Information Security Risk Management (IE3052)

Risk Assessment Report.

Sri Lanka Institute of Information Technology

Lecturer: Kavinga Yapa Abeywardena

Date of Submission: 2024/05/02

IT numbers	Name
IT21826368	Nanayakkara Y.D.T. D
IT21822612	Mendis H.R.M
IT21831904	Weerasinghe K.M
IT21828348	Dissanayaka K.D.A.R. A

YOUBESOFT:

Security Risk Assessment Report

2024

By YOUBESOFT Entertainment.

1 Contents

2 Executive Summary

This Security evaluation was carried out by **YOUBESOFT Entertainment**, in one month time duration. The aim was to provide reliable and secure gaming solutions that protect customer data and ensure uninterrupted gaming experiences by identifying the Confidentiality, Integrity, and Availability of the company's systems and data, specifically in preparation for the migration of its game servers to a cloud-based infrastructure. Despite recognizing severe threats and vulnerabilities, the **OCTAVE ALLEGRO** risk assessment approach was used. After completing the Qualitative risk analysis of the system, a Quantitative risk analysis was performed for the critical assets. Predicting the probability levels of each asset.

Key Concerns and Recommendations

- **YOUBESOFT Engine** is a proprietary game server software developed by YOUBESOFT Entertainment that has some Vulnerabilities that can lead to arbitrary code execution.

There is a vulnerability in the YOUBESOFT engine which leads to arbitrary code execution that may compromise the web and game server, which can result in service outages and user data loss. to mitigate this threat effectively it is vital to have frequent updates and patches to the system, as well as applying safe coding techniques which can help addressing this vulnerability.

- **SALESFORCE customer relationship management (CRM) system** is used to manage player accounts and it was attacked by a privilege escalation.

Attackers utilized a vulnerability in abuse elevation control mechanisms and TCC manipulation to obtain unauthorized access to the CRM system, resulting to unauthorized access to sensitive information. To prevent this, regular reviews of applications, automation under security and privacy options, software upgrades, and macOS or Sierra+ systems are suggested, as well as system integrity protection (SIP) enabled.

- **SALESFORCE Database Management System (DBMS),** which contains vital information about consumers' purchases of virtual currencies is vulnerable to SQL injection attacks.

SQL injection vulnerability in a company's salesforce database could allow attackers to access sensitive information about consumers' virtual currency purchases, posing risks of identity theft and financial fraud. Input validation and parameterized queries are crucial techniques to prevent SQL injection attacks. These methods ensure user input is sanitized, separate SQL code from user input, and adhere to the least privilege principle.

- The company saves game assets on **AWS cloud servers** and runs server environments there, yet it's vulnerable to attacks like DDoS which might impact operations.

Because of its susceptibility to DDoS attacks, the enterprise's AWS infrastructure can potentially disrupt services, leading to downtime, player disappointment, financial losses, and a loss of income for products that rely on online connectivity. Use AWS Shield, Auto Scaling, AWS CloudWatch, Debugging the API code, fix configurations, regularly monitor the services to defend against DDoS attacks.

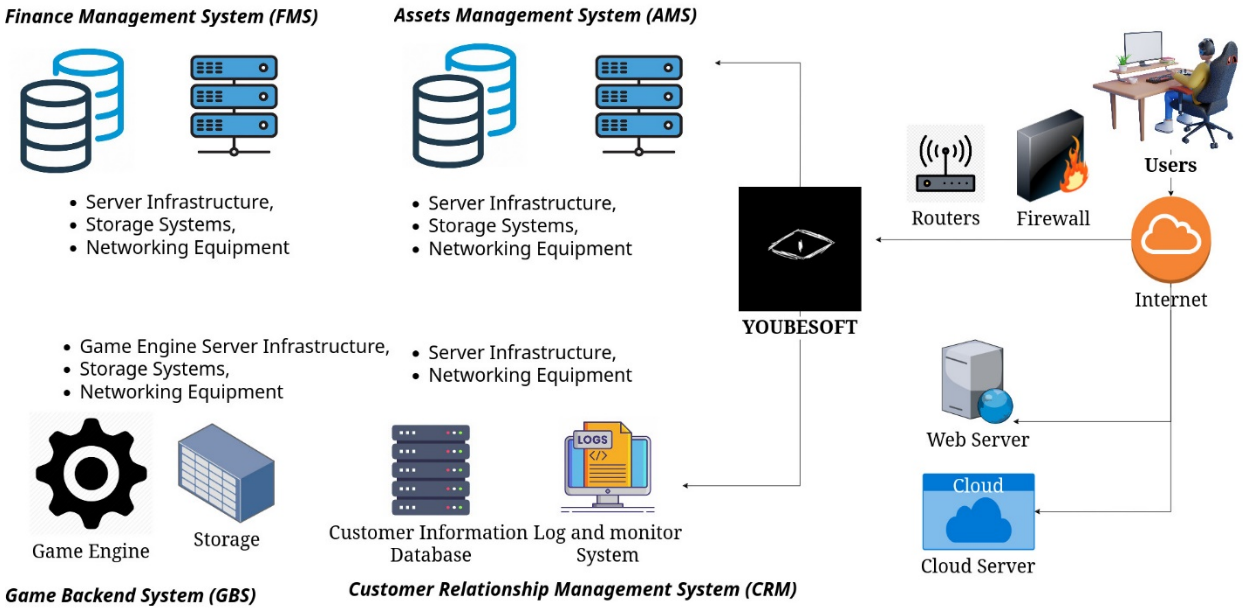
- **Cisco ISR 4000 Series Integrated Service Routers** are deployed within the network infrastructure of YOUBESOFT Entertainment to facilitate secure and reliable communication.

