End of Project Report

‘Evaluate Incident Response Plan’

Contents

1. Overview 3

1.1 Summarise IRP 3

2. Blue team strategy 5

2.1 Discuss, evaluate, and outline blue-teaming strategy 5

2.2 Incident/event identification results summarised 7

2.3 Review of effectiveness of communications between cyber analyst and SOC shift supervisor. 9

2.4 Review of effectiveness of communications between SOC shift supervisor and SOC manager. 11

3. Red team strategy 12

3.1 Discuss, evaluate, and outline red-teaming strategy 12

4. Lessons Learnt 14

4.1 What went right 14

4.2 What went wrong 15

4.3 Recommended improvements 17

5. Review and Evaluate 19

5.1 Suggestions on Vendor Products to monitor Risk 214

--

1. Overview

1.1 Summarise IRP

Gelos Enterprises' Incident Response Plan (IRP) for a data breach was initiated when network disruptions were promptly identified by **Fernando Remi**, who reported the issue to his manager, **Chris Smith**. **Lee Dowling**, the Security Administrator, swiftly investigated and verified the likelihood of a breach. Dowling collaborated with **Lucas Isaaks** and the IT Security Team, engaging **Data Trust** to conduct a comprehensive security audit aimed at assessing the breach, identifying vulnerabilities, and determining its root causes.

To further evaluate the organisation's security posture, a **red team assessment** was conducted. This team of cybersecurity specialists employed tools and techniques such as **Zap**, **Hydra**, **Nikto**, **spidering**, and **SQL injection testing**. They also used **Linpeas** for privilege escalation analysis, successfully identifying system weaknesses and exploitable vulnerabilities.

Simultaneously, the **blue team**—responsible for defending and monitoring the network—utilised tools such as **Splunk**, and **Wireshark** to observe red team activities and reinforce the system's defensive measures. Their focus was on strengthening patches, configurations, and controls to prevent further breaches.

Following the identification of vulnerabilities and associated risks, the **IT Security Team**, in partnership with Data Trust, implemented mitigation strategies to minimise the breach's impact and secure the network. These actions included patching outdated systems, updating software, and enhancing overall security configurations.

Throughout the incident response process, detailed documentation was maintained to record all actions, findings, and lessons learned. This documentation now serves as a vital reference for future incidents and contributes to the ongoing improvement of **Gelos Enterprises' cybersecurity framework**.

Planned **enhancements to the Incident Response Plan (IRP)** focus on improving incident detection, communication and collaboration, regular testing and updates, technical capabilities, cross-team coordination, and staff training.

Enhancing incident detection requires implementing advanced monitoring systems and leveraging threat intelligence for real-time alerts. Proactive network traffic and system log monitoring, coupled with intrusion detection and prevention systems, will ensure rapid identification and containment of threats—reducing response times and minimising potential damage.

Streamlining communication and collaboration is equally critical. Clear communication protocols must be established between teams, stakeholders, and departments. A centralised incident management platform should support real-time collaboration, task tracking, and escalation workflows. Regular coordination meetings and structured information-sharing practices will further enhance response efficiency.

Lastly, **strengthening technical capabilities and resources** is essential to an effective response. Equipping the team with robust hardware, software tools, and cybersecurity platforms enables more accurate simulations and analyses. Adequate allocation of virtualised resources ensures realistic testing environments and improves the organisation's readiness to manage complex incidents.

Ongoing refinement and continuous improvement of the Incident Response Plan (IRP) are essential to maintaining its effectiveness. Treating the IRP as a dynamic, living document enables timely adjustments in response to evolving threats and organizational changes. Regular reviews and updates should integrate insights from team members, stakeholders, and external evaluations. Conducting periodic tabletop exercises and simulations ensures that the IRP is rigorously tested, validated, and remains aligned with current best practices.

Employee training is a cornerstone of effective incident response. Comprehensive education on incident procedures, security best practices, and threat awareness empowers staff to play an active role in identifying, reporting, and mitigating potential incidents. Consistent training sessions, interactive workshops, and awareness initiatives help cultivate a security-conscious culture across the organisation. By keeping employees informed about emerging threats, the organisation strengthens its overall response capability.

