VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

FALL SEMESTER 2023-24

LAB ASSESSMENT -4

NAME:- Namit Mehrotra

Registration Number:- 21BCE0763

Course Name:- Information Security Analysis and Audit Lab BCSE353E

Slot:- L57+L58

Date:- 13-07-2023

A. Data Backup and Recovery Policy

Policy Statement:
This Data Backup and Recovery Policy outlines the guidelines and procedures for the regular backup, storage, and recovery of data within the higher educational institution, with the goal of ensuring the integrity, availability, and recoverability of critical institutional data in the event of data loss, system failures, or disasters.

1. Purpose:
The goal of this policy is to provide a framework for institutional data backup, storage, and recovery. It attempts to reduce data loss, promote quick restoration of essential systems, guard against data breaches, and assure regulatory compliance.

2. Description:
This policy controls institutional data backup and recovery operations, such as student records, teacher and staff information, research data, financial records, and other vital data. It goes through the methods, responsibilities, and requirements for putting in place a solid backup and recovery system.

3. Defined terms:

a. Data Backup: The practise of making duplicate copies of data and storing them in different places to guard against data loss or corruption.

b. Recovery Point Objective (RPO): The maximum tolerable data loss that an organisation is prepared to suffer after a system failure or data loss event, measured in time.

c. Recovery Time Objective (RTO): The maximum acceptable downtime for essential systems and data, defining the timeframe for restoring systems and data.

4. Prerequisites:

a. Backup Frequency: To maintain data integrity and availability, regular backups of institutional data must be done according to preset backup plans.
Backup data must be securely kept in remote places to defend against physical damage, theft, or natural catastrophes.

c. Backup Media: Backup data must be stored on suitable backup media such as tape drives, network-attached storage (NAS), or cloud-based storage solutions.

d. Encryption: Backup data must be encrypted in transit and at rest using certified encryption methods and protocols.

e. Testing and Validation: Backup and recovery methods must be tested and verified on a regular basis to verify their efficacy and dependability.

f. catastrophe Recovery Plan: In the case of a catastrophe or substantial interruption, a complete disaster recovery plan describing processes for restoring essential systems and data must be prepared.

5. Client Protection:
a. User Awareness: Clients must be informed on the need of data backup as well as the processes for protecting their own data.

b. Data Integrity: It is the responsibility of the client to ensure the correctness and integrity of their data before it is backed up.

6. Server Protection:
a. Access Controls: To prevent unauthorised access or manipulation, servers hosting backup data must be secured by proper access controls.

b. Redundancy and Fault Tolerance: To maintain data availability, backup servers and storage systems must be constructed with redundancy and fault tolerance techniques.

7. Policy Compliance:
This policy applies to all members of the higher education institution, including professors, staff, and students. Failure to comply may result in disciplinary action and the loss of data access rights.

8. Responsibilities:

Name	Responsibility
Chief Information Officer (CIO)	Policy Owner and overall responsibility for data backup and recovery
Director of IT Operations	Implementation and oversight of backup and recovery procedures
Data Owners and Stewards	Identifying critical data, determining appropriate backup schedules, and ensuring data integrity
IT Security TeamEnsuring	proper encryption of backup data and adherence to security controls
System Administrators	Performing regular backups, monitoring backup systems, and managing backup media
Disaster Recovery Team	Developing and maintaining the disaster recovery plan, including data recovery procedures
IT Help Desk	Assisting end-users with data recovery requests and providing support for backup-related issues
Internal Audit Team	Auditing and assessing compliance with data backup and recovery policies
Data Center Facilities Team	Ensuring the physical security and environmental controls of backup media and storage locations
End-users	Complying with backup and recovery procedures, reporting any data loss incidents promptly
Data Backup and Recovery Specialist	Managing and executing backup and recovery operations,

9. Attachments and Related Documents:

a. Disaster Recovery Plan
b. Data Classification and Handling Policy
c. Information Security Policy
d. Incident Response Plan

Conclusion:

This Data Backup and Recovery Policy defines the principles and methods for guaranteeing crucial institutional data availability and recoverability. By following these principles, the higher education institution may safeguard its data assets, reduce data loss, and guarantee operational continuity in the event of a system failure or catastrophe.

b) Anti-Virus and Malware Protection Policy

Policy Statement:
This Anti-Virus and Malware Protection Policy explains the standards and processes for safeguarding the systems and networks of the higher educational institution against viruses, malware, and other dangerous threats. By deploying appropriate antivirus and malware protection methods, the policy strives to preserve the integrity, availability, and confidentiality of institutional data.

1. Purpose:
The aim of this policy is to provide a framework for deploying effective antivirus and malware prevention methods. The policy attempts to secure the institution's systems, networks, and data assets by preventing and mitigating the risks associated with viruses, malware, and other dangerous threats.

2. Description:
This policy controls the installation, setup, and upkeep of antivirus and malware protection systems inside the higher education institution. It describes the roles, responsibilities, and processes required to guard against viruses, malware infections, and other cyber threats.

3. Definitions:
a. Virus:
A computer programme that replicates itself and spreads to other computers, possibly causing harm or unauthorised behaviour.

b. Malware:
Malicious software such as viruses, worms, ransomware, spyware, and other malicious programmes that are meant to disrupt or compromise systems and data.

