







CS668: Practical Cybersecurity for Cybersecurity Practitioners

Assignment-3 Group - 1

Name	Roll No	Contributed
Bikash Saha (Group Lead)	231110610	
Ashutosh Agrawal	210219	
Sandeep Nitharwal	210921	
Lt Cdr Sunil Kumar	231110025	
NIKHIL MEENA	210667	
SUSOVAN PATRA	22111061	

To conduct a high-level cyber risk assessment for the Grameena Vikas Bank, we follow the guidelines outlined in NIST SP800-30, which focus on identifying threats, vulnerabilities, likelihood of threat exploitation, impacts, and overall risk rating. Our assumptions, threats and vulnerability are based on the key base of cybersecurity: **People, Process, and Technology (PPT)**. The answers to the given questions are discussed below:

I. Based on the business processes described and any assumption you make about a rural bank’s functions (assumptions must be explicitly stated) – list the cyber threats you consider for your risk assessment exercise.

For this task, we considered a range of cyber threats that could potentially impact its operations and security posture. These considerations are based on the detailed description provided, along with assumptions about typical functions and vulnerabilities of a rural bank. The assumptions are stated below along with the context in which these threats are identified.

Below are some critical details of the Grameena Vikas Bank:

No.	Given Detail	Description
G1	Depreciated Operating System	Server are running on Linux (Ubuntu 18.04), which is depreciated according to official notification ^{1,2}
G2	Use of Windows 11 21h2 10.0.22000.739 on ARM64	30 machines are running Win11 on given setup which is susceptible to several vulnerabilities ^{3,4}
G3	Use of Windows 10 1903 on X86	20 machines are running Win10 on given setup, which is susceptible to several vulnerabilities ^{5,6,7}
G4	HTTP server	HTTP server is running which facilitates communication in plain text rather than encrypted

¹ <https://ubuntu.com/blog/18-04-end-of-standard-support>

² <https://computing.cs.cmu.edu/news/2022/eol-ubuntu-1804>

³

https://nvd.nist.gov/products/cpe/search/results?namingFormat=2.3&orderBy=2.3&keyword=cpe%3A2.3%3Ao%3Amicrosoft%3Awindows_11_21h2%3A10.0.22000.739&status=FINAL

⁴

https://nvd.nist.gov/vuln/search/results?adv_search=true&isCpeNameSearch=true&query=cpe%3A2.3%3Ao%3Amicrosoft%3Awindows_11_21h2%3A10.0.22000.739%3A*%3A*%3A*%3A*%3Aarm64%3A*

⁵ https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-32238/version_id-640739/Microsoft-Windows-10-1903.html

⁶

https://nvd.nist.gov/products/cpe/search/results?namingFormat=2.3&keyword=cpe%3A2.3%3Ao%3Amicrosoft%3Awindows_10_1903%3A*%3A*%3A*%3A*%3A*%3Ax86#

⁷

https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&isCpeNameSearch=true&seach_type=all&query=cpe:2.3:o:microsoft:windows_10_1903:-:*:*:*:*:x86.*

G5	Use of FortiGate 6500F network firewall	This firewall is susceptible to heap-based buffer overflow vulnerability ^{8,9}
-----------	--	---

Assumptions:

No	Assumption	Description
A1	Digital and Mobile Banking Services	The bank offers online and mobile banking services to its customers, including account management, funds transfer, withdrawals and loans. The interface of these platforms may not consider security measures while development.
A2	Internet Connectivity	The bank's operations are heavily reliant on internet connectivity for both internal operations and customer-facing services.
A3	Limited Resources	As a small rural bank, Grameena Vikas Bank has limited resources dedicated to cybersecurity, impacting its ability to implement sophisticated security measures. All of its machine and server might be at same place and no backup server might be present
A4	Employee Training	The bank's staff are not highly trained in cybersecurity best practices, which increases the risk of falling to social engineering and other attacks which involve humans as an attack vector.
A5	Physical Security	Being in a rural area, the physical security measures might be less stringent than those in urban settings, assuming a lower crime rate but potentially overlooking targeted attacks.
A6	Employee Access to Sensitive Information	Employees have access to customer financial information and transaction processing systems.
A7	Customer Base	Customers are primarily from rural areas and might lack awareness about cybersecurity,

8

https://nvd.nist.gov/vuln/search/results?adv_search=true&isCpeNameSearch=true&query=cpe%3A2.3%3Ah%3Afortinet%3Afortigate-6500f%3A-%3A*%3A*%3A*%3A*%3A*%3A*%3A*

⁹ CVE-2022-42475: <https://nvd.nist.gov/vuln/detail/CVE-2022-42475>

		making them more susceptible to phishing attacks and fraud.
A8	Third-Party Dependencies	Reliance on third-party vendors for critical banking applications, which may introduce risks if these parties are not properly vetted or if their security measures are inadequate.
A9	Absence of Cybersecurity Department	Bank does not have any cybersecurity-specific team or department for regular assessment. Also, given the limited resources, the bank cannot hire third parties to do assessments. The bank may have misconfigured the firewall and threat susceptible server setups.