Together, these initiatives enhance incident detection, communication, collaboration, and technical readiness—while fostering a proactive and resilient incident response culture.

2. Blue team strategy

2.1 Discuss, evaluate, and outline blue-teaming strategy

Strategy 1 – Continuous Monitoring

Discussion: The blue team employs continuous monitoring to collect and analyse data from multiple sources, including network devices, systems, applications, and user activities. Tools such as Splunk and Wireshark are utilised to actively monitor network traffic and identify unusual behaviour. This proactive surveillance enables early detection of suspicious or abnormal activity that may indicate a security incident in progress.

Evaluation: Continuous monitoring is fundamental to maintaining strong cybersecurity resilience. It allows organisations to remain vigilant and identify potential threats in real time. By constantly observing system behaviour and traffic patterns, the blue team can quickly detect anomalies, respond to threats, and reduce the impact of potential incidents.

Outline: The monitoring process should include the implementation of reliable tools and technologies that capture and analyse network traffic, system logs, and user activities. The blue team must establish clear monitoring protocols, define indicators of compromise or suspicious behaviour, and set alert thresholds. Regular reports and automated notifications should be generated to ensure swift awareness and response to potential threats.

Strategy 2 – Incident Detection and Response

Discussion: The blue team develops and implements robust incident detection and response mechanisms to identify, contain, and mitigate security incidents efficiently. Technologies such as Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM) platforms, and Endpoint Detection and Response (EDR) solutions are leveraged to detect anomalies and suspicious patterns. Tools like Splunk, and Wireshark are employed to analyse network traffic and pinpoint potential attack vectors.

Evaluation: Incident detection and response form a cornerstone of an effective blue-team strategy. By using advanced detection tools and structured response workflows, the blue team can identify security incidents quickly and execute targeted containment measures. This reduces the window of exposure and minimises the impact on organisational data and systems.

Outline: The blue team should establish well-defined procedures for incident detection, escalation, and resolution. This includes proper deployment and configuration of detection tools, clearly defined response workflows, and designated team roles. Communication channels for incident reporting and escalation must be maintained, and regular drills or tabletop exercises should be conducted to ensure preparedness for diverse security scenarios.

Strategy 3 – Threat Hunting

Discussion: The blue team engages in proactive threat hunting to uncover signs of compromise or advanced persistent threats (APTs) within the organisation's systems. By leveraging threat intelligence, security logs, and behavioural analytics, they proactively search for indicators of compromise (IOCs) or patterns that suggest undetected intrusions. During the Gelos Enterprises exercise, the blue team conducted active network scans using Wireshark, Nessus, Nikto, and Zap to identify potential vulnerabilities.

Evaluation: Threat hunting is an invaluable practice that exposes sophisticated risks often missed by traditional security measures. By investigating subtle anomalies and indicators of compromise, the blue team can detect and neutralise threats before they escalate into significant incidents, thus improving the organisation's resilience.

Outline: A formal threat hunting framework should be developed, specifying the tools, data sources, and methodologies to be used. Hunting objectives must be prioritised based on risk level and organisational context. The process should include structured data collection, correlation, and analysis. Collaboration with other teams—particularly those focused on threat intelligence and incident response—is essential to ensure effective detection and knowledge sharing.

Strategy 4 – Security Architecture Review

Discussion: The blue team performs regular reviews of the organisation's security architecture, including its network infrastructure, access control systems, and policy frameworks. These evaluations help identify gaps, misconfigurations, or inefficiencies within the existing security controls and ensure that defences remain aligned with best practices.

Evaluation: Comprehensive security architecture reviews are critical to maintaining a robust and adaptive defence posture. By identifying vulnerabilities and areas for optimisation, the blue team helps the organisation strengthen its foundational security and enhance overall resilience against evolving cyber threats.

Outline: Periodic architecture assessments should cover all key areas, including network design, authentication mechanisms, encryption standards, and access control policies. Findings should be documented and prioritised, with actionable recommendations provided to stakeholders. Collaboration between IT, operations, and security teams is essential to ensure that improvements are effectively implemented and fully integrated into the organisation’s infrastructure.

