Risk:

A risk is defined as the probability of exposure or loss resulting from a cyber-attack or data breach on an organization

Risk Statements :

The organization faces a high risk of cybersecurity attacks, including but not limited to phishing, malware, ransomware, and data breaches, due to the increasing sophistication of cyber threats, inadequate security measures, and reliance on interconnected systems and networks. These attacks could lead to unauthorized access, data loss, financial losses, reputational damage, and potential legal and regulatory consequences.

Causes of Risk:

Process: Inadequate security documents
People: Non skilled staff
Systems: Lack of systems for implementation

Systems : Bamboo, SAP, Jira, Internet Banking, Learning Management, Loan System

Domain Name: Banking

Obligations:

1. Management Commitment: Top-level management should demonstrate a commitment to cybersecurity by providing adequate resources and support for the implementation of controls.

2. Policy Development: Develop clear and comprehensive cybersecurity policies that outline the organization's approach to risk management and control implementation.

3. Training and Awareness: Ensure that all employees receive regular cybersecurity training and are aware of their responsibilities in safeguarding information and adhering to security policies.

4. Compliance with Regulations: Ensure that the organization complies with relevant cybersecurity laws, regulations, and industry standards.

5. Regular Assessments: Conduct periodic risk assessments and cybersecurity audits to identify vulnerabilities and areas for improvement.

6. Documentation and Records Management: Maintain records of cybersecurity activities, policies, and incidents to facilitate monitoring, analysis, and reporting.

7. Timely Updates and Patch Management: Stay up-to-date with security patches and software updates to address known vulnerabilities promptly.

8. Monitoring and Incident Response: Establish a monitoring system to detect and respond to cybersecurity incidents promptly and effectively.

9. Vendor Oversight: Monitor and assess the cybersecurity practices of third-party vendors to ensure they meet the organization's security requirements.

10. Data Privacy and Protection: Implement measures to protect personal and sensitive data in accordance with relevant data protection laws.

11. Business Continuity Planning: Develop and test a business continuity plan to ensure the organization can recover quickly from cybersecurity incidents.

12. Reporting and Communication: Establish a communication process to report cybersecurity incidents to relevant stakeholders and authorities, as required.

13. Continuous Improvement: Continuously evaluate the effectiveness of cybersecurity controls and update them based on lessons learned from incidents and changing threats.

14. Legal and Regulatory Compliance: Comply with all legal and regulatory obligations related to cybersecurity and data protection.

15. Board Oversight: The board of directors should provide oversight and review of the organization's cybersecurity program to ensure its adequacy and effectiveness.

Controls to Mitigate risks:

1. **Employee Training and Awareness:** Conduct regular cybersecurity training to educate employees about potential threats, phishing awareness, and best practices for data protection.

2. Multi-Factor Authentication (MFA): Enforce MFA for all accounts to add an extra layer of protection against unauthorized access.

3. Strong Password Policies: Implement policies requiring strong, unique passwords and regular password changes to minimize the risk of credential-based attacks.

4. Regular Software Updates and Patch Management: Keep all systems, software, and applications up-to-date to address known vulnerabilities.

5. Firewalls and Intrusion Detection Systems (IDS): Deploy firewalls and IDS to monitor and block suspicious network traffic and activities.

6. Endpoint Protection: Install and regularly update antivirus and anti-malware software on all devices.

7. Data Encryption: Use encryption to protect sensitive data both at rest and during transmission.

8. Network Segmentation: Segment the network to isolate critical systems and limit the impact of potential breaches.

9. Access Control and Privilege Management: Enforce the principle of least privilege, ensuring users have access only to the data and systems necessary for their roles.

10. Incident Response Plan: Develop and regularly test an incident response plan to efficiently respond to and mitigate cyber incidents.

11. Data Backup and Disaster Recovery: Implement regular data backups and have a robust disaster recovery plan in place to recover from potential data loss due to cyberattacks.

12. Third-Party Security Assessments: Conduct regular security assessments of third-party vendors to ensure their security practices meet the organization's standards.

13. Continuous Monitoring and Threat Intelligence: Utilize continuous monitoring and threat intelligence services to detect and respond to emerging threats promptly.

14. Cybersecurity Governance: Establish a cybersecurity governance framework to ensure accountability, responsibility, and oversight in cybersecurity practices.

15. Penetration Testing and Vulnerability Assessments: Conduct regular penetration testing and vulnerability assessments to identify and address weaknesses in the organization's systems.

Scenarios & Impacts

1. **Phishing Attack:** An employee receives an email that appears to be from a legitimate source requesting sensitive information or login credentials. The employee falls victim to the phishing attack and unknowingly discloses confidential data.
    - Data Breach: The unauthorized disclosure of sensitive information may lead to reputational damage and legal liabilities.
    - Financial Loss: Phishing attacks can result in financial losses due to fraudulent transactions or compromised accounts.