4. Prerequisites:
a. Antivirus and Malware Protection Software:
All computers and devices connected to the institutional network must have credible antivirus and malware protection software installed.

b. Regular Updates:
In order to identify and block new threats, antivirus and malware protection software must be maintained up to date with the most recent virus definitions and security updates.

c. Scanning and Detection:
System, file, and incoming data must be scanned on a regular basis to identify and minimise virus and malware infestations.

d. Quarantine and Removal: Infected files or systems must be quarantined immediately, and necessary steps must be taken to remove viruses, malware, or other dangerous software.
a. Safe Internet Practises: Users must practise safe internet practises, such as not downloading files from unknown sources and exercising caution when opening email attachments or clicking on suspicious links.

f. User Awareness and Training: Users should be educated on prevalent malware dangers, social engineering tactics, and recommended practises for preventing infestations via regular awareness programmes.

g. System and software updates: Applying security updates and patches to operating systems, apps, and firmware on a regular basis helps defend against known vulnerabilities exploited by malware.

h. Network Segmentation: Using network segmentation separates key systems and minimises malware transmission in the event of an attack.

i. Incident Response: Creating a strategy for reporting, containing, and managing virus and malware occurrences.

j. Security Monitoring: Constantly monitoring network traffic and system records for suspicious activity or symptoms of malware infestation.

5. Client Protection:
a. Users are responsible for protecting their computers by installing and updating certified antivirus and malware protection software.

b. Users must notify the IT Help Desk or authorised security contact immediately of any suspicious actions, suspected malware infections, or security events.

6. Server Protection:

a. Antivirus and malware protection software must be installed and routinely updated on servers hosting vital systems and services.

b. To prevent servers from unauthorised access and possible malware infections, access restrictions and system hardening measures must be established.

7. Policy Compliance:
This policy applies to all members of the higher education institution, including professors, staff, and students. Noncompliance may result in disciplinary action and eventual system access limitations.

8. Responsibilities:

Name	Responsibility
Chief Information Officer (CIO)	Policy Owner and overall responsibility for antivirus and malware protection
IT Security Team	Implementation and management of antivirus and malware protection systems
Director of IT Operations	Monitoring and updating antivirus and malware protection software and configurations
End-users	Adhering to antivirus and malware protection policies, promptly reporting suspicious activities or potential threats
System Administrators	Managing antivirus and malware protection systems, including software deployment and updates
IT Help Desk	Providing support for antivirus and malware related issues, assisting with malware detection and removal
Security Incident Response Team	Responding to and managing antivirus and malware incidents, conducting investigations and mitigation
Internal Audit Team	Auditing and assessing compliance with antivirus and malware protection policies
IT Procurement Team	Ensuring procurement of reliable and up-to date antivirus and malware protection solutions
Network Administrators	Implementing network-level controls and monitoring to detect and block malicious activities
Information Security Awareness Team	Conducting training and awareness programs to educate users about antivirus and malware protection best practices
Software Developers	Integrating secure coding practices and implementing safeguards to prevent malware vulnerabilities in applications
Data Owners and Stewards	Ensuring appropriate protection measures for data against viruses and malware
Third-Party Vendors	Ensuring compliance with antivirus and malware protection requirements for vendor provided systems and services

9. Attachments/Related Documents:
a. Information Security Policy
b. Incident Response Plan
c. User Awareness Training Materials
d. Policy on Software Patching e. Policy on Access Control

Conclusion:
The Anti-Virus and Malware Protection Policy establishes a framework for efficiently safeguarding the higher education institution's systems, networks, and data assets from viruses, malware, and other dangerous threats. The institution can reduce the risk of infection, preserve data integrity, and protect the confidentiality and availability of essential information resources by adhering to this policy.

c) Email Policy

Policy Statement:
The norms and procedures for the proper and secure use of email inside the higher educational institution are outlined in this Email Policy. The policy's goal is to protect the confidentiality, integrity, and availability of institutional email communications while also encouraging professional and responsible usage.

1. purpose:
The goal of this policy is to set standards for the use of email inside the higher education institution in order to ensure effective communication, secure sensitive information, and mitigate risks associated with abuse, unauthorised access, and data breaches.

2. Policy Summary:
This policy covers the usage of institutional email accounts and applies to all academics, staff, students, and other authorised users who use institutional email services. It covers appropriate email use, security measures, data protection, and the obligations that come with it.

3. Definition:

a. Institutional Email: Email services given by a higher learning institution, such as official email accounts issued to teachers, staff, students, and authorised users.

b. Confidential Information: Sensitive information that must be protected from unauthorised access, disclosure, or modification.

c. Spam: Unwanted and unsolicited email communications, sometimes of a commercial or harmful character.

4. Expectations:

a. **Authorised Use:** Institutional email accounts must be used for official academic, administrative, and business correspondence.

b. **User Identification:** When sending email messages, users must correctly identify themselves by giving their complete name and contact information.

c. **Proper Email Etiquette:** When interacting inside and outside the institution, users must maintain a professional tone and follow proper email etiquette.
d. **Confidentiality:** where transmitting confidential information over email, users must exercise care and take adequate precautions to secure sensitive data, such as utilising encryption where required.

e. **Data Retention:** Users must follow institutional data retention rules and email storage and archiving recommendations.

f. **Anti-Spam Measures:** The institution must adopt and maintain anti-spam filters and anti-spam measures to reduce the effect of spam emails.

g. **Security Awareness:** Users must be trained and educated on recommended practises for email security, such as recognising and avoiding phishing efforts, suspicious attachments, and social engineering tactics.

h. **Virus Protection:** All email accounts and computers must be equipped with current antivirus software to identify and prevent the propagation of viruses and malware through email attachments or links.

i. **Email Monitoring:** The institution retains the right to monitor email use for security and compliance reasons, to ensure policy and regulatory conformity.