Strategy 5 – Collaboration with Red Teams

Discussion: The blue team works closely with the red team, which simulates real-world attacks to test and challenge the organisation’s defences. This collaboration provides deep insights into potential attack vectors, enabling the blue team to identify weaknesses and improve its detection and response strategies. Through red team exercises, both teams contribute to building a comprehensive understanding of the organisation’s threat landscape.

Evaluation: Red team collaboration is vital to enhancing collective security maturity. It enables both teams to evaluate defensive effectiveness, identify weaknesses, and develop stronger, more adaptive countermeasures. This partnership promotes a culture of continuous learning and improvement across security functions.

Outline: The blue team should establish structured channels of communication and collaboration with the red team. Joint exercises—such as red team–blue team simulations—should be conducted regularly to test defences, assess detection capabilities, and identify improvement areas. Following each exercise, both teams should conduct debriefs to share findings, document lessons learned, and implement remediation measures to strengthen organisational resilience.

2.2 Incident/event identification results summarised

Incident number	Incident type	Description of the Threat
1	Access Control Breach	The presence of username and password hints within the **robots.txt** file suggests a possible lapse in access control protocols, increasing the risk of unauthorised access or disclosure of sensitive information.

2	Weak Password	The use of the password **“Password1!”** on the Blackbox host represents a significant security vulnerability, as it is easily guessable and susceptible to compromise. To strengthen system security, it is essential to implement robust password management practices—such as enforcing complex password requirements, promoting unique credentials, and adopting regular password rotation policies.
3	Privilege Escalation	The incorrect configuration of the **SUID permission** on the Nano editor introduces a **privilege escalation vulnerability**, potentially enabling unauthorised users to obtain elevated system privileges. Implementing robust configuration management controls—such as regular permission audits, least-privilege enforcement, and secure baseline configurations—is essential to prevent unauthorised access and maintain system integrity.
4	Security Risks from Underutilised HTTP Service	The existence of an **underutilised HTTP service**, combined with the exposure of the **robots.txt** file, introduces potential security vulnerabilities. To mitigate these risks, all active and inactive services should be securely configured, routinely reviewed, and continuously monitored to reduce the attack surface and prevent unauthorised access.
5	Outdated Operating System and Application Patches	The use of **unsupported Windows and Linux versions** highlights inadequate patching and maintenance practices, leaving systems exposed to known vulnerabilities. Implementing a **comprehensive patch management process**—including regular system updates, version control, and vulnerability assessments—is critical to maintaining security compliance and safeguarding against exploitable threats.
6	Bind Shell Backdoor Detection	The detection of a Bind Shell Backdoor indicates a potential system compromise, suggesting unauthorised access and control. Robust malware and backdoor detection measures are essential to quickly identify and neutralise such threats.

7	Data Disclosure	The exposure of NFS Exported Share information poses risks to data privacy and confidentiality. Enforcing strict access controls and secure configuration settings is essential to prevent unauthorised access or data leaks.
8	Weak Authentication	The use of a VNC Server with the password set as ‘password’ reflects poor authentication practices, leaving the system vulnerable to unauthorised access. Implementing strong authentication measures, including complex passwords and multi-factor authentication, is critical to improving system security.
9	Application-Level Vulnerabilities	The detection of an SQL injection vulnerability in phpMyAdmin, along with weaknesses in the Debian OpenSSH/SSL random number generator, underscores the importance of effective vulnerability management. Regular scanning and timely patching are essential to address application-level flaws and reduce the risk of exploitation.

2.3 Review of effectiveness of communications between cyber analyst and SOC shift supervisor.

A comprehensive review was conducted to assess the communication effectiveness between the cyber analyst and the SOC shift supervisor within the blue team. The objective of this assessment was to enhance incident response efficiency and strengthen collaboration across the security team. The following key findings were identified:

• **Clarity and Timeliness:** Communication between the cyber analyst and SOC shift supervisor was consistently clear, accurate, and timely. Both parties effectively exchanged information, ensuring that critical details were understood without delay. This high level of clarity supported rapid decision-making and enabled the team to respond efficiently to evolving incidents.