Cyber Threats:

No.	Threats	Description	Non-exhaustive Possible Reasons & Related Assumptions
T1	Phishing Attacks	Both employees and customers might get targeted by phishing campaigns designed to steal login credentials, install malware or start infection.	A4: Employee Training A7: Customer Base A9: Absence of Cybersecurity dept.
T2	Ransomware	Given the critical nature of the organization, ransomware attacks could encrypt sensitive data, demand payment for decryption keys, and may steal customers' personal Identification information. The reliance on digital services increases this risk. Given the bank's limited IT resources, recovery from such an attack could be particularly challenging.	A1: Digital and Mobile Banking Services A3: Limited Resources A9: Absence of Cybersecurity dept.
T3	DDoS Attacks	Attempts to overload the bank's internet-facing servers, disrupting service	A2: Internet Connectivity

		availability to users and potentially masking other malicious activities by leveraging the bank's dependency on internet connectivity.	A3: Limited Resources A9: Absence of Cybersecurity dept.
T4	Vulnerability Exploitation	The bank's critical server is running on a Linux machine (Ubuntu 18.04), and this has been depreciated in the year 2023. This version is vulnerable to several attacks including SQL injection (CVE-2020-9402), which can potentially expose customer data or allow unauthorized transactions. The windows versions running of Employees machines are also vulnerable to several attacks such as CVE-2024-21407 (RCE) in Win11 and CVE-2023-21722 (DOS) in Win10. Also, the FortiGate 6500F firewall is vulnerable to CVE-2022-42475 (Heap Overflow).	G1: Depreciated Operating System G2: Use of Windows 11 21h2 10.0.22000.739 on ARM64 G3: Use of Windows 10 1903 on X86 G5: Use of FortiGate 6500F network firewall A9: Absence of Cybersecurity dept.
T5	Insider Threats	Employees with access to sensitive information might intentionally or unintentionally leak data or misuse their access privileges, compounded by potential oversights in access control due to limited resources.	A6: Employee Access to Sensitive Information A9: Absence of Cybersecurity dept.
T6	Advanced Persistent Threats (APTs)	Targeted, stealthy threats aimed at espionage or long-term access to financial data. While more common against larger institutions, smaller banks could be targeted due to perceived lower defenses.	It can include individual or various combinations of details/assumptions
T7	Malware Attack	Infections on employee or bank machines, including those within privileged network segments, that could lead to data leakage or unauthorized access to sensitive banking operations.	It can include individual or various combinations of details/assumptions
T8	Social Engineering	Beyond phishing, other forms of social engineering could trick employees into divulging sensitive information or performing unauthorized transactions.	A4: Employee Training A7: Customer Base A9: Absence of Cybersecurity dept.
T9	Physical Theft or Tampering	Assuming lower physical security standards, there could be a risk of theft or tampering with	A5: Physical Security

		physical assets, including servers and network devices.	A9: Absence of Cybersecurity dept.
T10	Man-in-the-Middle (MitM) Attacks	Attackers could intercept communications between the bank's servers and clients or within the internal network, aiming to steal or manipulate data as communication is going on in plain text, i.e., HTTP not HTTPS.	G4: HTTP server A9: Absence of Cybersecurity dept.
T11	Supply-Chain Attack	Reliance on third-party vendors may introduce a supply chain attack.	A8: Third party Dependencies A9: Absence of Cybersecurity dept.

Addressing these threats requires a comprehensive cybersecurity strategy that includes technical controls, employee training, and regular assessments to adapt to evolving risks.

II. What kind of vulnerabilities should be considered? How are you going to find the vulnerabilities?

In the context of Grameena Vikas Bank and under the assumptions regarding its operations and environment, several categories of vulnerabilities should be considered. These vulnerabilities stem from human factors (**People**), procedural (**Process**), and technical (**Technology**). Identifying and addressing these vulnerabilities is crucial for enhancing the bank's cybersecurity posture. Below, we explored the types of vulnerabilities to consider and methodologies for finding them.

Types of Vulnerabilities:

No.	Type	Name	Description	Non-Exhaustive Related Threats
V1	Technical Vulnerabilities	Outdated Software	Running outdated versions of operating systems (Windows 10 1903, Ubuntu 18.04) and applications that may contain known security flaws, lacking modern security features.	T2: Ransomware T4: Vulnerability Exploitation T6: Advanced

				Persistent Threats (APTs) T7: Malware Attack
V2		Configuration Errors	Misconfigured network devices (e.g., FortiGate 6500F firewall) and servers that could expose unnecessary services to the internet or internal users.	T3: DDoS Attack T7: Malware Attack T4: Vulnerability Exploitation T10: Man-in-the-Middle (MitM) Attacks
V3		Exposed Services	Services unnecessarily exposed to the internet can be entry points for attacks.	T3: DDoS Attack
V4		Insecure Interfaces	Web interfaces for banking services that may not adequately validate user input, leading to injection attacks or unauthorized access.	T4: Vulnerability Exploitation T10: Man-in-the-Middle (MitM) Attacks
V5	Procedural Vulnerabilities	Lack of Incident Response Plan	Inadequate preparation for identifying and responding to security incidents could exacerbate the impact of breaches.	T2: Ransomware T6: Advanced Persistent Threats (APTs)
V6		Insufficient Access Control Policies	Not strictly enforcing the principle of least privilege within departments, allowing employees more access than necessary for their role.	T1: Phishing Attack T6: Advanced Persistent Threats (APTs) T11: Supply-Chain Attack