5. **Client Security:**

a. Users are responsible for securing their email accounts by using strong passwords, changing them on a regular basis, and not sharing login information.

b. Users must immediately report any suspected email-based security issues, phishing attempts, or unauthorised email account access.

a. Email servers must be safeguarded with proper security measures, such as firewalls, access restrictions, and intrusion detection systems.

b. Email servers must get regular security upgrades and patches to fix vulnerabilities and safeguard against email-based attacks.

6. **Server Protection:**

a. Email servers shall be protected with appropriate security controls, including firewalls, access controls, and intrusion detection systems.

b. Regular security updates and patches shall be applied to email servers to address vulnerabilities and protect against email-based threats.

7. **Compliance with Policy:**

All users of institutional email services are required to comply with this policy. Non- compliance may result in disciplinary action, loss of email privileges, and potential legal consequences.

8. Responsibilities:

Name	Responsibilities
Chief Information Officer (CIO)	Policy Owner and overall responsibility for email usage and security.
IT Department	Management and maintenance of email systems, implementation of security measures, and providing user support.
System Administrators	Configuration, monitoring, and maintenance of email servers and security controls.
Users	Adherence to email policy, responsible use of email services, protection of login credentials, and reporting any security incidents or concerns.
IT Help Desk	Support for email-related issues, assisting users with email setup, configuration, and troubleshooting.
Information Security Officer	Ensuring compliance with email security policies, monitoring email usage, and conducting periodic security assessments.
Network Administrators	Network-level protection for email services, implementing firewalls, intrusion detection systems, and monitoring for email-based threats.
Internal Audit Team	Auditing and assessing compliance with email policy and security controls.
Data Owners and Stewards	Ensuring appropriate protection and handling of confidential information sent via email.
Security Awareness Team	Providing training and education on email security best practices, raising awareness about phishing attempts and email-based threats.
Legal and Compliance Team	Ensuring compliance with data protection regulations, privacy laws, and industry standards regarding email communications.
Human Resources	Communicating and enforcing the email policy within the organization, including onboarding and training employees on acceptable email usage.
Internal Communications Team	Disseminating official communications through email channels, ensuring compliance with branding and messaging guidelines.

9. Related Documents/Attachments:

a. Information Security Policy

b. Data Classification and Handling Policy

c. Acceptable Use Policy

d. Incident Response Plan

e. Email Encryption Policy (if applicable)

Conclusion:
The Email Policy establishes guidelines for the appropriate and secure use of institutional email services. By adhering to this policy, the higher educational institution can ensure effective communication, protect sensitive information, and mitigate risks associated with unauthorized access, data breaches, and misuse of email resources.

d) Access Control Policy

Policy Statement:
This Access Control Policy outlines the guidelines and procedures for managing access to the information systems and data within the higher educational institution. The policy aims to ensure the confidentiality, integrity, and availability of institutional resources by implementing appropriate access controls and authorization mechanisms.

1. Purpose:
The purpose of this policy is to establish a framework for granting and managing access to institutional systems, networks, and data. The policy aims to prevent unauthorized access, protect sensitive information, and ensure compliance with applicable laws and regulations.

2.Description:
This policy governs the access control mechanisms and procedures within the higher educational institution. It covers the principles and practices for granting, managing, and revoking user access to institutional resources, including systems, applications, data, and physical facilities.

3. Definitions:

a. Access Control: The process of granting or restricting permissions to users, allowing them to access specific resources based on their roles, responsibilities, and the principle of least privilege.

b. Authentication: The process of verifying the identity of an individual or system attempting to gain access to resources.

c. Authorization: The process of granting specific permissions and privileges to an authenticated user based on their role and responsibilities.

d. Principle of Least Privilege: Granting users the minimum necessary access rights and permissions required to perform their job functions.

4. Requirements:

a. User Identification and Authentication: Users shall be assigned unique user IDs and required to authenticate themselves using strong passwords or other approved authentication methods.

b. Access Control Mechanisms: Access controls, such as role-based access control (RBAC), access control lists (ACLs), or attribute-based access control (ABAC), shall be implemented to manage and enforce access permissions.

c. User Access Provisioning and Deprovisioning: User access rights shall be provisioned based on job roles and responsibilities. Access rights shall be promptly revoked or modified upon employee termination, role changes, or access policy violations.

d. Regular Access Reviews: Periodic access reviews shall be conducted to ensure that users have appropriate access rights and to identify and remove any unnecessary or outdated permissions.

e. Multi-factor Authentication (MFA): MFA shall be implemented for privileged accounts and access to sensitive systems and data, adding an extra layer of security beyond passwords.

f. Physical Access Controls: Physical access controls, such as card-based entry systems, locks, and surveillance cameras, shall be implemented to restrict unauthorized physical access to critical areas and facilities.

g. Logging and Monitoring: Access control systems shall log access attempts and events for auditing and monitoring purposes, enabling the detection of unauthorized access or suspicious activities.

h. Access Control Policies for Third-Party Users: Access controls shall be extended to third-party vendors, contractors, and other external entities granted access to institutional resources.

i. Separation of Duties: Critical functions, such as system administration, shall be separated to prevent unauthorized actions or conflicts of interest.

j. Access Control Training and Awareness: Training programs shall be provided to educate users on access control policies, procedures, and best practices.