• **Incident Reporting and Escalation:** A structured process for incident reporting and escalation was observed within the SOC. The cyber analyst promptly reported incidents to the shift supervisor in accordance with established procedures. Clearly defined escalation criteria ensured that critical incidents were addressed by the appropriate personnel or management teams, minimising potential impact and mitigating risks in a timely manner.

- **Information Sharing:** Information sharing between the cyber analyst and SOC shift supervisor was efficient and continuous. Both individuals maintained open communication regarding incidents, threat intelligence, and operational updates. This consistent exchange of information improved situational awareness, supported coordinated response efforts, and strengthened the team's understanding of the security environment.

- **Documentation and Knowledge Transfer:** The review found that documentation practices were thorough and well-organised. Details of incidents, response actions, and lessons learned were carefully recorded and distributed within the team. This disciplined approach to documentation promoted consistency, enabled effective knowledge transfer, and allowed the team to build upon previous experiences to improve incident response capability.

- **Collaboration and Feedback:** A strong culture of collaboration and constructive feedback was evident between the cyber analyst and SOC shift supervisor. Both parties engaged actively in discussions, shared insights, and sought input from one another. This proactive feedback loop fostered teamwork, encouraged continuous improvement, and contributed to refining incident response strategies and procedures.

- **Tools and Technologies:** The cyber analyst and SOC shift supervisor effectively utilised available communication platforms, incident management systems, and supporting technologies. These tools streamlined workflows, enhanced the speed and accuracy of information exchange, and contributed to overall operational efficiency within the SOC.

In conclusion, the review confirmed that communication between the cyber analyst and SOC shift supervisor within the blue team was effective in supporting incident response and collaboration. Ongoing evaluation and process optimisation are recommended to further strengthen communication practices, ensuring continued operational excellence and improved security outcomes.

2.4 Review of effectiveness of communications between SOC shift supervisor and SOC manager.

An in-depth assessment was conducted to evaluate the effectiveness of communication between the SOC shift supervisor and SOC manager within the blue team. The objective was to ensure seamless collaboration, streamlined incident response, and effective coordination between these critical roles. The following key findings were identified:

• **Clarity and Promptness:** Communication between the SOC shift supervisor and SOC manager demonstrated a high standard of clarity and timeliness. Information was conveyed accurately and efficiently, ensuring a shared understanding of critical details. This clarity supported rapid decision-making and enabled the team to respond effectively to emerging incidents and operational demands.

• **Reporting and Updates:** A robust reporting and update process was observed between the SOC shift supervisor and SOC manager. Regular, detailed updates on ongoing incidents, operational activities, and emerging threats were communicated promptly. This ensured comprehensive situational awareness and enabled the SOC manager to make informed, timely decisions based on current intelligence.

• **Incident Escalation:** The assessment confirmed a well-defined and efficient incident escalation framework. High-priority incidents were promptly escalated to the SOC manager for further analysis and decision-making. This structured approach ensured that appropriate resources were deployed swiftly, reducing potential impact and effectively mitigating associated risks.

• **Strategic Alignment:** The communication between the SOC shift supervisor and SOC manager reflected strong alignment with organisational goals and strategic priorities. The SOC manager effectively communicated overarching objectives and provided strategic direction, while the shift supervisor reported on operational execution and incident response performance. This alignment ensured that team operations were in sync with broader organisational objectives, enhancing both efficiency and effectiveness across security operations.

• **Feedback and Guidance:** A consistent exchange of feedback and professional guidance was observed between the SOC shift supervisor and SOC manager. Constructive feedback from the SOC manager supported continuous learning and development, while insights from the shift supervisor informed operational improvements. This two-way feedback loop fostered collaboration, strengthened team performance, and reinforced adherence to best practices.

- **Documentation and Reporting:** The review highlighted strong documentation and reporting standards. Incident reports, performance metrics, and key indicators were thoroughly recorded, reviewed, and shared. This practice provided valuable insights into operational performance, ensured accountability, and served as a reliable reference point for future analysis and decision-making.

In conclusion, the assessment confirmed that communication between the SOC shift supervisor and SOC manager within the blue team was highly effective in supporting operational efficiency, collaboration, and incident response readiness. Clear communication, timely reporting, structured escalation, and constructive feedback contributed to a cohesive and capable security function. Ongoing evaluations and continuous process improvements are recommended to further enhance communication practices and maintain peak operational performance.