V7		Inadequate Data Protection Measures	Failure to implement proper data backup and encryption policies for sensitive customer information and financial data.	T1: Phishing Attack T2: Ransomware T6: Advanced Persistent Threats (APTs) T7: Malware Attack T11: Supply-Chain Attack
V8	Human Factor Vulnerabilities	Phishing Susceptibility	Employees might not be adequately trained to recognize phishing attempts, leading to unauthorized access or data breaches.	T1: Phishing Attack T7: Malware Attack T8: Social Engineering
V9		Insider Threats Vulnerability	Potential for malicious actions by employees or accidental misuse of systems due to lack of awareness regarding security policies.	T5: Insider Threats T8: Social Engineering
V10	Physical Security Vulnerabilities	Physical Access to Critical Infrastructure	Unauthorized physical access to servers and network devices can lead to cyber breaches.	T5: Insider Threats T9: Physical Theft or Tampering
V11		Surveillance Gaps	Areas not covered adequately by CCTV, leading to potential security breaches without evidence.	T9: Physical Theft or Tampering

Finding Vulnerabilities:

No.	Method	Description	Non-Exhaustive Covered Vulnerability
F1	Automated Vulnerability Scanning	Utilize automated tools to scan the bank's network and systems for known vulnerabilities. These tools can identify	V1: Outdated Software V2: Configuration Errors

		outdated software, misconfigurations, and known security flaws in the operating systems and applications used by the bank.	V3: Exposed Services V4: Insecure Interfaces
F2	Penetration Testing	Conduct regular penetration tests to simulate cyber-attacks on the bank's infrastructure. This hands-on approach helps identify weaknesses in both technical defenses and employee practices.	V1: Outdated Software V2: Configuration Errors V3: Exposed Services V4: Insecure Interfaces V6: Insufficient Access Control Policies V7: Inadequate Data Protection Measures V8: Phishing susceptibility
F3	Phishing Simulation and Training	Run phishing simulation exercises to evaluate employee susceptibility to phishing attacks. This can help identify the need for further training and awareness programs.	V8: Phishing susceptibility
F4	Third-Party Security Assessments	Evaluate the security measures of third-party vendors and service providers. This can include reviewing security certifications, conducting audits, or requiring security assessments as part of contractual agreements.	V3: Exposed Services V4: Insecure Interfaces V7: Inadequate Data Protection Measures
F5	Software Dependency Checks	Regularly review and update all software dependencies to ensure they are up-to-date and free from known vulnerabilities. This includes operating systems, database management systems, and any third-party libraries or frameworks.	V1: Outdated Software V4: Insecure Interfaces
F6	Physical Security Reviews	Perform regular reviews and audits of physical security measures, checking for potential vulnerabilities and ensuring that controls are effective.	V10: Physical Access to Critical Infrastructure V11: Surveillance Gaps

F7	Access Control Reviews	Periodically review access rights and privileges for all users, especially focusing on high-privilege accounts, to ensure that they align with the principle of least privilege.	V6: Insufficient Access Control Policies V9: Insider Threats Vulnerability
F8	Security Audits	Perform comprehensive security audits that review both the technical environment and operational procedures. This includes assessing firewall configurations, access control policies, encryption standards, and incident response plans.	V1: Outdated Software V2: Configuration Errors V3: Exposed Services V4: Insecure Interfaces V5: Lack of Incident Response Plan V6: Insufficient Access Control Policies V7: Inadequate Data Protection Measures V8: Phishing susceptibility V9: Insider Threats Vulnerability V11: Surveillance Gaps

Addressing these vulnerabilities requires a multifaceted approach that includes keeping software up to date, implementing strong configuration management practices, enhancing employee training programs, and adopting a proactive stance towards cybersecurity threat management. Continuous monitoring and regular reviews are essential to adapt to new threats and vulnerabilities as they emerge.

III. Explain your rationale for likelihood of various threat, vulnerability combinations. For the vulnerabilities you identify and threats you consider, build a matrix to show the qualitative likelihood for all the pairs (threat, vulnerability).

Our analysis involves considering the nature of each vulnerability, the organization's environment, and the common tactics, techniques, and procedures employed by cyber

adversaries. The rationale behind evaluating the likelihood of threat-vulnerability combinations includes factors are following:

- **Prevalence of the Threat Type:** How often a given threat exploits a specific vulnerability in the wild. Higher prevalence increases the likelihood rating.
- **Attractiveness of the Target:** The potential gain for an attacker, which can make certain vulnerabilities more tempting to exploit, thereby raising the likelihood.
- **Difficulty of Exploitation:** How easy it is for an attacker to exploit the vulnerability. Easier exploitation leads to a higher likelihood.
- **Potential Impact of a Successful Attack:** The severity of the outcome if the vulnerability is exploited. Vulnerabilities leading to significant impacts are targeted more aggressively.