5. Client Protection:

a. Users must protect their login credentials, keep passwords confidential, and promptly report any suspected unauthorised access or account compromise.

b. When not in use, users must log out or lock their systems to prevent unauthorised access.

6. Server Protection:

a. Servers hosting institutional systems and data must be protected with appropriate security controls, such as firewalls, intrusion detection systems, and regularly updated patches.

b. Access controls on servers must be configured to limit and monitor access to sensitive data and system resources.

7. Policy Compliance:

This policy applies to all users of institutional systems and data. Noncompliance may result in disciplinary action, loss of access rights, and legal ramifications.

8. Responsibilities:

Name	Responsibilities
Chief Information Officer (CIO)	Policy Owner and overall responsibility for access control.
IT Security Team	Development, implementation, and enforcement of access control policies and measures.
System Administrators	Configuration and maintenance of access control mechanisms on systems and applications.
Network Administrators	Implementation and management of network-level access controls, including firewalls and network segmentation.
Data Owners and Stewards	Identifying and classifying data, determining appropriate access controls, and managing access permissions.
Human Resources IT Help Desk	Collaborating with IT to ensure appropriate access provisioning and revocation during the employee lifecycle. Provisioning and deprovisioning user accounts and assisting users with access related issues and requests.
Employees	Adhering to access control policies, using only authorized accounts, and reporting any suspicious or unauthorized access attempts.
Data Custodians	Ensuring the security and integrity of data within their respective areas of responsibility, implementing access controls accordingly.
Security Incident Response Team	Investigating and responding to security incidents related to unauthorized access or breaches.
Internal Audit Team	Auditing and assessing compliance with access control policies and monitoring access-related activities.
Compliance Officer	Ensuring compliance with relevant laws, regulations, and industry standards regarding access control and data protection.
IT Procurement Team	Evaluating and selecting access control tools and solutions that align with policy requirements.

8. Additional Documents/Attachments:

- Policy on Information Security
- Policy on Data Classification and Handling - Policy on Acceptable Use
- Incident Response Plan - Procedures for User Access Management
- Policy on Physical Security

Conclusion:

The Access Control Policy outlines the methods and principles for regulating access to institutional systems, networks, and data. The higher education institution may prevent unauthorised access, secure sensitive information, and guarantee compliance with relevant laws and regulations by adhering to this policy. Access controls help to ensure the confidentiality, integrity, and availability of institutional resources.

e) Firewall Policy

Statement of Policy :
This Firewall Policy describes the standards and processes for configuring, managing, and using firewalls inside the higher education institution. The policy's goal is to create an effective network security perimeter by adopting suitable firewall rules to prevent unauthorised access, network threats, and data breaches.

1. Purpose:
This policy defines the standards and practises for the implementation, configuration, and administration of firewalls inside the higher education institution. The policy strives to protect sensitive information and mitigate possible risks by ensuring the security and integrity of the institution's networks and systems.

2. Description:
This policy covers the use of firewalls to provide a secure network perimeter by regulating and monitoring network traffic that enters and exits the institution's networks. It explains how to configure, install, monitor, and maintain firewalls to guard against unauthorised access, network-based threats, and possible vulnerabilities.

3. Definitions:
a. A firewall is a network security device that monitors and filters network traffic according to specified security rules in order to safeguard networks and systems from unauthorised access and possible threats.

b. Network Perimeter: The line that separates an organization's internal network from external networks, such as the internet, and where firewalls are often implemented.

4. Prerequisites:

a. Firewall Deployment: To construct a secure network perimeter, firewalls must be implemented at all network ingress and egress points, including internet gateways and links to external networks.

b. Configuration and Rule Set: Firewalls must be designed to implement the concept of least privilege, permitting only authorised traffic based on predetermined security rules and access control lists (ACLs).]

c. Regular upgrades and Patching: Firewalls must be updated with the most recent firmware, security patches, and vendor upgrades to fix vulnerabilities and guard against new threats.

d. . Monitoring and Logging: Firewalls must be set to create logs and monitor network traffic for possible security events, intrusion attempts, and policy breaches.

e. Network Segmentation: Firewalls must be used to separate internal networks depending on security needs, prohibiting unauthorised access between network segments and mitigating the consequences of any breaches.

f. Remote Access: Using strong authentication and encryption, firewalls must be set to manage and protect remote access to internal networks, including virtual private network (VPN) connections.

g. Denial of Service (DoS) Protection: Firewalls must be designed to detect and block excessive traffic or suspicious behaviour in order to mitigate and prevent DoS assaults.

Changes to firewall settings must go through a systematic change management procedure to guarantee adequate testing, approval, and documentation.

i. Incident Response: Security issues must be monitored by firewalls, and suitable response mechanisms must be in place to handle possible breaches or unauthorised access attempts.

j. Vendor assistance and Maintenance: Firewalls must be maintained by the vendor or authorised third-party suppliers, who must offer technical assistance, software updates, and patches.

5. Client Safety:

a. When using the internet and external networks, users must adhere to the institution's acceptable usage policy, avoiding behaviours that may jeopardise network security or breach rules.