-

3. Red team strategy

3.1 Discuss, evaluate, and outline red-teaming strategy

Strategy 1: Reconnaissance and Information Gathering

Discussion**:** The red team conducts reconnaissance activities to collect detailed information about the target organisation. This process involves methods such as open-source intelligence (OSINT) collection, network scanning, and social engineering strategies. The primary aim is to uncover potential vulnerabilities and weaknesses within the organisation's systems, infrastructure, and processes. Tools including Zap, Hydra, Nikto, spidering, and SQLi have been employed to perform comprehensive network scanning and information gathering.

Evaluation**:** Reconnaissance plays an essential role in red teaming by offering critical insights into an organisation's attack surface and exposing possible points of entry for threat actors. Through extensive reconnaissance, red teams are able to replicate realistic adversarial behaviour, evaluate existing security measures, and determine how effectively the organisation can detect and respond to potential attacks.

Outline**:** Red teams should employ a diverse range of reconnaissance tools and techniques—such as Nmap for network scanning, online intelligence gathering, and social engineering exercises. Information should be collected on the organisation's systems, infrastructure, personnel, and any publicly accessible data sources. These insights must then be documented and used to guide and refine subsequent attack simulations.

Strategy 2: Exploitation and Attack Simulation

Discussion: The red team performs simulated cyberattacks to assess the organisation's security defences and uncover potential vulnerabilities. This process involves exploiting weaknesses across systems, applications, and human behaviour to test how easily unauthorised access could be obtained or assets compromised. Tools such as Zap, Hydra, Nikto, spidering, SQLi, and Linpeas have been employed to conduct exploitation and attack simulations effectively.

Evaluation: Attack simulations enable red teams to measure the organisation's capability to detect, respond to, and recover from various attack scenarios. By replicating real-world threats, these exercises help expose hidden vulnerabilities and evaluate the overall strength and responsiveness of existing security measures and incident response mechanisms.

Outline: Red teams should apply a range of attack methodologies, including penetration testing and dictionary attacks, to create authentic and controlled simulations. Each step of the process—tools used, techniques applied, and payloads deployed—should be thoroughly documented. The objective is to highlight weaknesses, validate existing controls, and deliver actionable recommendations to enhance the organisation's overall security posture.

Strategy 3: Post-Exploitation and Lateral Movement

Discussion: Once initial access is obtained, red teams conduct post-exploitation exercises to evaluate the organisation's capacity to detect and respond to advanced persistent threats (APTs). These simulations involve lateral movement across the network, privilege escalation, and attempts to access or extract sensitive data and critical systems, mirroring the actions of sophisticated threat actors.

Evaluation: Post-exploitation simulations enable red teams to assess how effectively an organisation can identify and contain complex attacks that rely on sustained access and stealthy movement within systems. By uncovering gaps in monitoring, access management, and detection mechanisms, red teams provide valuable insights that strengthen the organisation's resilience against Advanced Persistent Threats.

Outline: Red teams should replicate key post-exploitation behaviours, including privilege escalation, data exfiltration, and lateral traversal between networked systems. The aim is to expose weaknesses in the organisation's defensive posture and pinpoint opportunities to enhance detection accuracy, response speed, and overall security readiness.

Strategy 4: Reporting and Recommendations

Discussion: Red teams compile comprehensive reports detailing their findings, identified vulnerabilities, and strategic recommendations to strengthen the organisation's overall security posture. These reports serve as a vital resource for stakeholders to understand system weaknesses uncovered during the red team engagement and to guide remediation planning. All relevant findings derived from tools such as Zap, Hydra, Nikto, spidering, SQLi, and Linpeas should be clearly documented within the report.

Evaluation: High-quality red team reporting is essential for driving meaningful security enhancements. Effective reports should present vulnerabilities in a clear and structured manner, explain their potential business and operational impacts, and outline actionable recommendations for risk mitigation and control improvement.

Outline: Red team reports should deliver a thorough summary of exploited vulnerabilities, detailing their origins, contributing factors, and overall implications for the organisation. Recommendations must be prioritised according to the severity of identified risks and include practical, evidence-based remediation steps. Reports should be disseminated to key stakeholders—including the blue team and senior management—to facilitate informed decision-making and ensure timely implementation of security improvements.