To ensure the Confidentiality, integrity, and availability of data transmitted over the networks software updates and patches must be done regularly. Also use a Role-Based Access Control (RBAC) to limit administrative access to Cisco ISR 4000 Series routers, allowing only authorized personnel to make configuration changes.

3 Detailed Analysis

3.1 Company Background

YOUBESOFT Entertainment is a leading game development company known for its innovative and high-quality gaming products and services. With a focus on providing engaging and immersive gaming experiences, YOUBESOFT Entertainment has established itself as a prominent player in the gaming industry since 2010. The company offers a wide range of gaming products and services to meet the diverse needs of gamers worldwide.



3.2 Purpose

YOUBESOFT Entertainment intends to migrate to a cloud-based architecture for its gaming servers to keep up with the increasing number of players and enhance scalability. All game information, including player user accounts, in-game purchases, and progress, are being moved to the cloud servers as part of this migration. The corporation has concerns about the potential cybersecurity dangers connected to cloud storage of player personal information, however. The importance of the assets to the gaming platform and the potential repercussions of security breaches or data loss were taken into consideration while determining which assets to safeguard. Maintaining player trust, safeguarding data privacy, and preserving the integrity of the gaming experience all depend on these resources being safeguarded. This migration's suggested design aims to guarantee the gaming platform's dependability, scalability, and security. This paper does not provide a comprehensive design, but the high-level architectural diagram illustrates the suggested structure.

3.3 Risk Assessment Framework

The OCTAVE ALLEGRO framework was utilized for a risk assessment, focusing on information security risks associated with vital firm assets. This approach saves time, money, and effort, identifying resources crucial for company goals and identifying vulnerabilities.

3.4 Asset Profile

Critical Asset	**Security Requirements**			
	Property	**High**	**Mid**	**Lo w**
Game Backend System (GBS) **Asset Value ($): 750,000** **Tech:** YOUBESOFT ENGINE, Web/Game Servers, Storage Systems. **Description:** A game backend system server is a computer system hosting online multiplayer games, managing rules, matchmaking, communication, progress storage, and performance under heavy loads, ensuring interactive and engaging gaming experiences.	Confidentiality		✓	
	Integrity	✓		
	Availability		✓	
Customer Relationship Management System (CRM) **Asset Value ($): 500,000**. ***Tech:*** Salesforce CRM***,*** Server Infrastructure, Storage Systems. ***Description***: CRM systems help companies manage client relationships, track interactions, and store contact details. They enhance customer service, marketing, and sales by connecting with other corporate software and providing a comprehensive picture of client connections.	Confidentiality		✓	
	Integrity	✓		
	Availability		✓	

Finance Management System (FMS) **Asset Value ($): 500,000** **Hardware**: Server Infrastructure, Storage Systems, Networking Equipment **Software**: SALESFORCE DBMS **Description:** The Finance Management System is a software application that helps businesses manage their financial operations. It has functions for financial reporting, payroll processing, invoicing, budgeting, and accounting. The system's integration with other business apps enhances financial decision-making by offering a thorough picture of the business's financial situation.	Confidentiality		✓	
	Integrity	✓		
	Availability		✓	
Assets Management System (AMS) **Asset Value ($): 400,000** **Tech:** Custom-Built AMS, AWS CLOUD Servers **Description:** The Assets Management System is a software application that helps businesses track and manage their physical assets efficiently. It has functions for inventory management, reporting, depreciation computation, asset tracking, and maintenance scheduling. Because it is hosted on AWS Cloud Servers, the system has security, scalability, and dependability.	Confidentiality		✓	
	Integrity	✓		
	Availability		✓	
Network Infrastructure **Asset Value ($): 600,000** **Devices Used:** CISCO ISR 4000 Series Integrated Server Routers, Cisco ASA, Cisco Catalyst series. **Description**: The hardware and software components	Confidentiality	✓		
	Integrity	✓		
	Availability	✓		

that provide data exchange and communication within an organization make up the network infrastructure. Switches, routers, firewalls, and other networking equipment are included. CISCO ISR 4000 Series Integrated Service Routers, which offer dependable and secure connectivity for data transfer, are used in the construction of the network infrastructure.				