6. Server Protection:

Firewalls must be configured to manage incoming and outgoing traffic to and from servers, ensuring that only authorised and essential network connections are permitted.

7. Policy Compliance:

This policy applies to all users and administrators of the higher educational institution's networks and systems. Noncompliance may result in disciplinary action, loss of network access rights, and legal ramifications.

8. Responsibilities:

Name	Responsibilities
Chief Information Officer (CIO)	Policy Owner and overall responsibility for firewall implementation and management.
IT Security Team	Designing, configuring, and monitoring firewall controls, enforcing policy compliance, and conducting firewall-related risk assessments.
Network Administrators	Configuring and maintaining firewall devices, monitoring firewall logs and traffic, and implementing firewall rules and policies.
System Administrators	Ensuring server configurations align with firewall rules, policies, and best practices.
IT Help Desk	Assisting users with firewall-related issues and inquiries, including troubleshooting firewall connectivity or access issues.
Users	Complying with firewall policies and procedures, reporting any suspected security incidents or policy violations.
Incident Response Team	Monitoring firewall logs, investigating and responding to firewall-related security incidents or breaches.
Internal Audit Team	Auditing and assessing compliance with firewall policies, rules, and configuration standards.
Compliance Officer	Ensuring compliance with relevant laws, regulations, and industry standards regarding firewall implementation and management.

9. Additional Documents/Attachments:

- Policy on Information Security
- Policy on Network Segmentation
- Policy on Acceptable Use
- Incident Response Plan - Policy on Change Management

Conclusion:

The Firewall Policy defines standards and processes for configuring, managing, and deploying firewalls inside the higher education institution. By following this policy, the institution may create a secure network perimeter, defend against unauthorised access and network-based risks, and protect sensitive data. Proper firewall controls help to keep the institution's networks and systems secret, secure, and up and running.

B) Risk Assessment Report

ASSESSING AZURE SENTINEL CAPABILITIES FOR COFCO INTERNATIONAL

1. Introduction and Overview:

The Azure Sentinel capabilities for COFCO International, a significant agriculture corporation, are evaluated in this risk assessment study. The purpose of the evaluation is to identify possible risks, strengths, and weaknesses associated with using Azure Sentinel as a security information and event management (SIEM) system. The outcomes of this study will assist COFCO International in making educated choices about the deployment and use of Azure Sentinel.

2. Members of the team:

The risk assessment team is made up of the following individuals:

- Information Security Analyst: Oversee the risk assessment process, including data gathering, analysis, and report writing.
- IT Operations Manager: Provide knowledge of current infrastructure and systems.
- Security Architect: Evaluate security measures and Azure Sentinel compatibility.
- Compliance Officer: Assess compliance concerns.
- IT Security Engineer: Contribute technical skills to the evaluation of the Azure Sentinel solution.

3. Risk Assessment Report:

The conclusions of the risk assessment undertaken for the Azure Sentinel deployment at COFCO International are presented in this report. The study contains an analysis of possible hazards, their effect, and mitigation strategies for the identified risks.

4. Responsibilities:

a. Data Collection:

- Examine current infrastructure and system documentation.
- Identify stakeholders and conduct interviews to elicit information.
- Examine the documentation and specs for Azure Sentinel.

b. Phase of System Documentation:

Document existing systems, network architecture, and infrastructure.

- Identify possible integration and compatibility issues.
- Examine current security measures for compliance with Azure Sentinel criteria.

c. Phase of Risk Determination:

Examine the possible hazards connected with Azure Sentinel installation.

- Evaluate the effect of identified threats on the security posture of the organisation.
- Assess each risk's probability and possible repercussions.

D. Phase of Safeguard Determination:

- Propose safeguard strategies to lessen the identified risks.
- Make advice on how to establish security measures and best practises.
- Develop a strategy for monitoring and reevaluating the efficacy of the safeguards.

5. System Documentation Phase:

During this phase, the risk assessment team analysed COFCO International's current systems, network architecture, and infrastructure documentation. The team highlighted possible integration points and compatibility issues that might occur during the Azure Sentinel installation.

6. Risk Determination Phase:

Based on the data gathered and the analysis performed, the risk assessment team identified possible hazards related with COFCO International's Azure Sentinel installation. The risks were evaluated based on their influence on the security posture of the organisation, chance of occurrence, and possible repercussions.

7. Safeguard Determination step:

The risk assessment team offered safeguard methods to minimise the identified hazards during this step. These precautions include:

- Thorough compatibility testing and system integration planning.
- An all-encompassing data input method, including validation and quality control techniques.
- Strong threat detection and response structure, with rules and processes that are frequently updated.
- Thorough automation and orchestration settings, with enough management and monitoring.
- Compliance measures that are in line with industry rules and data protection legislation.
- Comprehensive user training and continuous support for Azure Sentinel's successful usage.

1.0 System Documents PhRisk Assessment Process:

1. System Documentation Phase:

During this phase, the risk assessment team acquires and examines documents pertaining to COFCO International's systems and infrastructure. This includes the following:

- System Inventory: Identifying and documenting the systems and components that comprise the infrastructure of the organisation.
- Network Architecture: Documenting the network structure, connectivity, and system dependencies.
- System Configuration: Gathering information about the system's configuration settings and parameters.
- System Interfaces: Identifying the systems' exterior and internal interfaces, as well as linkages to other systems or networks.
- Data Flows: Identifying essential data assets and understanding the movement of data inside systems.