4. Lessons Learnt

4.1 What went right

What team did right in the context of the exercise.	
Action 1	Thorough Analysis and Investigation The Data Trust team demonstrated an outstanding approach through their detailed examination and investigation of the cybersecurity breach at Gelos Enterprises. They carried out an extensive analysis to

	determine the extent and impact of the breach, with focused attention on the potential exposure of highly sensitive customer information. This rigorous investigation allowed the team to gain a deeper understanding of the incident and its broader implications.
Action 2	Engaging with Red Team and Blue Team Recognising the importance of integrating both offensive and defensive approaches, the Data Trust team actively promoted collaboration between the red and blue teams throughout the exercise. The red team was tasked with conducting penetration tests, while the blue team focused on monitoring, detecting, and defending against simulated attacks. This cooperative setup created a realistic testing environment to assess Gelos Enterprises' incident response capabilities, ultimately enhancing the depth and accuracy of the overall incident response evaluation.
Action 3	Proactive Incident Response Planning The Data Trust team demonstrated a highly proactive approach to incident response planning throughout the exercise. With clearly defined and well-documented response procedures, actions, and workflows in place, they were able to react quickly and effectively to the simulated cybersecurity incident. Their strong preparation ensured that all response activities were carried out in a coordinated and systematic way, reducing confusion and enhancing the team's capacity to contain and mitigate the potential impact of the incident.

4.2 What went wrong

3 issues/problems, or actions that did not go as planned.

Issue/ Problem 1	<u>Insufficient RAM for Virtualization and Limited Access to Tools</u> The Data Trust team faced several challenges during the incident response exercise, primarily due to inadequate RAM for virtualization and restricted access to key tools. Since virtualization is essential for creating isolated environments used in analysis and investigation, these limitations impeded the team's ability to perform tasks efficiently. The lack of sufficient RAM particularly affected their capacity to execute virtualization processes effectively, which may have reduced the speed and accuracy of their breach analysis and containment efforts. To overcome these limitations, the Data Trust team should prioritise increasing available RAM resources to better support virtualization during incident response operations. Collaboration with Gelos Enterprises' IT or infrastructure department is recommended to evaluate current system capabilities and implement necessary upgrades to enhance overall performance and response effectiveness.
Issue/ Problem 2	<u>Communication Challenges and Impromptu Meetings</u> The Data Trust team experienced communication difficulties during the incident response exercise, particularly due to impromptu meetings that disrupted effective coordination and information flow. Unplanned or ad hoc meetings often result in reduced participation and unclear communication, which can delay crucial decision-making and hinder timely response actions. To mitigate these challenges, the Data Trust team should adopt a more structured communication framework that includes scheduled and well-planned meetings. Establishing regular team meetings will help

	ensure consistent participation from all key members, promote collaboration, and enable efficient exchange of information. Additionally, maintaining thorough documentation of meeting discussions, decisions, and action points will support accountability and streamline future response efforts.
Issue/ Problem 3	Lack of Employee Awareness and Training The scenario indicates that Fernando Remi reported a network access issue to his manager, who subsequently directed him to contact Lee Dowling, the Security Administrator. This sequence of actions highlights a potential gap in employee awareness and training concerning cybersecurity incidents and the correct reporting channels. To mitigate this issue, the Data Trust team should place greater emphasis on employee education and training initiatives. Regular cybersecurity awareness sessions should be implemented to inform staff about common cyber threats, phishing scams, and the importance of promptly reporting any suspicious activity or security incidents.