3.5 Threat Profile

Asset	**Threat/ Vulnerability**	**Impact Assessment**	**Mitigation**
Game Backend System (GBS)	**Threat:** The Servers can expose to the Arbitrary Code Execution attacks. Which can compromise the whole system. **Vulnerability:** Improper Input Validation was found in the server configurations.	**Outcome:** Potential compromise of game server. Leading to service disruption and data loss. **Risk Level: HIGH**	Regularly Update and Patch the Server. Implement Secure Coding Practices. **Annual Cost of Mitigation** = $50,000
Before Mitigation Applied		**After Mitigation Applied**	
EF	70%	20%	
SLE	$750,000 x 0.70 = $525,000	$750,000 x 0.20 = 150,000	
ARO	2		
ALE	$525,000 x 2 = $1,050,000	$150,000 x 2 = $300,000	
Cost/Benefit	$1,050,000 - $300,000 -$50,000 = $700,000		

Asset	**Threat/ Vulnerability**	**Impact Assessment**	**Mitigation**
Customer Relationship Management System (CRM)	**Threat:** Because we have access controls the system can have privilege escalation from the SALESFORCE software and some weak configurations **Vulnerability:** We have found Abuse Elevation Control Mechanism: TCC Manipulation in the system. **CVE-2022-32862:** score: 5.5	**Outcome:** unauthorized administrative access to the CRM Leading to unauthorized access to sensitive data **Risk Level: HIGH**	Routinely check applications using Automation under Security & Privacy System Preferences, Update software. Where possible, ensure systems are macOS Sierra+ and SIP is enabled.

	(Medium)		***Annual Cost of Mitigation*** *= $40,000*
Before Mitigation Applied		**After Mitigation Application**	
EF	100%	15%	
SLE	$500,000 x 0.100% = $500,000	$500,000 x 0.15% = $75,000	
ARO	3		
ALE	$500,000 x 3 = $1,500,000	$75,00 x 3 = $225,000	
Cost/Benefit	$1,500,000 - $225,000 - $40,000 = $1,235,000		

Asset	Threat/ Vulnerability	Impact Assessment	Mitigation
Finance Management System (FMS)	**Threat**: System can be bypassed using a SQL Injection due to its Vulnerabilities. **Vulnerability**: Lack of input validation, Parameterized Queries	**Outcome**: Unauthorized access to consumer data Which could lead to data breaches and financial fraud. **Risk Level: HIGH**	Implement input validation, Parameterized queries. **Annual Cost of Mitigation =** $34,000
Before Mitigation Applied		**After Mitigation Application**	
EF	40%	10%	
SLE	$500,000 x 0.40 = $200,000	$500,000 x 0.10 = $ $10,00	
ARO	2		
ALE	$200,000 x 2 = $ =400,000	$10,000 x 2 = $20,000	
Cost/Benefit	$400,000 - $20,000 - $34,000 = $346,000		

Asset	Threat/ Vulnerability	Impact Assessment	Mitigation
Assets Management System (AMS)	**Threat:** Report Generating API in the Management system is not functional it can result in DDOS attack. **Vulnerability:** We have found exposed APIs used in the Server	**Outcome:** Service disruption and financial losses leading to system downtime **Risk Level: MEDIUM**	Use AWS Shield, Auto Scaling, AWS CloudWatch, regularly monitor. Debugging the API code, fixing configuration.

			Annual Cost of Mitigation = $30,000
Before Mitigation Applied		**After Mitigation Application**	
EF	30%	5%	
SLE	$400,000 x 0.30 = $120,000	$400,000 x 0.05 = $20,000	
ARO	4		
ALE	$120,000 x 4 = $480,000	$20,000 x 4 = $100,000	
Cost/Benefit	$480,000 - $ 100,000 - $30,000 = $350,000		

Asset	Threat/ Vulnerability	Impact Assessment	Mitigation
Network Infrastructure	**Threat:** In the Cisco ISR routers we found a vulnerability in CISCO IOS (Integrated Operating System) which can used to have unauthorized Access to the system infrastructure. **Vulnerability:** The server software is Lack of Regular Updates and Patches	**Outcome:** Compromised data integrity and service disruption **Risk Level: HIGH**	Regularly update and patch Cisco ISR 4000 Series Integrated Service Routers (ISR) **Annual Cost of Mitigation $50,000**
Before Mitigation Applied		**After Mitigation Application**	
EF	35%	5%	
SLE	$600,000 x 0.35 = $210,000	$600,000 x 0.05 = $30,000	
ARO	2		
ALE	$210,000 x 2 = $420,000	$30,000 x 2 = $60,000	
Cost/Benefit	$420,000 - $60,000 - $50,000 = $310,000		

4 Technical Summary

4.1 Key Tasks:

YOUBESOFT Entertainment, a leading game production company, conducted risk assessments to assess system architecture security, identifying five critical assets. The technical staff is now responsible for implementing suggested solutions to mitigate vulnerabilities.

Game Backend System - The **YOUBESOFT Engine**, a proprietary game server software, is vulnerable to arbitrary code execution. To address this vulnerability, implement frequent updates and patches to the

YOUBESOFT Engine and apply secure coding techniques. Furthermore, we must monitor for any suspicious activities.

Customer Relationship System -The **SALESFORCE (CRM)** System, used for managing player accounts, has been compromised due to abuse of control mechanisms and manipulation of TCC. To prevent unauthorized access, technical staff must conduct regular application reviews, automate security and privacy settings, perform software upgrades, and ensure macOS Sierra+ systems are running with System Integrity Protection enabled.

Finance Management System - The **SALESFORCE Database Management System (DBMS),** containing vital information about consumers' purchases of virtual currencies, is vulnerable to SQL injection attacks. To prevent such attacks, the technical staff must implement input validation and parameterized queries to ensure that user input is sanitized, and that SQL code is separated from user input.

