RISK ASSESSMENT PROJECT

Remote Work Security Risks in a Gaming Company

Prepared by: *Raghad Lafe Al Suraihi*

Cybersecurity Graduate – GRC Focus

Date: *June 2025*

Note:

This report is based on a fictional scenario created for educational and portfolio purposes. It includes process documentation and data visualization

CONTENTS

PART I: PROJECT OVERVIEW AND INTRODUCTION

EXECUTIVE SUMMARY

This project presents a focused cybersecurity risk assessment for a (Company A) a gaming startup, with the explicit goal to transition key technical roles to fully remote work. The assessment is conducted in a hypothetical environment that imitates a real business setting.

As a fresh graduate in cybersecurity, this project serves as a portfolio deliverable to demonstrate applied skills in cybersecurity risk assessment. A structured methodology from NIST SP800-30 Rev. 1, and considers local cybersecurity controls by the Saudi National Cybersecurity Authority (NCA).

The goal of the project is to reflect on the ability to connect academic and professional training with real world practices.

1. INTRODUCTION

This project outlines a structured methodology for conducting a cybersecurity risk assessment in a controlled, hypothetical environment. The project simulates a realistic scenario involving a gaming startup. Due to the absence of direct industry access, the hypothetical company scenario will enable:

- Safe simulation of risk assessment processes without legal exposure.
- Depth of analysis in a risk rich, creative industry (gaming).
- Demonstrated understanding of industry specific threats in a remote work environment.

The gaming industry was chosen for this project due to the extra cybersecurity risks it faces. As these companies depend on things like intellectual property (IP) and proprietary assets (source code, design documents), they are highly attractive to attackers and vulnerable to risks. Additionally, fully remote operations for core technical employees greatly increase the attack surface. Therefore, in this case it becomes very suitable and justified to apply risk assessment.

2. PROJECT OBJECTIVE

- Display applied knowledge of cybersecurity risk assessment.
- Produce a deliverable (portfolio project) based on existing knowledge and skills.
- Directly supports the demonstration of expertise in cybersecurity risk assessment.
- Showcase core skills like analytical thinking, regulatory alignment, risk scoring, and professional reporting.

3. THE HYPOTHETICAL COMPANY (A)

Company Overview

Name: Company A
Industry: Game Development
Location: Saudi Arabia
Size: Around 370 employees
Structure: Hybrid (onsite + remote work model)

Company A intends to convert the following departments to fully remote positions for perceived convenience and flexibility:

- **Engineering Department:** Game Programmers
- **Design Department:** Game Designers

4. SCOPE

This project focuses on conducting a cybersecurity risk assessment for Company A's intended transition of its core development teams to fully remote work.

5. APPROACH

This project will employ a structured approach to conduct the cybersecurity risk assessment, primarily guided by the **NIST Special Publication 800-30 Revision 1, "Guide for Conducting Risk Assessments."** While this guidance was published in 2012, its foundational principles and systematic approach to risk identification, analysis, and evaluation remain highly relevant and widely accepted within the cybersecurity industry. Its detailed guidance on the risk assessment process provides a robust and well-understood structure crucial for this project. The framework is selected for its comprehensive and well-defined process that facilitates a systematic assessment of cybersecurity risks.

The risk assessment process will encompass the core stages outlined in NIST SP 800-30 Rev. 1:

1- **Prepare for the Assessment:** Defining the purpose, scope, assumptions, and constraints of the risk assessment.
2- **Conduct the Assessment:**
    - **Identify Threat Sources and Events:** Recognizing potential adversaries and the types of malicious or accidental actions they might undertake.
    - **Identify Vulnerabilities and Predisposing Conditions:** Discovering weaknesses in systems, processes, or controls that could be exploited by threat sources.
    - **Determine Likelihood of Occurrence:** Estimating the probability of a threat event exploiting a specific vulnerability.
    - **Determine Magnitude of Impact:** Assessing the severity of harm that could result from a successful threat event.
    - **Determine Risk:** Combining the likelihood and impact to calculate the overall risk level.
3- **Communicate Results:** The results of the risk assessment will be shared with Company A's management and key stakeholders in a clear and straightforward way. To support this, an interactive Power BI dashboard will be used. The dashboard will highlight the most critical risks, show key trends, and give a quick overview of the overall risk. It will include visuals that break down:
    - The overall risk posture
    - Top critical and high impact risks,
    - Risk categories based on affected assets, departments, threat sources, and vulnerability types.
    - The goal is to turn complex risk data into insights that are easy to understand and act on helping leadership make informed decisions and prioritize resources effectively.
4- **Maintain the Assessment:** While this project represents a one-time, static assessment for portfolio purposes, in the real world. This involves regularly reviewing and updating the risk register to reflect changes in the organizational environment, new threats, evolving vulnerabilities, and the effectiveness of implemented controls. This ensures that the risk assessment remains relevant and valuable over time, supporting Company A's ongoing security posture.