2. System Identification:

In this phase, each system within the COFCO International infrastructure is identified and documented. The following information is recorded for each system:

System Name	**The name or identifier assigned to the system.**
System Purpose and Description	**A brief explanation of the system's purpose and its intended functionality within the organization.**
System Owner	**The individual or department responsible for the management and operation of the system.**
-System Security Level	**The assigned security level or classification of the system, indicating the sensitivity and criticality of the data and operations it handles.**

3. Risk Identification and Analysis:

Once the systems are identified, the risk assessment team proceeds with the identification and analysis of potential risks and vulnerabilities. This involves:

- Threat Identification: Identifying potential threats that could exploit vulnerabilities within the systems.
- Vulnerability Assessment: Assessing the weaknesses and vulnerabilities within the systems that could be exploited by threats.
- Risk Analysis: Evaluating the likelihood and impact of identified risks, considering factors such as the probability of occurrence, potential consequences, and existing controls.

4. Safeguard Determination:

Based on the identified risks, the risk assessment team determines appropriate safeguards to mitigate or manage the risks effectively. This includes:

- Control Recommendations: Providing recommendations for implementing security controls, such as access controls, encryption, monitoring mechanisms, and incident response procedures.
- Risk Treatment Plan: Developing a plan that outlines the specific actions required to implement the recommended controls and mitigate the identified risks.
- Risk Acceptance: Assessing risks that may be accepted based on business or operational requirements, while ensuring appropriate risk management measures are in place.

5. Ongoing Monitoring and Review:

The risk assessment process is not a one-time activity. It should be conducted periodically to account for changes in systems, technology, and threats. Ongoing monitoring and review ensure that risks are continuously identified, assessed, and addressed to maintain an effective security posture.

2.0 Risk determination process

The goal of the Risk Determination Phase is to calculate the level of risk for each threat / vulnerability pair based on the likelihood of a threat exploiting a vulnerability, and the severity of impact that the exploited vulnerability would have on the system, its data and its business function. Consider the impact in terms of loss of confidentiality, integrity or availability of the data classified in Task 1.3.

Information will be collected in the form of questionnaires, interviews, documentation review, and automated scanning tools.

The Risk Determination Phase is comprised of six steps:

I. Identify potential dangers to information and system (threats).
II. Identify the system weakness that could be exploited (vulnerabilities) associated to generate the threat / vulnerability pair.
III. Identify existing controls to reduce the risk of the threat exploiting the vulnerability.
IV. Determine the likelihood of occurrence for a threat exploiting a related vulnerability given the existing controls.
V. Determine the severity of impact on the system by an exploited vulnerability.
VI. Determine the risk level for a threat/vulnerability pair given the existing controls.

This six-step process for Risk Determination is conducted for each identified threat / vulnerability pair. Use the Risk Determination Table in Appendix D to document the analysis performed in this phase.

2.1 Identify Threats and Vulnerabilities

First, identify threats that could exploit system vulnerabilities. Refer to the *CMS Threat Identification Resource* (www.cms.hhs.gov/it/security/docs/ Threat_ID_resource.pdf) for possible environmental, physical, human, natural, and technical threats. Using the output of task 1.2, consider the system's connections, dependencies with other systems, inherited risks and controls, risks from software faults and staff errors and malicious intent, and such factors as proximity to the Internet, incorrect file permissions, risks from maintenance procedures and personnel changes.

Next, consider the potential vulnerabilities associated with each threat, to produce a pair. A vulnerability can be associated with one or more threats. Collect input from previous risk assessments, audits, system deficiency reports, security advisories, scanning tools, security test results, system development testing, industry and government listings, such as sans.org, securityfocus.com, vendor advisories, and the NIST vulnerability database at icat.nist.gov.

Task 2.1:	Descriptions of threat/vulnerability pairs.
Key Team Member	System administrator Technical reviewer System technical owner
Output:s:	Complete the "Item No.", "Threat Name" and "Vulnerability Name" columns in *2.0 Risk Determination* table in Appendix D.

2.2 Describe Risks

Describe how each vulnerability creates a risk to the system in terms of confidentiality, integrity, availability, auditability or accountability elements that may result in a compromise of the system.

Task 2.2:	Describe risks in relation to threat/vulnerability pairs.
Key Team Members:	System administrator Technical reviewer System technical owner
Output:	Complete the "Risk Description" column of the *2.0 Risk Determination* table in Appendix D.

2.3 Identify Existing Controls

Identify existing controls that reduce the likelihood or probability of a threat exploiting a system vulnerability, and/or reduce the magnitude of impact of the exploited vulnerability on the system. Existing controls may be management, operational or technical controls depending on the threat / vulnerability and the risk to the system.

Task 2.3:	Description of system controls, cross-referenced with threat / vulnerability pairs.
Key Team Members:	System administrator Technical reviewer System technical owner
Output:	Complete the "Existing Controls" column of *2.0 Risk Determination* table in Appendix D.

2.4 Determine Likelihood of Occurrence

Estimate the likelihood that a threat will exploit a vulnerability. Likelihood of occurrence is based on a number of factors that include system architecture, system environment, information system access and existing controls; the presence, motivation, tenacity, strength and nature of the threat; the presence of vulnerabilities; and the effectiveness of existing controls.