Assets Management System - The company's **AWS Cloud Servers**, where game assets are stored and server environments are run, are vulnerable to DDoS attacks. To defend against these attacks and prevent service disruption, downtime, and financial losses, the technical staff must implement AWS Shield, Auto Scaling, and AWS CloudWatch. Additionally, they should debug the API code, fix configurations, and regularly monitor services to detect and mitigate DDoS attacks.

Network Infrastructure - Procuring **Cisco ISR 4000 Series Integrated Services Routers** to serve as the primary gateway for network traffic between on-premises and cloud-based infrastructure, ensuring secure and reliable communication between game servers, player devices, and the cloud. Additionally, enterprise-grade firewalls will be deployed to protect the cloud-based infrastructure from unauthorized access and network-based attacks. Load balancers will also be deployed to distribute incoming player traffic evenly across multiple game servers, optimizing performance and ensuring scalability. Finally, identity and access management (IAM) software will be procured and deployed to manage user identities, access rights, and permissions within the gaming platform, ensuring secure authentication and authorization processes.

5 Appendix

5.1 Appendix A

Assumptions

Scalability:

The cloud-based infrastructure is designed to scale dynamically based on demand, allowing YOUBESOFT to accommodate its growing player base without compromising performance.

YOUBESOFT Entertainment takes cybersecurity seriously:

The organization is taking action to fix the flaws it discovered in its systems. It also indicates that the organization places a high premium on cybersecurity.

The company's systems contain sensitive data:

YOUBESOFT Entertainment's systems, including the game backend system, customer relationship system, finance management system, assets management system, and network infrastructure, store and process sensitive data such as player accounts, financial information, and game assets.

The company is committed to continuous improvement:

YOUBESOFT Entertainment is implementing a range of security measures, including frequent updates, secure coding techniques, regular application reviews, security automation, and employee training. This suggests a commitment to ongoing security improvement and adaptation to emerging threats.

Compliance is a priority:

The company is aware of regulatory requirements and aims to ensure compliance with relevant industry standards and regulations such as GDPR, HIPAA, or PCI DSS.

Investment in infrastructure and technology:

To strengthen its security posture and secure its systems and data, YOUBESOFT Entertainment is prepared to invest in infrastructure, technology, and security solutions like load balancers, enterprise-grade firewalls, Cisco ISR routers, and IAM software.

A multi-layered security approach is being adopted:

Instead of depending on a single fix to fix its security flaws, the company is putting in place a multi-layered security strategy that involves staff training, software updates, network infrastructure advancements, and secure coding methodologies.

Regular monitoring and maintenance are priorities:

YOUBESOFT Entertainment recognizes the importance of regular monitoring, maintenance, and testing to ensure the effectiveness of its security measures over time.

Qualitative Analysis Parameters

Risk = Magnitude of Impact X Threat Probability

Magnitude of Impact

Impact	Score	Definition
HIGH	10	This has a significant effect. This can lead to significant asset and financial losses that are irreversible. It will either take proper handling or adaptation, or it will be impossible to handle.
MEDIUM	5	This has a major influence. This can result in the loss of recoverable assets as well as financial losses. In normal conditions, it is manageable.
LOW	1	This has a small impact. This can result in small financial and asset losses. It may be necessary to make an attempt to reduce management effort, or it may not be necessary.

Threat Probability

Threat	Score	Definition
HIGH	1.0	The threat source has a high chance of thwarting the scheme, and existing safeguards provide inadequate defense. Efficient countermeasures must be taken right away.
MEDIUM	0.5	The threat source has a moderate chance of thwarting the device, and existing safeguards have some defenses that could significantly mitigate the threat.
LOW	0.1	There is little risk that the threat source will be able to prevent the device, and existing protections provide near-complete defense.

Risk Calculation

Impact/Threat	Low	Medium	High
High (1.0)	Low Risk (1.0 x 1 = 1)	Medium Risk (1.0 x 5 = 5)	High Risk (1.0 x 10 = 10)
Medium (0.5)	Low Risk (5.0 x 1 = 5)	Medium Risk (0.5 x 5 = 2.5)	High Risk (0.5 x 10 = 5)
Low (0.1)	Low Risk (5.0 x 1 = 0.1)	Medium Risk (0.1 x 5 = 0.5)	High Risk (0.1 x 10 = 1)
Risk Scale – Low (0.1 to 1) Medium (>1 to 5) High (>5 to 10)			

5.2 Allegro worksheets

System 1

Allegro Worksheet 8	**CRITICAL INFORMATION ASSET PROFILE**	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Game backend server	Are the core of the gaming infrastructure handles player data, game logic and player interactions. Has an immediate impact on gaming services.	YOUBESOFT Engine, a proprietary game server software, manages player data, game logic, and interactions in online games, ensuring security against service outages, data loss, and unauthorized access.
(4) Owner(s) *Who owns this information asset?*		
YOUBESOFT company		
(5) Security Requirements *What are the security requirements for this information asset?*		
□ **Confidentiality**	Only authorized personnel can view this information asset, as follows: Administrators, Developers, and IT Staff	Customer's sensitive information including payment information, personal information, purchase history and login credentials must be protected from other customers or unauthorized parties.
□ **Integrity**	Only authorized personnel can modify this information asset, as follows: Administrators	Only authorized personnel with appropriate privileges can modify customer data, sensitive information
□ **Availability**	This asset must be available for these personnel to do their jobs, as follows: Administrators, Developers, and IT staff.	