In addition to NIST SP 800-30 Rev. 1, this project will also integrate:

- **Saudi National Cybersecurity Authority (NCA) Essential Cybersecurity Controls (ECC):** These controls will be used as a reference to ensure that proposed recommendations align with regulatory requirements and best practices for cybersecurity within Saudi Arabia.

These approaches ensure that risk assessment is not only academically sound but also practically relevant and aligned with established industry standards and regulations.

6. LIMITATIONS

- Entirely fictional scenario
- No real stakeholders
- Static, more of a one time assessment

RISK ASSESSMENT REPORT

Cybersecurity Risk Assessment for Remote Work Transition

Date: *June 2025*

Prepared for: *Company A Management*

Prepared by: *Raghad Lafe – GRC Analyst*

Version: *1.0*

CONTENTS

EXECUTIVE SUMMARY

This report details a cybersecurity risk assessment conducted for Company A's Engineering and Design Departments transitioning to a fully remote work model. A total of **12** risks were identified and evaluated using a semi-quantitative methodology. The assessment revealed a significant risk landscape, comprising **1 Critical risk**, **9 High risks**, and **2 Medium risks**.

The most pressing concerns include the critical risk of **Game Source Code Compromise via Phishing (R-01)**, highlighting a major human element vulnerability. Other high-priority risks stem from potential **insider threats (R-02)**, **weak cloud security configurations (R-03, R-04, R-09)** leading to intellectual property exposure, and **unpatched software vulnerabilities (R-10, R-12)** in critical infrastructure like VPNs and the Unity Engine. Furthermore, prevalent threats like **ransomware (R-07)** and network intrusions due to **misconfigured firewalls (R-11)** pose substantial threats.

To mitigate these identified risks, the report provides actionable recommendations aligned with NCA. These include enhancing security awareness training, strengthening insider threat programs, implementing robust cloud and data protection measures, and improving vulnerability and patch management across remote workstations and critical software. Addressing these prioritized controls is essential for Company A to establish a resilient security posture in its new remote operating environment and protect its valuable intellectual property.

1. INTRODUCTION

1.1 PURPOSE OF THE RISK ASSESSMENT

The purpose of the risk assessment is to identify, analyze and evaluate the cyber risks associated with the transition of the two main core departments (**Engineering Department, Design Department**) employees of Company A to a fully remote work model. The aim of the assessment is to provide Company A's management with a clear understanding of the potential risks and provide practical and implementable recommendations to reduce these risks to an acceptable level.

1.2 SCOPE OF THE RISK ASSESSMENT

Departments:

- **Engineering Department**
- **Design Department**

Procedures:

- **Game development procedures**
- **file storage and sharing**
- **access to cloud infrastructure**
- **remote collaboration**

This assessment excludes the physical office infrastructure still used by other departments, as well as any risks that aren't directly related to the transition to remote work for the specified Departments.

2. METHODOLOGY

2.1 RISK ASSESSMENT FRAMEWORK

This risk assessment was conducted based on the methodology outlined in NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments. Additionally, the recommendations were aligned with the Essential Cybersecurity Controls (ECC) issued by Saudi Arabia's National Cybersecurity Authority (NCA) was used as a reference for proposing security controls.

2.2 ASSESSMENT TYPE

A semi-quantitative methodology was adopted for this risk assessment. This method uses numerical scales to evaluate both the likelihood of occurrence and the potential impact of each risk scenario, allowing for a more precise calculation of risk scores. These calculated scores are then mapped to descriptive risk levels (Critical, High, Medium, Low) to support clear communication, prioritization, and decision making.