2. **Ransomware Infection:** A cybercriminal exploits a vulnerability in outdated software to infiltrate the organization's network and deploy ransomware. The malware encrypts critical data, rendering it inaccessible until a ransom is paid.
    - Data Encryption: Ransomware can encrypt critical data, making it inaccessible until a ransom is paid, leading to operational disruptions and potential data loss.
    - Downtime and Productivity Loss: Remediation efforts and system restoration may cause significant downtime, impacting productivity and business operations

3. **Insider Threat:** An employee with excessive access privileges intentionally or accidentally leaks sensitive customer data or intellectual property to a competitor or unauthorized parties.
    - Data Breach: Insider threats can result in the unauthorized disclosure or theft of sensitive information, causing reputational damage and regulatory penalties.
    - Intellectual Property Theft: Insider actions may lead to the theft of valuable intellectual property, affecting the organization's competitive advantage.

4. Unauthorized Network Access: A hacker exploits a weak password or unsecured Wi-Fi network to gain unauthorized access to the organization's network and steal confidential data.

- Data Breach: Unauthorized access to the network can result in the exposure of sensitive data and customer information.
- Service Disruption: A successful network breach may cause service disruptions and affect business continuity.

5. Data Breach from Third-Party Vendor: A third-party vendor with inadequate cybersecurity practices experiences a data breach, resulting in the exposure of sensitive customer information shared with the organization.

- Reputational Damage: A data breach involving a third-party vendor can erode customer trust and damage the organization's reputation.
- Legal and Regulatory Consequences: The organization may face legal and regulatory penalties for failing to protect customer data shared with vendors.

6. Malware on Mobile Device: An employee's mobile device is infected with malware while connected to an unsecured public Wi-Fi network, leading to data theft and unauthorized access to the organization's network.

- Data Compromise: Malware-infected mobile devices can lead to data compromise and unauthorized access to the organization's network.
- Data Theft: Confidential data stored on compromised mobile devices may be stolen or exposed.

7. **Denial-of-Service (DoS) Attack:** A cyber attacker floods the organization's website or network with excessive traffic, causing service disruptions and rendering the system inaccessible to legitimate users.
    - Service Disruption: A successful DoS attack can render critical services and systems unavailable to legitimate users, impacting business operations and customer experience.
    - Revenue Loss: Downtime resulting from a DoS attack may lead to financial losses due to missed business opportunities.

8. Data Loss from Insider Error: An employee unintentionally deletes critical data or accidentally shares sensitive information with unauthorized parties, resulting in data loss.

- Data Exposure: Data loss incidents caused by employee errors can result in the exposure of sensitive or confidential information.
- Compliance Violations: Such incidents may lead to non-compliance with data protection regulations, attracting legal consequences.

Treatments

Cybersecurity Event management involves monitoring and responding to security events and incidents. It aims to detect potential threats, investigate suspicious activities, and take appropriate actions to mitigate risks. Here's how event management can be applied to the scenarios mentioned earlier:

1. Phishing Attack: Implement email security solutions that detect phishing attempts and alert security teams when suspicious emails are received. Train employees to report phishing incidents immediately so that the security team can investigate and respond promptly.

2. Ransomware Infection: Event Management: Deploy security tools that monitor for unusual file encryption patterns or changes in file extensions, which could indicate ransomware activity. Set up alerts to trigger when such behaviour is detected, allowing the incident response team to isolate and remediate affected systems.

3. Insider Threat: Monitor user activity and data access patterns to identify unusual or suspicious behaviour. Establish alerts and triggers for activities that may indicate insider threats, such as access to sensitive data outside of regular business hours or accessing data from unfamiliar locations.

4. Unauthorized Network Access: Implement network monitoring tools to track and analyze network traffic. Set up intrusion detection systems (IDS) to identify potential unauthorized access attempts and alert the security team for immediate investigation and response.

5. Data Breach from Third-Party Vendor: Establish a process for continuous monitoring of third-party vendor activities, including data transfers and access to sensitive information. Set up alerts for unusual or unauthorized vendor activities to quickly detect potential breaches and initiate an incident response plan.

6. Malware on Mobile Device: Utilize mobile device management (MDM) solutions to monitor and track mobile device activity. Set up alerts for suspicious behavior or malware indicators, and remotely wipe or quarantine compromised devices when necessary.

7. Denial-of-Service (DoS) Attack: Deploy network traffic analysis tools to identify abnormal patterns indicative of a DoS attack. Set up automated responses or manual actions to divert or block malicious traffic, minimizing the impact on the organization's services.

8. Data Loss from Insider Error: Monitor data access and transfers to detect unusual or potentially risky activities. Implement data loss prevention (DLP) solutions to prevent accidental data leakage, and establish alerts to notify the security team of potential data loss incidents.

Key Risk Indicators (KRI):

Below are the list of Key risk indicators**,**

1. Phishing Attack
2. Ransomware Infection
3. Insider Threat
4. Unauthorized Network Access
5. Data Breach from Third-Party Vendor
6. Malware on Mobile Device
7. Denial-of-Service (DoS) Attack
8. Data Loss from Insider Error