	This asset must be available for 24 hours 365 days.	The YOUBESOFT Engine must be reliably accessible to administrators, developers, and IT staff to maintain uninterrupted gaming services, perform updates, and troubleshoot issues, ensuring optimal performance and user experience.
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows: -	

(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*			
❑ Confidentiality	❑ Integrity	❑ Availability	❑ Other

Allegro - Worksheet 10			**Information Asset Risk Worksheet**
Information Asset Risk	**Threat**	Information Asset	Game-ba**ckend server**
		Area of Concern	*Arbitrary code execution*
		(1) Actor *Who would exploit the area of concern or threat?*	Outside attacker
		(2) Means / Access *How would the actor do it? What would they do?*	Improper validation within the server configurations can lead to arbitrary code execution on the server. This could trigger a system control breach.
		(3) Motive *What is the actor's reason for doing it?*	Deliberate: compromission of game server. Service disruptions.
		(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ❑ **Interruption**

(5) Security Requirements *How would the information asset's security requirements be breached?*	failing to patch and update the server on a regular basis, as well as failing to use secure coding techniques		
(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **80%**	❑ **Medium** **50%**	❑ **Low** **30%**
(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value (Rating from 0 – 10 or sth)**	**Score (Risk value = Prob x value)**
Service disruptions and data breaches can lead to loss of user trust and potential financial losses, affecting reputation and customer confidence.	Reputation & Customer Confidence	9	4.5
	Financial	8	4.0
decreased production while resources are redirected to fix the security breach and bring back services.	Productivity	5	2.5
	Data loss	8	4.0
Possible legal penalties due to non-compliance with data protection regulations.	Fines & Legal Penalties	7	3.5
	Disruption of services	9	4.5
		Relative Risk Score	**23.0**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

□ **Accept**	□ **Defer**	□ [✓ **Mitigate**]	□ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Administrative Controls	Establish clear policies defining who can access and modify the game server and data. Ensure only authorized personnel (administrators, developers, IT staff) have access.
Technical Controls	Use strong authentication methods, such as multi-factor authentication (MFA) and role-based access control (RBAC), to ensure only authorized personnel can access the system.
Residual Risk	Newly discovered vulnerabilities that have not yet been patched could be exploited by attackers.

System 2

Allegro Worksheet 8	**Critical Information Asset Profile**	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Salesforce CRM database	Helps to manage client account relationships and store information.	It's a customer relationship management tool used to manage user accounts with sensitive information about user interactions making it important for securing this database
(4) Owner(s) *Who owns this information asset?*		
YOUBESOFT Entertainment		
(5) Security Requirements *What are the security requirements for this information asset?*		
□ **Confidentiality**	Only authorized personnel can view this information asset, as follows: Administrators	To protect sensitive client information, such as personal details, interaction history, and financial data, access is restricted to administrators. This ensures that confidential information is safeguarded from unauthorized access, reducing the risk of data breaches and privacy violations.
□ Integrity	Only authorized personnel can modify this information asset, as follows: Administrators	Ensuring data integrity means that only administrators with the appropriate privileges can alter client information. This control prevents unauthorized modifications that could lead to data corruption, loss of data integrity, and potential trust issues with clients.

□ **Availability**	This asset must be available for these personnel to do their jobs, as follows: Administrators	To support continuous business operations and client interactions, the CRM database must always be reliably accessible. Ensuring high availability minimizes downtime and maintains consistent service, crucial for effective client relationship management.
	This asset must be available for 24 hours, 365 days.	
□ **Other**	This asset has special regulatory compliance protection requirements, as follows: GDPR	

(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*			
□ Confidentiality	□ [✓ Integrity]	□ Availability	□ Other

Allegro - Worksheet 10			**INFORMATION ASSET RISK WORKSHEET**
Information Asset Risk	**Threat**	Information Asset	Salesforce CRM database
		Area of Concern	*Abuse elevation control mechanism*
		(1) Actor *Who would exploit the area of concern or threat?*	Outsider
		(2) Means / Access *How would the actor do it? What would they do?*	An abuse elevation control mechanisms was found and can lead to unauthorized administrative access to CRM
		(3) Motive *What is the actor's reason for doing it?*	Deliberate
		(4) Outcome *What would be the resulting effect on the information asset?*	□ [✓ **Disclosure**] □ **Destruction** □ [✓ **Modification**] □ **Interruption**
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Not doing regular security checks, not having latest security patches, not enabling SIP, and having a lower macOS version below Sierra+

(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **80%**	❑ **Medium** **50%**	❑ **Low** **30%**
(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value (Rating from 0 – 10 or sth)**	**Score (Risk value = Prob x value)**
Exposure of sensitive customer information could lead to financial loss, reputational damage, and legal repercussions.	Reputation & Customer Confidence	7	3.5
	Financial	7	3.5
Interruption of CRM services could impact customer satisfaction and business productivity.	Productivity	5	2.5
	Data loss	9	4.5
Failure to secure customer data in accordance with regulations could result in fines and penalties.	Fines & Legal Penalties	8	4.0
	Disruption of services	7	3.5
		Relative Risk Score	**21.5**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

☐ **Accept**	☐ **Defer**	[✓ ☐ **Mitigate**]	☐ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Administrative Control	Conduct periodic audits to ensure compliance with security policies and identify any vulnerabilities in the system.
Technical Control	Implement strong authentication methods, such as multi-factor authentication (MFA), and role-based access control (RBAC) to ensure that only authorized administrators can access or modify the database.
Technical Control	Deploy continuous monitoring and logging of database activities to detect and respond to any suspicious behavior or unauthorized access attempts.
Technical Control	Use encryption for data at rest and in transit to protect sensitive client information from unauthorized access and breaches.
Technical Control	Keep the CRM software and underlying systems up to date with the latest security patches and updates to protect against known vulnerabilities.