Based on these considerations, we create a matrix that pairs identified vulnerabilities with potential threats, assigning a qualitative likelihood (High, Medium, Low) to each combination. This matrix helps prioritize risk management efforts by highlighting the most critical vulnerabilities that need addressing to mitigate potential threats. The simplified rationale for matrix entries is following:

- **High (H):** A direct, well-documented path exists for the threat to exploit the vulnerability, with a history of widespread exploitation or significant potential impact. A vulnerability provides a straightforward or particularly effective avenue for a threat.
- **Medium (M):** The vulnerability could facilitate the threat under certain conditions, or there's a less direct path for exploitation. There's a plausible but less direct connection; exploitation may require additional steps or conditions.
- **Low (L):** An indirect relationship where exploitation is possible but less likely due to complexity, lower attacker interest, or mitigating factors. The link between vulnerability and threat is tenuous, indirect, or would be unusual as a primary attack vector.

Identified Threats:

- **T1:** Phishing Attacks (PA)
- **T2:** Ransomware (R)
- **T3:** DDoS Attacks (DDA)
- **T4:** Vulnerability Exploitation (VE)
- **T5:** Insider Threats (IT)
- **T6:** Advanced Persistent Threats (APT)
- **T7:** Malware Attack (MA)
- **T8:** Social Engineering (SE)

- **T9:** Physical Theft or Tampering (PTT)
- **T10:** Man-in-the-Middle (MitM) Attacks (MMA)
- **T11:** Supply-Chain Attack (SCA)

Identified Vulnerabilities:

- **V1:** Outdated Software (OS)
- **V2:** Configuration Errors (CE)
- **V3:** Exposed Services (ES)
- **V4:** Insecure Interfaces (II)
- **V5:** Lack of Incident Response Plan (LIRP)
- **V6:** Insufficient Access Control Policies (IACP)
- **V7:** Inadequate Data Protection Measures (IDPM)
- **V8:** Phishing Susceptibility (PS)
- **V9:** Insider Threats Vulnerability (ITV)
- **V10:** Physical Access to Critical Infrastructure (PACI)
- **V11:** Surveillance Gaps (SG)

Threat-Vulnerability Likelihood Matrix:

Vulnerability/Threat	T1: PA	T2: R	T3: DD A	T4: VE	T5: IT	T6: APT	T7: MA	T8: SE	T9: PTT	T10: MMA	T11: SCA
V1: OS	M	H	L	H	L	H	H	M	L	H	H
V2: CE	L	H	M	H	M	H	H	L	L	H	M
V3: ES	L	M	H	H	L	H	M	L	L	M	M
V4: II	M	H	L	H	L	H	H	M	L	H	H
V5: LIRP	L	H	H	H	H	H	H	H	M	M	H
V6: IACP	L	H	L	H	H	H	H	H	M	M	M
V7: IDPM	L	H	L	H	H	H	H	H	H	H	H
V8: PS	H	M	L	M	L	M	M	H	L	L	L
V9: ITV	L	H	L	H	H	H	H	H	H	L	M
V10: PACI	L	M	L	L	H	L	L	L	H	L	L
V11: SG	L	L	L	L	M	L	L	L	H	L	L

This matrix highlights the intersection of threats and vulnerabilities, providing a visual representation to guide the prioritization of mitigation efforts. It's important to address high likelihood combinations immediately with appropriate controls and continuously monitor for new vulnerabilities or emerging threats.

The concise reason of selecting High, Medium, and Low for each pair is discussed below:

- **Outdated Software**

- **Phishing Attacks (Medium):** Phishing can deliver exploits targeting outdated software vulnerabilities.
- **Ransomware (High):** Frequently targets known vulnerabilities in outdated software for easy entry.
- **DDoS Attacks (Low):** Software currency has minimal impact on DDoS vulnerability.
- **Vulnerability Exploitation (High):** Outdated software is a prime target for exploiting known vulnerabilities.
- **Insider Threats (Low):** Less relevant, unless insiders deliberately exploit these vulnerabilities.
- **APTs (High):** APTs often exploit outdated software for initial access or persistence.
- **Malware Attack (High):** Outdated software often lacks defenses against modern malware techniques.
- **Social Engineering (Medium):** Social engineering tactics might encourage actions exploiting outdated software.
- **Physical Theft/Tampering (Low):** Not directly relevant to the software's currency.
- **MitM Attacks (High):** Older software may not support modern, secure protocols, increasing MitM risk.
- **Supply-Chain Attack (High):** Components with outdated software can be initial vectors in a supply chain attack.

- **Configuration Errors**

- **Phishing Attacks (Low):** Indirect impact unless specific configurations make users more susceptible.
- **Ransomware (High):** Misconfigurations can leave systems more vulnerable to ransomware deployment.
- **DDoS Attacks (Medium):** Poor configurations can expose services to higher risks of DDoS attacks.