4.3 Recommended improvements

3 recommendations to improve the effectiveness of the IRTx	
Improvement 1	Enhance Technical Capabilities and Resources: Ensure that the Data Trust team is equipped with adequate technical resources and capabilities to effectively carry out the IRTx. This should include sufficient RAM for virtualization, upgraded hardware and software systems, and access to

	essential cybersecurity tools and platforms. Strengthening technical capabilities will enable the team to simulate realistic scenarios, conduct thorough incident analyses, and accurately evaluate the organisation’s response effectiveness.
Improvement 2	Foster Cross-Team Collaboration and Communication: Highlight the critical role of collaboration and communication within the Data Trust team and among all stakeholders involved in the IRTx. Regular meetings—both scheduled and impromptu—should be encouraged to share insights, review findings, and coordinate response strategies. Implementing a centralized incident communication platform will support real-time information sharing, task management, and documentation. Strengthening cross-team collaboration and communication ensures smooth coordination and enhances the overall effectiveness of the IRTx.
Improvement 3	Continuously Improve and Update the Incident Response Plan (IRP): The IRP should be maintained as a dynamic, evolving document that adapts to the organisation’s changing needs and the ever-shifting threat landscape. It should be reviewed and updated regularly to reflect lessons learned from the IRTx and real-world security incidents. Feedback from team members, stakeholders, and external audits or assessments should be integrated to strengthen its effectiveness. Periodic tabletop exercises and simulations should also be conducted to validate and test the IRP, ensuring it remains responsive and prepared to address emerging threats and

	challenges.

5. Review and Evaluate

The following section outlines the review and assessment of the risk management strategies implemented throughout the cyber exercise project. The aim of this evaluation is to determine the effectiveness of the risk mitigation measures and monitoring processes used to manage identified risks. The review specifically examines key risk areas, including limited stakeholder availability, resource constraints, ineffective communication, inadequate documentation, technical challenges, data loss or corruption, and insufficient time allocation or delayed delivery.

1. Lack/Insufficient Stakeholder Availability:

   Risk Mitigation: A stakeholder engagement plan was established to clearly define roles, responsibilities, and communication pathways. Early engagement of key stakeholders helped align schedules and priorities, while stakeholder management tools were employed to track availability and identify potential scheduling conflicts. Regular reviews and updates were conducted using real-time data to ensure effective coordination.

   Risk Monitoring: Stakeholder availability was continuously monitored throughout the cyber exercise, with open communication channels maintained to quickly resolve any conflicts or availability issues that arose.

2. Insufficient Resources:

   Risk Mitigation: A thorough resource assessment was carried out to identify the necessary equipment, tools, personnel, and budget requirements. Resources were allocated based on identified needs, with contingency plans established to address potential shortfalls. Resource management software was utilized to monitor allocation and availability, while regular evaluations were conducted to identify any gaps or constraints.

   Risk Monitoring: Resource adequacy and availability were continuously monitored, with budget utilization tracked to prevent shortages. A structured feedback mechanism was implemented to identify areas for improvement and address emerging resource constraints.

3. Ineffective Communication:

Risk Mitigation: Clear communication protocols and channels were established to ensure consistent information flow. Team members received training on effective communication techniques and the use of relevant tools. A culture of openness, active listening, and constructive feedback was promoted to strengthen collaboration. Real-time communication and collaboration platforms were utilized, supported by project management tools that enabled communication tracking and reporting.

Risk Monitoring: The effectiveness of communication channels was continuously assessed, with any issues or breakdowns promptly addressed. Regular feedback from team members and stakeholders was encouraged to identify gaps and drive ongoing improvements in communication practices.

4. Insufficient Documentation:

   Risk Mitigation: Standardized documentation templates and guidelines were developed to ensure consistency and clarity. Clear responsibility for documentation was assigned, supported by an established review and approval process. Documentation management systems were employed to organize and maintain records, while version control mechanisms were implemented to track updates and prevent data inconsistencies.

   Risk Monitoring: Documentation practices were routinely reviewed to ensure compliance with established standards. Regular audits were conducted to verify accuracy, completeness, and quality. Additionally, a knowledge management system was introduced to enhance information accessibility and support effective knowledge sharing across the team.

5. Technical Issues:

   Risk Mitigation: Comprehensive testing and validation of all systems, tools, and infrastructure were carried out prior to the cyber exercise to ensure operational reliability. Backup and recovery protocols were established, supported by a clear response plan for managing technical issues. Monitoring and alerting tools were utilized to detect anomalies, and regular system audits were performed to maintain performance integrity.

   Risk Monitoring: System performance and infrastructure stability were continuously monitored throughout the exercise. Incident tracking and resolution processes were implemented to promptly identify, document, and address any technical issues that arose.