System 3

Allegro Worksheet 8	**Critical Information Asset Profile**	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Finance management system	Stores important data to help manage businesses financial operations.	It is essential tool for managing payroll processing, invoicing, budgeting, and accounting of the company
(4) Owner(s) *Who owns this information asset?*		
Finance department of YOUBESOFT entertainment		
(5) Security Requirements *What are the security requirements for this information asset?*		
□ **Confidentiality**	Only authorized personnel can view this information asset, as follows: administrators	Access to sensitive financial data and consumer information is restricted to administrators and authorized financial personnel to protect against unauthorized disclosure and ensure data privacy.
□ **Integrity**	Only authorized personnel can modify this information asset, as follows: administrators	To maintain the accuracy and reliability of financial data, only administrators and authorized personnel with the appropriate privileges are allowed to make modifications. This control prevents unauthorized changes that could compromise data integrity.

□ **Availability**	This asset must be available for these personnel to do their jobs, as follows: Administrators and Financial Personnel	Ringing the Salesforce Management System is reliably accessible and always is critical for continuous financial operations, including payroll processing, invoicing, budgeting, and accounting. High availability minimizes downtime and ensures consistent financial management and reporting.
	This asset must be available for 24 hours, 365 days.	
□ **Other**	This asset has special regulatory compliance protection requirements, as follows:	

(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*			
□ Confidentiality	□ Integrity	□ Availability	□ Other

Allegro - Worksheet 10			**Information Asset Risk Worksheet**
Information Asset Risk	**Threat**	Information Asset	Finance management system
		Area of Concern	*SQL injection*
		(1) Actor *Who would exploit the area of concern or threat?*	outsider
		(2) Means / Access *How would the actor do it? What would they do?*	Improper validation within the implementation can lead to SQL injection on the system. This could trigger a Data breach.
		(3) Motive *What is the actor's reason for doing it?*	Deliberate
		(4) Outcome	□ **Disclosure** □ **Destruction**

What would be the resulting effect on the information asset?	□ **Modification**	□ **Interruption**	
(5) Security Requirements *How would the information asset's security requirements be breached?*			
(6) Probability *What is the likelihood that this threat scenario could occur?*	□ **High** **80%**	□ **Medium** **50%**	□ **Low** **30%**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value (Rating from 0 – 10 or sth)**	**Score (Risk value = Prob x value)**
Loss of trust from customers, partners, and stakeholders due to compromised network security and service disruptions.	Reputation & Customer Confidence	9	7.2
	Financial	10	8.0
Significant disclosure of Financial Information.	Productivity	6	4.8
	Data Loss	7	5.6
	Fines & Legal Penalties	9	7.2
	Service Disruption	6	4.8
		Relative Risk Score	**37.6**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

□ **Accept**	□ **Defer**	[✓ □ **Mitigate**]	□ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Administrative Control	Conduct regular training sessions for administrators and financial personnel on security policies, secure handling of sensitive financial data, and awareness of SQL injection threats.
Administrative Control	Perform periodic audits to ensure compliance with security policies and identify any vulnerabilities in the system.
Technical Control	Use encryption for sensitive financial data both in transit and at rest to protect against unauthorized access and breaches.
Technical Control	Implement input validation and parameterized queries to mitigate the risk of SQL injection attacks.
Residual Risk	Despite training, there remains a risk that employees could be tricked by sophisticated social engineering attacks.

System 4

Allegro Worksheet 8	**CRITICAL INFORMATION ASSET PROFILE**	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
asset management system	The Asset Management System is crucial to the organization as it manages and tracks all company assets, ensuring efficient allocation, maintenance, and utilization. This system supports operational efficiency, financial management, and regulatory compliance, making it essential for the organization's overall performance.	The Asset Management System is an essential tool for managing the company's assets, including equipment, infrastructure, and other valuable resources. It facilitates tracking, maintenance scheduling, depreciation calculations, and overall asset lifecycle management, ensuring assets are effectively utilized and maintained.
(4) Owner(s) *Who owns this information asset?*		
IT Department and the Finance Department		
(5) Security Requirements *What are the security requirements for this information asset?*		
□ **Confidentiality**	Only authorized personnel can view this information asset, as follows: Administrators, Finance Department, and IT Staff.	Access to the Asset Management System is restricted to ensure that sensitive information about the company's assets is protected from unauthorized access, which could lead to data breaches and misuse.
□ **Integrity**	Only authorized personnel can modify this information asset, as follows: Administrators and IT Staff.	Ensuring data integrity by allowing only authorized personnel to modify the system prevents unauthorized changes that could compromise the accuracy and reliability of asset data.

