Muzammil Mohammadikb Tirmizi
- Venkata Sai Suraj Mantha
- Vicky Fernandes

Participants Attended:

- Aakash Kumar Gurung
- Mohammed Shaad Mehboob Matcheswala
- Venkata Sai Suraj Mantha
- Vicky Fernandes

Discussion points:

- Proofreading of the final group activity document was performed.

- Any suggestions given by group members for the final draft were taken into consideration, and the final document was prepared.

Date: 17th January 2021

Time: 3 hours

Invitees:

- Aakash Kumar Gurung
- Mohammed Shaad Mehboob Matcheswala
- Muzammil Mohammadikb Tirmizi
- Venkata Sai Suraj Mantha
- Vicky Fernandes

Participants Attended:

- Aakash Kumar Gurung
- Mohammed Shaad Mehboob Matcheswala
- Venkata Sai Suraj Mantha
- Vicky Fernandes

Discussion points:

- Final editing of the document.
- Submission of the final group coursework report on Learning Central.

References:

Blackwell, C. 2009. *The insider threat combatting the enemy within*. 1st ed. Ely, U.K:IT Governance Pub.

Flowerday, S. v. and Tuyikeze, T. 2016. Information security policy development and implementation: The what, how and who. *Computers & Security* 61, pp. 169–183. doi: 10.1016/j.cose.2016.06.002.

ISO 27001 Toolkit. [no date]. Available at: https://www.itgovernance.co.uk/shop/product/iso-27001-toolkit [Accessed: 18 January 2022].

IT Acceptable Use Policy. [no date]. Available at: https://www.bath.ac.uk/corporate-information/it-acceptable-use-policy/ [Accessed: 18 January 2022].

Prachi [no date]. Design Information Security Policies the Right Way. Available at: https://www.bizzsecure.com/design-information-security-policies-the-right-way/ [Accessed: 18 January 2022].

Security Risk Assessment. [no date]. Available at: https://www.synopsys.com/glossary/what-is-security-risk-assessment.html#:~:text=A%20security%20risk%20assessment%20identifies%2C%20assesses%2C%20and%20implements,view%20the%20application%20portfolio%20holistically%E2%80%94from%20an%20attacker%E2%80%99s%20perspective. [Accessed: 10 January 2022].

Susan Moore [no date]. Mitigate Risk with an Effective Security Policy. Available at: https://www.gartner.com/smarterwithgartner/mitigate-risk-with-an-effective-security-policy [Accessed: 18 January 2022].

Thomas R.Peltier 2005. *Information Security Risk Analysis*. Second. Auerbach Publications.

Walton, J.P. 2002. Developing an enterprise information security policy. In: *Proceedings of the 30th annual ACM SIGUCCS conference on User services - SIGUCCS '02*. New York, New York, USA: ACM Press, pp. 153–156. doi: 10.1145/588646.588678.

Wissam Abbass ; Amine Baina ; Mostafa Bellafkih [no date]. Using EBIOS for risk management in critical information infrastructure. In: *2015 5th World Congress on Information and Communication Technologies (WICT)*. Morocco: IEEE. Available at: https://ieeexplore.ieee.org/abstract/document/7489654?casa_token=H3okqKC5IOAAAAAA:3zvNTWUzprJgHuAlo8SqhBF8nls3esd1-nMZp5ddaQ6uoRT3HAoj58dheuYjPMgBV6IsK7c [Accessed: 18 January 2022].

Zeki Yazar [no date]. A Qualitative Risk Analysis and Management Tool - CRAMM. *SANS WhitePaper* . Available at: https://www.sans.org/white-papers/83/ [Accessed: 14 January 2022].