2.3 RISK MODEL

- **Likelihood Scales:** A numerical scale from 1 to 5 was used to estimate the likelihood of a threat event exploiting vulnerability.

Score	Qualitative Level	Description
1	**Very Low**	Very unlikely to occur
2	**Low**	Unlikely to occur, but possible
3	**Medium**	Likely to occur
4	**High**	Very likely to occur
5	**Very High**	Almost certain to occur, or occurs continuously

(Table 1: Likelihood Scales)

- **Impact Scales:** A numerical scale from 1 to 5 was used to estimate the potential impact should the risk materialize, considering effects on *intellectual property confidentiality*, *operational processes*, *reputation*, *Employee* and *financial aspects*. The maximum impact across these categories was considered.

Score	Qualitative Level	Description
1	**Negligible**	Insignificant overall effect.
2	**Minor**	Slight, easily manageable negative effect.
3	**Moderate**	Noticeable negative effect, requiring resources to address.
4	**Major**	Serious negative effect, impacting key objectives.
5	**Catastrophic**	Devastating effect, threatening company viability.

(Table 2: Impact Scale)

- **Risk Matrix (Semi-Quantitative: 5x5)**
  - Risk Score = Likelihood x Impact Score
  - Risk Level is determination based on the risk score -> mapped to a qualitative risk level for prioritization:

    1 - 4: Low

    5 - 9: Medium

    10 - 15: High

    16 - 25: Critical

Likelihood \ Impact	Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Very Low 1	1	2	3	4	5
Low 2	2	4	6	8	10
Medium 3	3	6	9	12	15
High 4	4	8	12	16	20
Very High 5	5	10	15	20	25

(Table 3: Semi-Quantitative Risk Matrix)

3. CONDUCT ASSESSMENT

3.1 ASSET IDENTIFICATION

According to Section 1.2 and the basic requirements for risk assessment, the first part of conducting the assessment was to find out which assets needed to be protected. These include hardware, software, data and employees needed for Engineering and Design remote work at Company A. For each asset, its value and importance were assessed based on its Confidentiality, Integrity, and Availability (CIA) requirements. **A complete and detailed list of identified assets can be found in Appendix A: Asset Inventory**

3.2 THREAT IDENTIFICATION

Once critical assets were identified, the next step involved systematically identifying potential **threat sources** and the **threat events** they might initiate. This process, aligned with NIST SP 800-30 Rev. 1, focused on understanding WHO AND WHAT could potentially cause harm to Company A's remote operations and intellectual property? And HOW might they do it?

Key categories of threats identified for Company A's remote work environment include:

- External Malicious Actor
- Malicious Insider
- Accidental (Human Error/System Failure)
- External Environmental Factors

3.3 VULNERABILITY IDENTIFICATION

Following the identification of assets and potential threats, the next critical step was to pinpoint **vulnerabilities**. These are the weaknesses or gaps within Company A's systems, security procedures, or remote work practices that a threat could exploit to achieve its objective. The approach involved reviewing typical vulnerabilities found in remote environments and specific weaknesses that might affect a gaming development company assets.

The assessment highlighted several key areas of vulnerability:

- **Remote Workstation Security**: Weaknesses related to the configuration and protection of company issued remote devices.
- **Cloud Service Security:** Given the heavy reliance on cloud platforms for collaboration, storage, and development, misconfigurations, inadequate access controls, or weak monitoring of cloud services present significant vulnerabilities.
- **Data Handling and Access Controls:** This covers weaknesses in how sensitive intellectual property and operational data are managed throughout remote work environment intellectual is stored, shared, and accessed.
- **People and Processes:** Human factors and procedural shortcomings.

- **Software Supply Chain Security**: Risks from using third-party software or assets that might have their own weaknesses.

Each specific vulnerability, when paired with a threat and an asset, contributes directly to the risk, detailed in the **Detailed in Appendix B: Risk Register.**

3.4 RISK DETERMINATION (RISK REGISTER)

Based on the methodology outlined in Section 2, a risk register has been developed to document the identified cybersecurity risks associated with the transition to a fully remote work model for the Engineering and Design Departments. A total of **12** risks were identified and assessed.