6. Data Loss or Corruption:

   Risk Mitigation: Comprehensive data backup and recovery procedures were established to safeguard critical information. Data encryption and strict access controls were implemented to protect sensitive assets. Staff received training on secure data handling practices and cybersecurity protocols. Advanced backup and recovery solutions, along with data loss prevention tools, were deployed to minimize the risk of data loss or corruption.

Risk Monitoring: Data backup systems were routinely evaluated to ensure reliability and effectiveness. Continuous monitoring of data integrity was conducted, supported by proactive security measures designed to detect, mitigate, and prevent any potential data loss or corruption.

7. Inadequate Time Allocation/Delayed Delivery:

   Risk Mitigation: Comprehensive project planning was undertaken to ensure accurate estimation of timelines, resources, and deliverables. Adequate time was allocated to each project phase, incorporating contingencies to accommodate unforeseen challenges. Project management software with built-in scheduling and tracking capabilities was utilized, supported by regular progress meetings and the use of tracking tools to maintain oversight and accountability.

   Risk Monitoring: Project progress was continuously tracked against the established schedule, with any delays promptly addressed through adjustments in resources, scope, or timelines. Consistent communication with stakeholders was maintained to manage expectations and ensure alignment on project milestones.

   The evaluation of risk strategies implemented during the cyber exercise project indicates that effective risk mitigation and monitoring practices were in place. Through the adoption of these strategies and continuous review processes, the project effectively managed identified risks and maintained operational efficiency. Ongoing reviews and updates to the risk strategy ensured its sustained effectiveness throughout the project lifecycle.

5.1 Suggestions on Vendor Products to monitor Risk

Based on the review and evaluation of current risk strategies, the following vendor products are recommended for monitoring risk rating criteria, taking into account their functionality, scalability, and industry reputation in risk management.

1. ServiceNow: ServiceNow is a leading platform that provides a comprehensive suite of IT Service Management (ITSM) and IT Operations Management (ITOM) solutions. Its advanced risk management capabilities make it highly suitable for monitoring and managing risk rating criteria within complex organisational environments. Key benefits of using ServiceNow include:

a. **Integrated Platform:** ServiceNow offers a centralized environment that consolidates various IT and business processes, including risk management. This integration enables organisations to manage workflows, data, and reporting from a single platform, improving efficiency and visibility across risk management activities.

b. **Risk Assessment and Mitigation:** The platform supports robust risk assessment processes, allowing users to define risk profiles, evaluate and assign risk ratings, and implement mitigation strategies. It also provides tools for tracking progress in addressing and resolving identified risks.

c. **Customization and Reporting:** ServiceNow's flexible architecture allows organisations to customize workflows and risk management processes to meet their specific operational needs. Its powerful reporting and analytics tools enable stakeholders to monitor risk rating criteria, generate actionable insights, and make informed, data-driven decisions.

2. Archer (by RSA): Archer, developed by RSA, is a highly regarded Governance, Risk, and Compliance (GRC) platform known for its robust and comprehensive risk management capabilities. It is a strong choice for monitoring risk rating criteria in this scenario for the following reasons:

a. **GRC Focus:**
Archer is purpose-built to address governance, risk, and compliance requirements. It offers a wide range of tools for risk assessment, control monitoring, and reporting, making it an effective solution for managing and tracking risk rating criteria with precision and consistency.

b. **Workflow Automation:**
Archer features advanced workflow automation capabilities that enhance efficiency in risk management processes. It allows organisations to design and automate risk assessment workflows, assign tasks, and monitor progress, ensuring timely and systematic evaluation of risk rating criteria.

c. **Regulatory Compliance:**
Archer facilitates compliance management by providing a structured framework that aligns organisational risk practices with regulatory standards and industry requirements. This functionality is particularly valuable for monitoring risk rating criteria in compliance-driven environments.

Both **ServiceNow** and **Archer** are trusted by organisations worldwide for their proven effectiveness in risk management. Each platform offers distinct strengths that complement one another. ServiceNow excels in IT operations integration, while Archer provides deep GRC functionality. Together, their extensive capabilities and strong market reputation make them ideal solutions for monitoring and managing risk rating criteria in the described context.