- **Vulnerability Exploitation (High):** Directly related; misconfigurations can introduce or expose vulnerabilities.
- **Insider Threats (Medium):** Misconfigurations can be exploited by insiders for unauthorized access.
- **APTs (High):** Target specific configuration weaknesses for entry or movement.
- **Malware Attack (High):** Misconfigurations can allow malware to bypass security controls.
- **Social Engineering (Low):** Less directly related; focuses more on manipulating human behavior.
- **Physical Theft/Tampering (Low):** Configuration errors primarily affect logical rather than physical security.
- **MitM Attacks (High):** Insecure network configurations increase susceptibility.
- **Supply-Chain Attack (Medium):** Configuration weaknesses in supply chain elements can be exploited.
- **Exposed Services**
 - **Phishing Attacks (Low):** Exposed services are less relevant to phishing, which typically targets individuals rather than direct service exploitation.
 - **Ransomware (Medium):** Exposed services can be entry points for ransomware to infiltrate networks if they exploit vulnerabilities in these services.
 - **DDoS Attacks (High):** Directly targets exposed services to overwhelm them, making them a prime vector for such attacks.
 - **Vulnerability Exploitation (High):** Exposed services are at high risk as they are accessible and can be probed and exploited by attackers looking for vulnerabilities.
 - **Insider Threats (Low):** Insider threats generally do not rely on exposed services to conduct malicious activities, focusing more on abusing legitimate access.
 - **Advanced Persistent Threats (APTs) (High):** APTs often exploit exposed services to gain initial access or maintain persistence within a target network.
 - **Malware Attack (Medium):** Exposed services can be vectors for malware delivery, especially if specific vulnerabilities within the services are exploited.

- **Social Engineering (Low):** Like phishing, social engineering targets individuals rather than exploiting technical vulnerabilities in exposed services.
- **Physical Theft or Tampering (Low):** This threat involves physical access and is not typically associated with exploiting exposed digital services.
- **Man-in-the-Middle (MitM) Attacks (Medium):** Exposed services, especially those not secured with proper encryption, are vulnerable to MitM attacks aiming to intercept or alter data in transit.
- **Supply-Chain Attack (Medium):** Exposed services might be exploited as part of a larger supply-chain attack, especially if they belong to a supplier or are critical dependencies of an organization.
- **Insecure Interfaces**
 - **Phishing Attacks (Medium):** Phishing attacks generally target users rather than system interfaces directly. However, insecure interfaces can be exploited if phishing leads to credential theft, enabling attackers to bypass interface security measures.
 - **Ransomware (High):** Insecure interfaces can be exploited to deliver ransomware into the system, especially if these interfaces allow file uploads or remote code execution.
 - **DDoS Attacks (Low):** DDoS attacks primarily target service availability and do not exploit software vulnerabilities directly. The security of interfaces influences the ease of mitigation rather than the likelihood of attack.
 - **Vulnerability Exploitation (High):** Insecure interfaces are a prime target for exploitation, as they can provide direct access to system functions and data if not properly secured.
 - **Insider Threats (Low):** Insider threats typically leverage legitimate access rather than exploiting vulnerabilities. However, insecure interfaces can exacerbate risks if insiders misuse their knowledge to exploit these weaknesses.
 - **Advanced Persistent Threats (APTs) (High):** APTs often use sophisticated methods to exploit vulnerabilities, including insecure interfaces, to gain sustained access to a network.
 - **Malware Attack (High):** Insecure interfaces can be exploited to inject malware into a system, especially if they allow for data input or file uploads without sufficient validation and sanitization.
 - **Social Engineering (Medium):** While social engineering targets individuals, insecure interfaces can be a vector for attackers to leverage information obtained from social engineering (like credentials) for unauthorized access.

- **Physical Theft or Tampering (Low):** Physical security threats are less about exploiting software vulnerabilities and more about unauthorized physical access, making interface security less relevant.
- **Man-in-the-Middle (MitM) Attacks (High):** Insecure interfaces, especially those not implementing proper encryption for data in transit, are vulnerable to MitM attacks, where attackers intercept or alter communications.
- **Supply-Chain Attack (High):** Insecure interfaces within a supply chain can be exploited to gain access to or compromise connected systems, making them a high-risk vector for supply-chain attacks.
- **Lack of Incident Response Plan**
 - **Phishing Attacks (Low):** An incident response plan is crucial after a phishing attack occurs, not for preventing the initial compromise. The low rating reflects the post-incident nature of response plans.
 - **Ransomware (High):** A robust incident response plan is critical for quickly addressing ransomware infections, mitigating damage, and restoring operations. Lack of a plan can significantly worsen the impact.
 - **DDoS Attacks (High):** Effective response to DDoS attacks requires coordinated actions to mitigate the attack and maintain service availability. Without a plan, prolonged disruptions are likely.
 - **Vulnerability Exploitation (High):** Post-exploitation, a well-defined incident response plan is essential for containing the breach and preventing further damage. Its absence leaves the organization vulnerable to extensive harm.
 - **Insider Threats (High):** Incident response plans are crucial for dealing with insider threats, as they often require a nuanced approach to investigation and mitigation. Lack of a plan complicates internal threat resolution.
 - **APTs (Advanced Persistent Threats) (High):** APTs are sophisticated and can linger undetected. A comprehensive incident response plan is vital for detection, eradication, and recovery. Without it, APTs can cause widespread and sustained damage.
 - **Malware Attack (High):** Quick and coordinated responses are necessary to isolate and remove malware, minimize spread, and restore services. The absence of a plan makes managing malware outbreaks more challenging.
 - **Social Engineering (High):** Effective responses to social engineering incidents often require immediate action and coordination, which are structured within an incident response plan. Without it, mitigating damage is harder.
 - **Physical Theft or Tampering (Medium):** While primarily physical security incidents, a comprehensive incident response plan includes procedures for

digital consequences of physical actions. Its lack could delay the recovery process.