The risk assessment revealed the following risk profile for Company A's remote operations:

- **1 Critical Risks**
- **9 High Risks**
- **2 Medium Risks**
- **0 Low Risks**

Key High-Level Risks Identified:

The most significant risks, categorized as Critical and High, requiring immediate attention and prioritization, include:

- **R-01: Compromise of Game Source Code via Phishing (Critical)**
    - Unauthorized access to sensitive game source code due to successful phishing attacks exploiting insufficient employee security awareness.
- **R-02: Malicious Insider Data Theft/Disruption (High)**
    - A malicious remote employee abusing authorized access to steal game data or disrupt development, causing significant financial and reputational loss due to inadequate monitoring of employee activity.
- **R-03: Theft/Modification/Deletion of Git Repository Content (High)**
    - Attackers gaining unauthorized access to critical Git repositories due to weak credential management practices, leading to the theft, modification, or deletion of critical game source code.
- **R-04: Sensitive GDDs Leaked from Cloud Storage (High)**

    - Unauthorized access to and leakage or theft of sensitive Game Design Documents (GDDs) from cloud storage due to misconfigurations (overly permissive access or public sharing).

- **R-06: Unauthorized Access via MFA Bypass (High)**
    - Successful MFA bypass, negating a critical security layer and allowing unauthorized access to remote workstations and sensitive data, due to employee susceptibility to fraudulent MFA prompts.
- **R-07: Ransomware Infection on Remote Workstations (High)**
    - Ransomware encrypting data on a remote workstation, leading to data loss, operational disruption, and potential spread to other systems, typically via malicious email attachments.
- **R-09: Data Exfiltration from Azure SQL Database (High)**
    - Unauthorized access to sensitive data stored in Azure SQL Database due to unencrypted connections, leading to data exfiltration or intellectual property theft.
- **R-10: Network Intrusion via Unpatched VPN Vulnerabilities (High)**
    - Exploitation of unpatched critical vulnerabilities in the remote access VPN server, providing attackers direct internal network access and bypassing perimeter defenses.
- **R-11: Network Intrusion due to Misconfigured Firewall (High)**
    - Unauthorized network intrusion, leading to compromise of internal systems, data loss, or disruption of operations, due to misconfigured firewall rules allowing malicious traffic.
- **R-12: Compromise of Unity Engine via Outdated Software (High)**
    - Exploiting known Unity bugs in an outdated Unity Engine version, allowing attackers to compromise the application, steal data, or inject malicious behavior.

For a complete and detailed list of all identified risks, including their full descriptions, calculated scores, and rationale, please refer to **Appendix B: Risk Register**.

4. RECOMMNDATIONS

1. Strengthen Employee Cybersecurity Awareness

- **Core Risk Addressed:** Critical risk of **Game Source Code Compromise via Phishing (R-01)** due to insufficient employee security awareness.
- **Recommendation:**
    - **Implement a comprehensive cybersecurity awareness program** that includes regular, mandatory training sessions, phishing simulations, and clear guidelines for handling sensitive intellectual property. This program should be engaging and updated frequently to reflect current threats.
- **NCA Alignment:**

- **ECC 1-10-1:** A cybersecurity awareness program must be developed and approved.
- **ECC 1-10-2:** The cybersecurity awareness program must be implemented.
- **ECC 1-10-3-1:** The cybersecurity awareness program must cover secure handling of email services, especially phishing emails.

2. Enhance Insider Threat Management & Monitoring

- **Core Risk Addressed:** High risk of **Malicious Insider Data Theft/Disruption (R-02)** due to inadequate monitoring of employee activity.
- **Recommendation:**
    - **Implement monitoring and auditing of user activity** on critical systems and for access to sensitive data.
    - **Enforce access controls based on the principle of "least privilege,"** ensuring employees only have access necessary for their roles.

- **NCA Alignment:**

  - **ECC 2-12-3-4:** Continuous monitoring of cybersecurity events (from critical information assets and remote/privileged user accounts).
  - **ECC 2-2-3-3:** User authorization based on identity and access control principles: Need-to-Know and Need-to-Use, Least Privilege and Segregation of Duties.
  - **ECC 2-12-3-2:** Activation of cybersecurity event logs on remote access and privileged user accounts.