□ **Availability**	This asset must be available for these personnel to do their jobs, as follows: Administrators, Finance Department, and IT Staff.	The Asset Management System must be always reliably accessible to support continuous asset tracking, management, and reporting, ensuring operational efficiency and minimal downtime.
	This asset must be available for 24 hours 365 days.	
□ **Other**	This asset has special regulatory compliance protection requirements, as follows:	
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		

□ Confidentiality	□ [✓ Integrity]	□ Availability	□ Other

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET**	
Information Asset Risk	**Threat**	Information Asset	Asset Management System
		Area of Concern	exposed APIs used in the Server Leads to DDoS Attacks
		(1) Actor *Who would exploit the area of concern or threat?*	External Threat Actors
		(2) Means / Access *How would the actor do it? What would they do?*	Use automated tools or botnets to exploit the exposed Report Generating API. By sending a large volume of requests, they can overwhelm the system, causing a denial of service.
		(3) Motive *What is the actor's reason for doing it?*	Deliberate
		(4) Outcome *What would be the resulting effect on the information asset?*	□ **Disclosure** □ **Destruction** □ **Modification** □ [✓ **Interruption**]
		(5) Security Requirements	Unauthorized access to sensitive asset data through the

		How would the information asset's security requirements be breached?	exploited API.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	□ **High** **80%**	□ **Medium** **50%**	□ **Low** **30%**
	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*		(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
			Impact Area	**Value (Rating from 0 – 10 or sth)**	**Score (Risk value = Prob x value)**
	Interruptions in asset tracking and management can lead to operational inefficiencies and delays.		Reputation & Customer Confidence	5	2.5
			Financial	9	4.5
	Exposure of sensitive information related to company assets could compromise competitive advantage and lead to legal repercussions.		Productivity	6	3.0
			Service Disruption	8	4.0
	Failure to secure the system adequately could result in non-compliance with industry regulations, leading to fines and legal actions.		Fines & Legal Penalties	7	3.5
			User Defined Impact Area	5	2.5
				Relative Risk Score	**20.0**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

☐ **Accept**	☐ **Defer**	☐ [✓ **Mitigate**]	☐ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Administrative Controls	Perform periodic audits to ensure compliance with security policies and regulatory requirements, and to identify any vulnerabilities in the system.
Administrative Controls	Establish and maintain an incident response plan to promptly address potential security breaches or data loss incidents.
Administrative Controls	Conduct regular training for administrators and relevant staff on security policies, secure handling of sensitive asset information, and awareness of potential threats.
Technical Controls	Secure APIs by implementing measures such as AWS Shield, Auto Scaling, and AWS CloudWatch. Regularly monitor and debug API code, and fix configuration issues to prevent exploitation.
Technical Controls	Implement regular backup procedures and ensure robust disaster recovery plans are in place to maintain data availability and integrity in case of a system failure or data loss event.
Technical Controls	Use encryption for sensitive data both in transit and at rest to protect against unauthorized access and breaches.

System 5

Allegro Worksheet 8	**CRITICAL INFORMATION ASSET PROFILE**	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Network Infrastructure Routers	The network infrastructure routers are crucial for the organization as they form the backbone of the network, managing and directing data traffic efficiently.	The network infrastructure routers, specifically Cisco ISR 4000 Series Integrated Service Routers (ISR), are used to manage and route data traffic within the organization's network. These routers play a vital role in ensuring network connectivity, performance, and security.
(4) Owner(s) *Who owns this information asset?*		
YOUBESOFT Entertainment		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows: -Network Administrators, IT Security Team, and System Administrators.	Ensuring the confidentiality of the network infrastructure routers is vital to protect sensitive data transmitted over the network. Unauthorized access to router configurations and traffic could result in exposure of confidential.
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows: - Network Administrators and IT Security Team.	Maintaining the integrity of the network infrastructure routers is critical to ensure accurate and reliable network communications. Unauthorized modifications to router settings and data traffic can disrupt normal operations, resulting in data corruption, incorrect routing, and loss of trust in the network's reliability.

□ **Availability**	This asset must be available for these personnel to do their jobs, as follows: Whole IT staff	The availability of network infrastructure routers is essential for the uninterrupted operation of the organization's IT environment. Any disruption or downtime can severely impact business operations, leading to productivity losses, financial damage, and a negative impact on customer satisfaction and trust.
	This asset must be available for 24 hours, 365 days.	
□ **Other**	This asset has special regulatory compliance protection requirements, as follows:	

(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*			
□ Confidentiality	□ Integrity	□ Availability	□ Other

Allegro - Worksheet 10		**Information Asset Risk Worksheet**	
Information Asset Risk	**Threat**	Information Asset	Network Infrastructure Routers
		Area of Concern	The server software is Lack of Regular Updates and Patches
		(1) Actor *Who would exploit the area of concern or threat?*	External Threat Actors
		(2) Means / Access *How would the actor do it? What would they do?*	External attackers could use automated tools to scan for vulnerable Cisco IOS versions and exploit the identified weakness to gain unauthorized access.
		(3) Motive *What is the actor's reason for doing it?*	Deliberate
		(4) Outcome *What would be the resulting effect on the information asset?*	□ **Disclosure** □ **Destruction** □ **Modification** □ **Interruption**
		(5) Security Requirements *How would the information asset's security*	The server software is Lack of Regular Updates and

requirements be breached?	Patches		
(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **80%**	❑ **Medium** **50%**	❑ **Low** **30%**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value (Rating from 0 – 10 or sth)**	**Score (Risk value = Prob x value)**
Significant disruption in network services, affecting business operations, communication, and productivity.	Reputation & Customer Confidence	5	4.0
	Financial	8	6.4
	Data loss	8	6.4
Costs associated with downtime, incident response, and potential regulatory fines due to data breaches.	Productivity	9	7.2
	Disruption of service	9	7.2
Loss of trust from customers, partners, and stakeholders due to compromised network security and service disruptions.	Fines & Legal Penalties	5	4.0
	User Defined Impact Area	5	4.0
		Relative Risk Score	**39.4**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