- **Man-in-the-Middle (MitM) Attacks (Medium):** Incident response plans include monitoring and response strategies that could mitigate ongoing MitM attacks' impact. However, prevention primarily relies on encryption and secure communication protocols.
- **Supply-Chain Attack (High):** Supply-chain attacks require a complex and coordinated response, often involving multiple stakeholders. The absence of an incident response plan greatly exacerbates the difficulty of managing and recovering from such attacks.

- **Insufficient Access Control Policies**

- **Phishing Attacks (Low):** Low. Phishing attacks typically aim to steal credentials or deliver malware and do not directly exploit access control policies. However, the impact of a successful phishing attack could be magnified if insufficient access control policies are in place, allowing broader access than necessary.
- **Ransomware (High):** High. Insufficient access controls can allow ransomware to spread more easily within a network if it gains initial access, affecting more systems and encrypting more data.
- **DDoS Attacks (Low):** Low. DDoS attacks primarily target network availability and does not exploit access control policies directly.
- **Vulnerability Exploitation (High):** High. Weak access controls can give attackers easier lateral movement capabilities, exploiting vulnerabilities in more privileged or sensitive systems.
- **Insider Threats (High):** High. Insiders can misuse or escalate their access due to insufficient policies, leading to unauthorized actions or data breaches.
- **APTs (High):** High. Advanced Persistent Threats often exploit access control weaknesses to maintain persistence and access within a target network stealthily.
- **Malware Attack (High):** High. Insufficient access controls can facilitate the spread and impact of malware across the network by not adequately segregating user privileges and system access.
- **Social Engineering (High):** High. Attackers using social engineering can more easily gain access or manipulate users into granting access if access controls are weak or poorly enforced.
- **Physical Theft or Tampering (Medium):** Medium. While physical security is distinct, weak access controls increase risks if physical security is breached, as attackers can more easily access or manipulate systems.

- **MitM Attacks (Medium):** Medium. Insufficient access control policies indirectly increased risk by potentially allowing attackers to position themselves to intercept or alter communications more easily if they gain access to the network.
- **Supply-Chain Attack (Medium):** Weak access controls can exacerbate the impact of a supply-chain compromise by allowing malicious actors more freedom once they've penetrated the network via a third-party component.
- **Inadequate Data Protection Measures**
 - **Phishing Attacks (Low):** Phishing primarily targets credential theft or malware delivery, not directly exploiting data protection measures.
 - **Ransomware (High):** Weak data protection can exacerbate ransomware impact by leaving sensitive data unencrypted and more susceptible to theft or loss.
 - **DDoS Attacks (Low):** DDoS attacks focus on disrupting service, not exploiting data protection weaknesses.
 - **Vulnerability Exploitation (High):** Exploits can target specific weaknesses in data protection mechanisms to access or exfiltrate unprotected data.
 - **Insider Threats (High):** Insiders may exploit inadequate data protection to access or misuse sensitive information without proper authorization.
 - **APTs (High):** Advanced threats often seek to stealthily access and exfiltrate sensitive data, exploiting inadequate protections.
 - **Malware Attack (High):** Malware (beyond ransomware) can be designed to steal or corrupt data, exploiting weak data protection measures.
 - **Social Engineering (High):** Social engineering can manipulate users into bypassing data protection measures, leading to data leaks or unauthorized access.
 - **Physical Theft or Tampering (High):** Physical security breaches can directly lead to data theft, especially if data is inadequately protected (e.g., unencrypted devices).
 - **Man-in-the-Middle (MitM) Attacks (High):** MitM attacks intercept data in transit. Inadequate protection (like lack of encryption) facilitates data interception and compromise.
 - **Supply-Chain Attack (High):** Compromised supply chain elements can exploit inadequate data protections to access, exfiltrate, or corrupt data within the network.
- **Phishing Susceptibility**

- **Phishing Attacks (High):** Directly targets this vulnerability. Phishing susceptibility indicates a lack of awareness among users, making them more likely to fall for phishing emails, leading to a high likelihood of successful attacks.
- **Ransomware (Medium):** Often distributed via phishing emails. The medium likelihood reflects that while phishing is a common vector, ransomware can also spread through other means, such as exploiting network vulnerabilities.
- **DDoS Attacks (Low):** Phishing susceptibility has a minimal direct impact on the likelihood of DDoS attacks, as these attacks target network infrastructure rather than individual susceptibilities to deceptive emails.
- **Vulnerability Exploitation (Medium):** Phishing emails can deliver malware designed to exploit system vulnerabilities. The medium likelihood is due to the attack's success depending partly on the presence of exploitable system vulnerabilities.
- **Insider Threats (Low):** While insider threats are a significant concern, phishing susceptibility is less directly related to this threat. Insider threats typically involve malicious actions by authorized users rather than deception through phishing.
- **Advanced Persistent Threats (APTs) (Medium):** APTs can use phishing as an entry point for long-term espionage or data exfiltration operations. The medium likelihood reflects that APTs use a variety of tactics, not limited to phishing.
- **Malware Attack (Medium):** Phishing emails are a common method for distributing malware. The medium likelihood acknowledges that, similar to ransomware, malware can also be spread through other methods.
- **Social Engineering (High):** Phishing is a form of social engineering, directly exploiting human vulnerabilities. High susceptibility to phishing indicates a broader vulnerability to social engineering tactics.
- **Physical Theft or Tampering (Low):** Phishing susceptibility has little to no direct correlation with the risk of physical theft or tampering, as these threats involve physical access rather than deceptive communication.
- **Man-in-the-Middle (MitM) Attacks (Low):** While phishing can sometimes facilitate MitM attacks, by, for example, tricking users into disclosing credentials, the direct link is less straightforward, resulting in a low likelihood.
- **Supply-Chain Attack (Low):** Phishing susceptibility within an organization has a minimal direct impact on the likelihood of a supply-chain attack, which targets vulnerabilities in suppliers or third-party service providers.