3. Secure Cloud Environments & Data Protection

- **Core Risks Addressed:** High risks of **Theft/Modification/Deletion of Git Repository Content (R-03)**, **Sensitive GDDs Leaked from Cloud Storage (R-04)**, and **Data Exfiltration from Azure SQL Database (R-09)** due to weak configurations and unencrypted connections.

- **Recommendation:**

  - **Conduct regular security assessments of all cloud services**

  - **Implement and maintain secure configuration baselines** for all cloud services, ensuring strong access permissions and disabling public access for sensitive data.

  - **Enforce data encryption for data at rest and in transit in Database.**

  - **Mandate Multi-Factor Authentication (MFA)** for all cloud service access and privileged accounts.

- **NCA Alignment:**

  - **ECC 4-2-1:** Cybersecurity requirements related to the use of hosting and cloud computing services must be defined, documented and approved.
  - **ECC 4-2-2:** The cybersecurity requirements related to the use of hosting and cloud computing services must be implemented.
  - **ECC 2-8-3-3:** Encryption of data in-transit and at-rest as per classification and related laws and regulations.
  - **ECC 2-2-3-2:** Multi-factor authentication for remote access.
  - **ECC 2-2-3:** The cybersecurity requirements for identity and access management must include Multi-Factor Authentication.

4. Robust Endpoint & Network Security Management

- **Core Risks Addressed:** High risks including **Unauthorized Access via MFA Bypass (R-06)**, **Ransomware Infection on Remote Workstations (R-07)**, **Network Intrusion via Unpatched VPN Vulnerabilities (R-10)**, **Network Intrusion due to Misconfigured Firewall (R-11)**, and **Compromise of Unity Engine via Outdated Software (R-12)**.
- **Recommendation:**
    - **Implement a comprehensive vulnerability management process** for all remote workstations, VPN servers, and critical development software. This includes regular vulnerability scanning and prompt patching.
    - **Deploy advanced anti-malware solutions**
    - **Implement and maintain secure network configurations**.
    - **Provide specific cybersecurity awareness training** on recognizing and avoiding social engineering tactics that attempt to bypass MFA.
- **NCA Alignment:**

- **ECC 2-10-1:** Cybersecurity requirements for technical vulnerabilities management must be defined, documented and approved.
- **ECC 2-10-2:** The cybersecurity requirements for technical vulnerabilities management must be implemented.
- **ECC 2-10-3-1:** Periodic vulnerabilities assessments.
- **ECC 2-10-3-4:** Security patch management.
- **ECC 2-3-3-1:** Advanced, up-to-date and secure management of malware and virus protection on servers and workstations.
- **ECC 2-5-1:** Cybersecurity requirements for network security management must be defined, documented and approved.
- **ECC 2-5-2:** The cybersecurity requirements for network security management must be implemented.
- **ECC 2-5-3-1:** Logical or physical segregation and segmentation of network segments using firewalls.
- **ECC 2-5-3-5:** Management and restrictions on network services, protocols and ports.

- **ECC 1-10-3:** The cybersecurity awareness program must cover the latest cyber threats and how to protect against them (specifically relevant to social engineering targeting MFA).

5. COMMUNICATE RESULTS

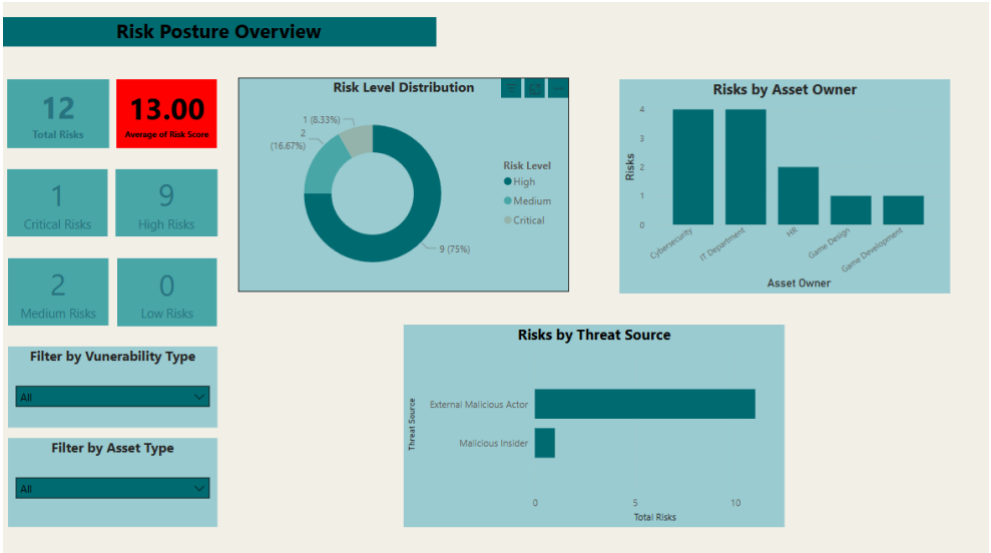
The results of this cybersecurity risk assessment will be shared with Company A's management and key stakeholders in a clear and straightforward way. To support this, an interactive Power BI dashboard has been developed. **The full interactive dashboard can be accessed publicly via the following link:**