Refer to this table to when estimating the likelihood that the threat will be realized and exploit the vulnerability on the system.

	likelihood of Occurrence Levels
Likelihood	**Description**
Negligible	Unlikely ever to occur
Very Low	Likely to occur two/three times every five years
Low	Likely to occur once every year or less
Medium	Likely to occur once every six months or less
High	Likely to occur once per month or less
Very High	Likely to occur multiple times per month
Extreme	Likely to occur multiple times per day

Task 2.4:	Threat / vulnerability pairs with likelihood of successful exploitation.
Key Team Members:	System administrator Technical reviewer System technical owner
Output:	Categorize threat / vulnerability pairs by likelihood of occurrence, complete the "Likelihood of Occurrence" column of *2.0 Risk Determination* table in Appendix D.

2.5. Determine Severity of Impact

Determine the magnitude or severity of impact on the system's operational capabilities and the information it handles, if the threat is realized and exploits the associated vulnerability. Determine the severity of impact for each threat / vulnerability pair by evaluating the potential loss in each security category (confidentiality, integrity, availability, auditability, accountability) based on the system's information security level as explained in Appendix A.

	Impact Severity Levels
Insignificant	Little or no impact
Minor	Minimal effort to repair, restore or reconfigure
Significant	Small but tangible harm, maybe noticeable by a limited audience, some embarrassment, some effort to repair
Damaging	Damage to reputation, loss of confidence, significant effort to repair
Serious	Considerable system outage, loss of connected customers, business confidence, compromise of large amount information
Critical	Extended outage, permanent loss of resource, triggering business continuity procedures, complete compromise of information
Task 2.5:	Threat / vulnerability pairs with severity of successful exploitation.
Key Team Members:	System administrator Technical reviewer System technical owner System business owner
Output:	Categorize threat / vulnerability pairs by severity or magnitude of impact, and complete the "Impact Severity" column of *2.0 Risk Determination* table in Appendix D.

2.6 Determine Risk Levels

Risk level is the likelihood of occurrence multiplied by the severity of impact. The final value is subject to the system business and technical owners' discretion.

Risk determination
For each threat / vulnerability pair, assess the following:

- Likelihood of the threat attempting to exercise the vulnerability;
- Magnitude of impact if the threat / vulnerability exploit is successful;
- Adequacy of planned or existing security controls for reducing or eliminating risk;

Note: The project team must decide whether to use only currently implemented controls for this analysis, or to include controls that are budgeted and scheduled for installation, and document that decision in the Report.

- Resulting risk to the information on the system from the threat and vulnerability.

This table shows the resulting risk level, for each degree of likelihood and each level of severity.

Risk Levels

Likelihood of Occurrence.	Impact Severity					
	Insignificant	Minor	Significant	Damaging	Serious	Critical
Negligible	Low	Low	Low	Low	Low	Low
Very Low	Low	Low	Low	Low	Moderate	Moderate
Low	Low	Low	Moderate	Moderate	High	High
Medium	Low	Low	Moderate	High	High	High
High	Low	Moderate	High	High	High	High
Very High	Low	Moderate	High	High	High	High
Extreme	Low	Moderate	High	High	High	High
Task 2.6:	Threat / vulnerability pairs with assigned risk levels.					
Key Team Member s:	System administrator Technical reviewer System technical owner System business owner					
Output:	Combine the likelihood of occurrence with magnitude of impact to derive the risk level for each threat / vulnerability pair. Consider the risks to the information on the system, and complete the "Risk Level" column of *2.0 Risk Determination* table in Appendix D.					

3.0 Safeguard Determination Phase

The safeguard determination phase involves identification of additional controls, safeguards or corrective actions to minimize the threat exposure and vulnerability to exploitation for each threat/ vulnerability pair with a moderate or high risk level. The residual risk level is the amount of risk that would remain if the recommended control or safeguard were implemented.

Safeguard determination steps:

- Identify controls and safeguards to reduce the risk level of each risk-threat pair, if the risk level is moderate or high.
- Determine the residual likelihood of occurrence of the threat if the recommended safeguard is implemented.
- Determine the residual impact severity of the exploited vulnerability once the recommended safeguard is implemented.
- Determine the residual risk level for the system.
- Consider safeguards related to testing and maintenance, improved audit capability, and restricting physical access.

3.1 Recommend Controls and Safeguards

Identify controls and safeguards to reduce the risk presented by each threat / vulnerability pair with a moderate or high risk level as identified in the Risk Determination Phase. When identifying a control or safeguard, consider:

- Security area where it belongs, such as management, operational, technical.
- Method it employs to reduce the opportunity for the threat to exploit the vulnerability.
- Its effectiveness in mitigating the risk to information.
- Policy and architectural parameters required for its implementation in the environment.
- Information security category (confidentiality, integrity, availability, access control, audit, etc.) to which the safeguard applies.
- Whether the cost of the safeguard is commensurate with its reduction in risk.
- If more than one safeguard is identified for the same threat / vulnerability pair, list them in this column in separate rows and continue with the analysis steps. The residual risk level must be evaluated during this phase of the assessment and may be further evaluated in risk management activities outside the scope of this project.
- If the recommended safeguard cannot be completely implemented in the environment due to cost, management, operational or technical constraints, document the circumstances and continue with the analysis.
- Consider control elements implemented as policies and procedures, training, and improved policy enforcement.