□ **Accept**	□ **Defer**	□ [✓ **Mitigate**]	□ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Administrative Controls	Perform periodic security audits and vulnerability assessments to ensure compliance with security policies and identify potential weaknesses.
Technical Controls	Implement a rigorous schedule for updating and patching the Cisco IOS to protect against known vulnerabilities.
Technical Controls	Deploy continuous monitoring and logging of network activities to detect and respond to suspicious behavior or unauthorized access attempts.
Technical Controls	Use IDS to detect and prevent potential exploitation of vulnerabilities in network routers.
Technical Controls	Implement network segmentation to isolate critical systems and limit the impact of any potential breach.

5.3 Appendix B

DBMS – Database Management Systems

GBS - Game Backend System

CRM - Customer Relationship Management System

FMS – Financial Management System

AMS - Assets Management System

EF – Exposure Factor (Percentage of asset loss caused by)

SLE – Single Loss Expectancy (Asset Value x EF)

ARO – Annualized Rate of Occurrence (Frequency a threat will occur within a year)

ALE – Annualized Loss Expectancy (SLE x ARO)

Cost/Benefit – (ALE before Safeguard – ALE After Safeguard – Annual Cost of Safeguard)

SANS Guideline for Estimating the Potential Exposure Factor (EF)

Potential Exposure Factor (EF)	Percentage Range
Low Impact	0% - 25%
Moderate Impact	26% - 50%
Significant Impact	51% - 75%
Severe Impact	76% - 100%

6 References

amazon.com. (n.d.). *aws-overview/aws-overview.pdf*. Retrieved from https://docs.aws.amazon.com/pdfs/whitepapers/latest/aws-overview/aws-overview.pdf

attack.mitre.org. (n.d.). *tactics/TA0004/*. Retrieved from https://attack.mitre.org/tactics/TA0004/

attack.mitre.org. (n.d.). *techniques/T1548/006/*. Retrieved from https://attack.mitre.org/techniques/T1548/006/

blog.techprognosis.com. (n.d.). *ebook_Ultimate-Guide-to-Salesforce-Data-Migration.pdf*. Retrieved from https://blog.techprognosis.com/unlocking-cybersecurity-excellence-with-octave-allegro/

cheatsheetseries.owasp.org. (n.d.). *SQL_Injection_Prevention_Cheat_Sheet.html*. Retrieved from https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32862. (n.d.). *CVE-2022-32862*. Retrieved from https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32862

https://insights.sei.cmu.edu/documents/786/2007_005_001_14885.pdf. (n.d.). *2007_005_001_14885.pdf*. Retrieved from https://insights.sei.cmu.edu/documents/786/2007_005_001_14885.pdf

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. (n.d.). *nvlpubs.nist.gov*. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

owasp.org. (n.d.). *owasp-api-security-top-10.pdf*. Retrieved from https://owasp.org/API-Security/editions/2019/en/dist/owasp-api-security-top-10.pdf

prodly.co. (n.d.). *ebook_Ultimate-Guide-to-Salesforce-Data-Migration.pdf*. Retrieved from https://prodly.co/wp-content/uploads/2022/06/ebook_Ultimate-Guide-to-Salesforce-Data-Migration.pdf

resources.docs.salesforce.com. (n.d.). *integration_patterns_and_practices.pdf*. Retrieved from https://resources.docs.salesforce.com/latest/latest/en-us/sfdc/pdf/integration_patterns_and_practices.pdf

www.aquasec.com. (n.d.). *arbitrary-code-execution/*. Retrieved from https://www.aquasec.com/cloud-native-academy/cloud-attacks/arbitrary-code-execution/

www.cisco.com. (n.d.). *4000-series-integrated-services-routers-isr/whitepaper_c11-732909.pdf*. Retrieved from https://www.cisco.com/c/dam/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/whitepaper_c11-732909.pdf

www.cisco.com. (n.d.). *ios-15-5m-t/series.html*. Retrieved from https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-15-5m-t/series.html

www.cloudflare.com. (n.d.). *BDES-2587-Design-Wrap-Refreshed-DDoS-White-Paper-Letter.pdf*. Retrieved from https://www.cloudflare.com/static/d442dfee7ea56f899d8df461bb7a077f/BDES-2587-Design-Wrap-Refreshed-DDoS-White-Paper-Letter.pdf

www.fortinet.com. (n.d.). *eb-best-practices-api-security.pdf*. Retrieved from https://www.fortinet.com/content/dam/fortinet/assets/ebook/eb-best-practices-api-security.pdf

www.salesforce.com. (n.d.). *crm-handbook-2021.pdf*. Retrieved from https://www.salesforce.com/content/dam/web/en_au/www/documents/pdf/crm-handbook-2021.pdf