https://app.powerbi.com/view?r=eyJrIjoiMTg5ZTFhOWUtOGMzMy00NWE1LTkxZmItY2I5YmQ0ZmM4ODk5IiwidCI6ImI0NTNkOTFiLTZhYzEtNGI2MS1iOGI4LTVlNjVlNDIyMjMzZiIsImMiOjI9

The dashboard will highlight:

- **The overall cybersecurity risk posture** of Company A.
- **Critical and high impact risks**, providing a focused view on the most pressing concerns.
- **Risk categories** broken down by affected assets, departments, threat sources, and vulnerability types, offering granular insights.

This visual representation, both in the interactive dashboard and through the screenshots included below, aims to provide a quick, intuitive overview of the identified risks and their implications.



6. CONCLUSION

The transition to a fully remote work model for Company A's Engineering and Design Departments introduces several significant cybersecurity risks, primarily within the Critical and High categories. These risks largely stem from vulnerabilities related to human factors, cloud service misconfigurations, and weaknesses in software and endpoint security.

By adopting the recommended security controls, Company A can significantly reduce its exposure to these identified threats, bringing the overall cyber risk posture to an acceptable level. Continuous monitoring, regular training, and a proactive approach to vulnerability management will be essential to maintaining a secure remote work environment and protecting the company's valuable intellectual property.

APPENDIX A: ASSET INVENTORY

Asset Inventory									
Asset ID	**Asset Name**	**Asset Description**	**Asset Type**	**Asset Owner**	**Location**	**Confidentiality**	**Integrity**	**Availability**	**Asset Value**
H-003	Remote Employees	Employees in the Game Design and Game Development departments that working remotely.	People	HR	Remote workstation	4	4	5	4
D-205	Game source codes	The collection of source code of all game projects that under devlopment.	Data	Game Development	Git repository	5	5	4	5
D-256	Core game design documents (GDDs)	Core documents outlining design specifications and game logic.	Data	Game Design	Cloud storage	5	5	4	5
SW-403	MS Teams	Platform the for remote team communication and colapration.	Software	IT Department	Remote workstation	3	3	4	3
SW-405	MFA Authentication System	Authentication system ensuring secure access to remote workstation.	Software	Cybersecurity	Remote workstation	5	5	5	5
HW-309	Remote Workstations	Devices issued by the company for remote Game Design & Dev Employees, secured with EDR.	Hardware	IT Department	Remote workstation	4	4	4	4
SW-406	Unity Engine	The game development platform used by developers to build game assets and logic.	Software	IT Department	Remote workstation	3	4	5	4
SW-407	Microsoft Defender for Endpoint (EDR)	The EDR solution securing remote workstations.	Software	Cybersecurity	Remote workstation	5	5	5	5
CS-110	Azure SQL Database	Cloud-hosted DB used by remote dev teams for game backend testing or storage.	Cloud Service	IT Department	Cloud Platform (Azure)	5	5	4	5
SW-404	GitHub	Used for hosting Git repositories.	Software	Game Development	Cloud Platform (GitHub)	5	5	4	5
SW-408	Remote Access VPN	Secure VPN tunnel allowing remote employees to access internal company resources.	Software	Cybersecurity	Remote Workstation / Network Gateway	5	5	5	5
SW-409	Firewall	Network security system controlling incoming/outgoing traffic to protect internal resources accessed remotely.	Software	Cybersecurity	Company Network Gateway / Remote Workstation	5	5	5	5