- **Insider Threats Vulnerability**

- **Phishing Attacks (Low):** Insider threats typically involve malicious or negligent insiders already having access to systems. Phishing is generally an external attack method aimed at gaining unauthorized access, making it less relevant to insider threats.
- **Ransomware (High):** Insiders with malicious intent or negligent behaviors can inadvertently or deliberately introduce ransomware into the system, bypassing external defenses.
- **DDoS Attacks (Low):** DDoS attacks are primarily external threats targeting the availability of services. Insider threats are less likely to utilize DDoS as it does not leverage their access or knowledge.
- **Vulnerability Exploitation (High):** Insiders can exploit known vulnerabilities within the system, leveraging their access and knowledge of the organization's infrastructure for malicious purposes.
- **Insider Threats (High):** Redundantly, the insider threats category directly correlates with itself, emphasizing the risk posed by individuals within the organization exploiting their access.
- **Advanced Persistent Threats (APTs) (High):** Insiders could be part of or aid APTs by providing access or sensitive information, thus facilitating these sophisticated and targeted attacks.
- **Malware Attack (High):** Insiders can intentionally introduce malware into the network or be tricked into doing so, exploiting their legitimate access to bypass security measures.
- **Social Engineering (High):** Insiders may be susceptible to social engineering by external parties or may use similar tactics internally to manipulate colleagues into divulging confidential information or performing unauthorized actions.
- **Physical Theft or Tampering (High):** Insiders, by virtue of their physical access to the organization's assets, can directly engage in theft or tampering of hardware, data, and other sensitive assets.
- **Man-in-the-Middle (MitM) Attacks (Low):** While possible, MitM attacks are more technically complex and less likely to be employed by insiders, who can directly access systems and data without needing to intercept communications.
- **Supply-Chain Attack (Medium):** Insiders could facilitate a supply-chain attack by compromising the security of products or services before they are delivered to clients or by providing sensitive information to external attackers targeting the supply chain.

- **Physical Access to Critical Infrastructure**

- **Phishing Attacks (Low):** Phishing primarily targets digital access through deceptive communications, not physical access.
- **Ransomware (Medium):** While typically launched via digital means, gaining physical access can facilitate direct deployment on critical systems, though less common.
- **DDoS Attacks (Low):** DDoS attacks are launched remotely to overwhelm systems with traffic, not reliant on physical access.
- **Vulnerability Exploitation (Low):** Exploitation usually occurs through digital vulnerabilities rather than through physical access mechanisms.
- **Insider Threats (High):** Insiders with physical access to critical infrastructure can directly misuse, damage, or steal hardware and data.
- **Advanced Persistent Threats (APTs) (Low):** APTs typically use stealthy digital methods for infiltration and long-term access, not direct physical access.
- **Malware Attack (Low):** Malware is generally introduced through digital vectors, although physical access could be used for direct installation, it's less typical.
- **Social Engineering (Low):** Social engineering aims to manipulate individuals into granting access or divulging confidential information, more aligned with digital access than physical.
- **Physical Theft or Tampering (High):** Direct physical access increases the risk of theft or tampering with critical systems and hardware.
- **Man-in-the-Middle (MitM) Attacks (Low):** MitM attacks intercept digital communications; physical access to infrastructure does not directly facilitate this attack method.
- **Supply-Chain Attack (Low):** Supply-chain attacks target software and hardware supply chains through digital means, not through direct physical access to the target's infrastructure.

- **Surveillance Gaps**

- **Phishing Attacks (Low):** Surveillance systems typically monitor physical spaces; thus, their effectiveness or gaps have minimal direct impact on phishing attacks, which occur in the digital domain.
- **Ransomware (Low):** Ransomware infections are initiated through digital vectors, such as email or network exploitation. Physical surveillance gaps do not contribute to the risk of ransomware.