Task 3.1:	Create a list of current, planned or available safeguards and controls suitable for protecting the information
Key Team Members:	System administrator System technical owner Technical reviewer
Output:	List of safeguards and controls, with implementation considerations. Complete the "Recommended Safeguard" column in *3.0 Safeguard Determination* table in Appendix D.

3.2 Determine Residual Likelihood of Occurrence

Follow the directions in section 2.4 of the Risk Determination phase, while assuming the selected safeguard has been implemented.

Task 3.2:	Categorize threat / vulnerability pairs by likelihood of occurrence, assuming the selected safeguard has been implemented.
Key Team Members:	System administrator Technical reviewer System technical owner
Output:	Complete the "Residual Likelihood of Occurrence" column of *3.0 Safeguard Determination* table in Appendix D.

3.3 Determine Residual Severity of Impact

Follow the directions in section 2.5 of the Risk Determination phase while assuming the selected safeguard has been implemented.

Task 3.3:	Categorize threat / vulnerability pairs by severity or magnitude of impact of a successful exploitation, assuming the selected safeguard has been implemented.
Key Team Members:	System administrator Technical reviewer System technical owner System business owner
Output:	Complete the "Residual Impact Severity" column of *3.0 Safeguard Determination* table in Appendix D.

3.4 Determine Residual Risk Levels

Determine the residual risk level for the threat/vulnerability pair and its associated risk once the recommended safeguard is implemented. The residual risk level is determined by examining the likelihood of occurrence of the threat exploiting the vulnerability and the impact severity factors in categories of Confidentiality, Integrity and Availability.

Follow the directions in Section 2.6 of the Risk Determination phase to determine the residual risk level once the recommended safeguard is implemented.

Depending on the nature and circumstances of threats and vulnerabilities, a recommended safeguard may reduce the risk level to "Low." Make a note of the situation with a description below the table, if needed, if such special conditions exist.

For new systems, the next steps would include creating a sensitivity assessment, system security requirements, risk assessment report, and system security plan in the SDLC.

Task 3.4:	Repeat the derivation the risk level for each threat / vulnerability pair from task 2.6, this time assuming the selected safeguard has been
Key Team Members:	System administratorimplemented. Technical reviewer System technical owner System business owner
Output:	Complete the "Residual Risk Level" column of *3.0 Safeguard Determination* table in Appendix D.

RISK DETERMINATION:

Item No.	Threat Name	Vulnerability Name	Risk Description	Existing Controls	Likelihood of Occurrence	Impact Severity	Risk Level
1	Insider Threat	Unauthorized Data Access	Insiders with unauthorized access privileges may misuse or disclose sensitive data, leading to data breaches or reputational damage.	Role-based access controls, user access monitoring, data classification	Low	High	Medium
2	Phishing Attacks	Lack of User Awareness	Insufficient user awareness about phishing attacks may result in successful phishing attempts, leading to unauthorized access or data breaches.	Security awareness training, phishing simulations, email filtering	Moderate	Moderate	Medium
3	Malware Infection	Inadequate Endpoint Protection	Systems may be vulnerable to malware infections if endpoint protection solutions are not deployed or regularly updated.	Antivirus software, endpoint protection policies, regular updates and patches	Low	High	Medium
4	Network Intrusion	Weak Network Perimeter	Inadequate security controls at the network perimeter may allow unauthorized individuals to gain access to the internal network.	Firewalls, intrusion detection and prevention systems, network segmentation	Moderate	High	Medium
5	Data Leakage	Insufficient Data Loss Prevention	Lack of data loss prevention measures may result in unauthorized disclosure of sensitive data, either through intentional or accidental actions.	Data loss prevention tools, data encryption, data access monitoring	Low	Moderate	Low

SAFEGUARD DETERMINATION:

item No.	Risk Description	Recommended Safeguards	Implementation Measures	Responsibility	Target Completion Date
1	Insider Threat - Unauthorized Data Access	Role-Based Access Controls (RBAC)	- Review and update user access privileges based on roles and responsibilities. - Implement strong authentication mechanisms.- Regularly monitor and audit user access activities.	IT Security Team, System Administrators	Q3 20XX
2	Phishing Attacks - Lack of User Awareness	Security Awareness Training	- Develop and deliver comprehensive security awareness training programs to educate employees about phishing techniques and preventive measures. - Conduct periodic phishing simulations to assess user awareness. - Implement email filtering mechanisms to detect and block phishing emails.	Security Awareness Team, IT Help Desk	Q4 20XX
3	Malware Infection - Inadequate Endpoint Protection	Endpoint Protection Solutions	- Deploy and maintain up-to-date antivirus software on all endpoints. - Implement endpoint protection policies and enforce regular updates and patches. - Enable real-time scanning and automatic threat detection and quarantine.	IT Security Team, IT Operations Team	Q2 20XX
4	Network Intrusion - Weak Network Perimeter	Enhanced Network Security Controls	- Regularly review and update firewall rules and configurations. - Implement intrusion detection and prevention systems (IDPS). - Segregate network segments and enforce access controls. - Implement network monitoring and logging mechanisms.	Network Administrators, IT Security Team	Q3 20XX
5	Data Leakage - Insufficient Data Loss Prevention	Data Loss Prevention (DLP) Solutions	- Deploy DLP tools to monitor and prevent unauthorized data disclosure. - Implement data encryption mechanisms to protect sensitive data at rest and in transit. - Implement data access monitoring and logging to detect and respond to data leakage incidents.	IT Security Team, Data Owners and Stewards	