APPENDIX B: RISK REGISTER

Risk Assessment										
		Threats Identification		Vulnerability Identification		Risk Analysis				
Risk ID	Asset ID	Threat Source	Threat Description	Vulnerability Type	Vulnerability Description	Risk Descrption	Impact Score	Likelihood Score	Risk Score	Risk Level
R-01	H-003	External Malicious Actor	Attackers execute Phishing Attacke (Social engineering)	People and Processes	Insufficient employee security awareness training, employee negligence	Unauthorized access to game source code via compromised remote employee credentials.	4	4	16	Critical
R-02	H-003	Malicious Insider	Malicious remote employee abuses authorized access to exfiltrate sensitive company data.	People and Processes	Inadequate monitoring of remote employee activity involving sensitive assets.	Malicious remote employee exploits access to steal game data or disrupt development, causing significant financial and reputational loss.	4	3	12	High
R-03	D-205	External Malicious Actor	Unauthorized access to Git repositories (GitHub)	Data Handling and Access Controls	Weak credential management practices for accessing Git repositories	Attackers gain unauthorized access to Git repository, leading to theft, modification, or deletion of critical game source code.	5	3	15	High
R-04	D-256	External Malicious Actor	Unauthorized access to cloud storage with GDDs.	Data Handling and Access Controls	Misconfiguration of cloud storage (overly permissive access or public sharing)	Sensitive GDDs leaked or stolen due to insecure cloud storage Misconfiguration sharing settings.	5	3	15	High
R-05	SW-403	External Malicious Actor	Malicious files are distributed via MS Teams messages.	People and Processes	Employees downloading and executing untrusted files received through MS Teams communications	Compromise of MS Teams leads to malware spread to workstations, impacting employee productivity.	3	3	9	Medium
R-06	SW-405	External Malicious Actor	Attacker execute MFA fatigue attacks. (Social engineering)	People and Processes	Employee susceptibility to approving fraudulent MFA prompts due to repeated, overwhelming requests.	Successful MFA bypass negates a critical security layer, allowing unauthorized access to remote workstations and sensitive data.	5	3	15	High
R-07	HW-309	External Malicious Actor	Ransomware encrypts data on a remote workstation	Remote Workstation Security	Remote workstation infected by ransomware via a malicious email attachment.	Ransomware on a remote workstation leads to data loss, operational disruption, and potential spread to other systems.	4	3	12	High
R-08	SW-407	External Malicious Actor	Sophisticated malware variant evades detection by the EDR solution.	Software Supply Chain Security	EDR solution's detection capabilities are bypassed by a novel or highly obfuscated malware strain.	Undetected malicious activity on workstations, potentially leading to data exfiltration, system compromise, or further network intrusion due to EDR bypass.	5	1	5	Medium
R-9	CS-110	External Malicious Actor	Data theft or leakage from Azure SQL Database	Data Handling and Access Controls	Lack of enforced encryption for all database connections.	Unauthorized access to sensitive data stored in Azure SQL Database due to unencrypted connections, leading to data exfiltration or intellectual property theft.	5	3	15	High
R-10	SW-408	External Malicious Actor	Attacker exploits a critical vulnerability (e.g., CVE-2023-27997, heap buffer overflow in Fortinet FortiOS SSL-VPN)	Software Supply Chain Security	Presence of unpatched known critical vulnerabilities in the remote access VPN server software.	Compromised VPN provides attackers direct internal network access, bypassing perimeter defenses and exposing sensitive internal resources.	5	3	15	High
R-11	SW-409	External Malicious Actor	Unauthorized network traffic bypasses the firewall	Software Supply Chain Security	Misconfiguration of the firewall rule	Unauthorized network intrusion, leading to compromise of internal systems or disruption of operations, due to misconfigured firewall rules that allowing malicious traffic.	5	3	15	High
R-12	SW-406	External Malicious Actor	Attacker exploits known vulnerabilities in an outdated Unity Engine version	Software Supply Chain Security	Failure to update Unity Engine regularly with security patches.	Exploiting known Unity bugs allows attackers to compromise the software, steal data, or inject malicious behavior.	4	3	12	High