- **DDoS Attacks (Low):** DDoS attacks target the availability of online services. The presence or absence of physical surveillance does not influence the likelihood of these attacks.
- **Vulnerability Exploitation (Low):** Exploitation of software or network vulnerabilities is unrelated to physical surveillance capabilities, focusing instead on digital weaknesses.
- **Insider Threats (Medium):** While primarily concerned with digital actions, insider threats can involve physical components, like unauthorized access to secure areas. Surveillance gaps can make it easier for insiders to physically access areas without detection.
- **Advanced Persistent Threats (APTs) (Low):** APTs are sophisticated, focusing on stealthy digital infiltration over time. Physical surveillance plays a minimal role in deterring or detecting such threats.
- **Malware Attack (Low):** Malware is typically introduced through digital means. Physical surveillance does not directly prevent or detect the digital introduction of malware.
- **Social Engineering (Low):** Social engineering attacks, like phishing, are primarily digital. Physical surveillance gaps do not significantly affect the success of such attacks.
- **Physical Theft or Tampering (High):** Directly impacted by surveillance gaps. Without adequate surveillance, the risk of physical theft or tampering with critical systems or sensitive information significantly increases.
- **Man-in-the-Middle (MitM) Attacks (Low):** MitM attacks are executed within network communications. Physical surveillance has little to no effect on the likelihood of such attacks occurring.
- **Supply-Chain Attack (Low):** These attacks target software supply chains and are executed through digital means. Physical surveillance of an organization's own premises has minimal impact on the risk of external supply-chain attacks.

IV. What are the impacts/consequences of compromising the various assets?

Assessing the impacts and consequences of compromising the various assets of Grameena Vikas Bank involves understanding the severity of potential outcomes from successful cyber threats exploiting identified vulnerabilities. The impact is categorized based on the nature of assets involved and the extent to which their compromise could affect the bank's operations, reputation, financial stability, and regulatory compliance.

No.	Type	Name	Description	Non-Exhaustive Involved Assets
1	Customer Data	Financial Loss to Customers	Unauthorized access to customer accounts could lead to direct financial loss through fraudulent transactions.	Critical Servers like HTTP Server and Database Servers, Transaction Approval Process, Core Banking Software, Customer Interface Platforms like online banking
2		Loss of Trust	Compromise of personal and financial information damages customer trust, potentially resulting in a loss of clientele.	Transaction Approval Process, Core Banking Software, Customer Interface Platforms like online banking
3		Identity Theft	Personal information can be used for identity theft, placing customers at long-term risk.	Network and Access Control Infrastructure, Core Banking Software, Customer Interface Platforms like online banking

4	IT Infrastructure and Critical Servers	Service Disruption	Attacks like DDoS can disrupt online banking services, affecting customer access to accounts and transactions.	Critical Servers like HTTP Server and Database Servers, Core Banking Software, Employee Devices, Customer Interface Platforms like online banking
5		Data Loss or Corruption	Malware or insider threats could lead to loss or corruption of critical data, impacting bank operations and requiring costly recovery efforts.	Critical Servers like HTTP Server and Database Servers, Network and Access Control Infrastructure, Core Banking Software, Employee Devices, Customer Interface Platforms like online banking
6		Compromise of Banking Operations	Successful exploitation of vulnerabilities could allow attackers to manipulate account balances, unauthorized transactions, or access sensitive operational information.	Critical Servers like HTTP Server and Database Servers, Employee Authentication System, Network and Access Control Infrastructure, CCTV Surveillance System, Core Banking Software, Employee Devices

7	Financial Assets	Direct Financial Loss	Cyber-attacks resulting in the theft of funds would directly impact on the bank's financial assets.	Critical Servers like HTTP Server and Database Servers, Transaction Approval Process, Core Banking Software, Customer Interface Platforms like online banking
8		Operational Costs	Costs associated with responding to breaches, such as forensic investigations, customer notifications, and system recovery, can be significant.	Critical Servers like HTTP Server and Database Servers, Employee Authentication System, Network and Access Control Infrastructure, CCTV Surveillance System, Core Banking Software, Employee Devices, Customer Interface Platforms like online banking
9		Regulatory Fines	Non-compliance with financial regulations due to a security breach could result in hefty fines.	Critical Servers like HTTP Server and Database Servers, Network and Access Control Infrastructure
10	Software Applications	Exploitation of Functionality	Compromise could lead to the exploitation of banking software for fraudulent purposes.	Critical Servers like HTTP Server and Database Servers, Core Banking Software,

				Customer Interface Platforms like online banking
11		Integrity Loss	Alteration of software logic could result in incorrect transaction processing, affecting financial integrity.	Critical Servers like HTTP Server and Database Servers, Network and Access Control Infrastructure, Core Banking Software, Customer Interface Platforms like online banking
12	Physical Premises and CCTV Systems	Physical Security Breach	Compromise of physical security systems could facilitate unauthorized access to bank premises, leading to theft or vandalism.	CCTV Surveillance System
13		Surveillance Evasion	Disabling or tampering with CCTV systems could help perpetrators avoid detection during or after carrying out physical or cyber-attacks.	CCTV Surveillance System
14	Employee Data and Authentication Systems	Identity and Access Theft	Compromising biometric or other authentication systems could allow unauthorized access to sensitive areas of the bank's network, enabling further attacks.	Employee Authentication System, Network and Access Control Infrastructure, Core Banking Software, Employee Devices, Customer Interface Platforms like online banking
15		Employee Impersonation	Theft of employee credentials or personal information could lead to impersonation attacks,	Employee Authentication System

			further compromising internal systems.	
16	Psychological and Emotional Impact on Employees	Morale and Productivity	A significant breach can create a stressful environment for employees, leading to decreased morale and productivity.	Employee Authentication System, Employee Devices
17		Employee Turnover	High-stress situations and a tarnished company image can lead to increased employee turnover.	Across Multiple Assets
18	Overall Impact Considerations	Reputational Damage	Beyond direct financial and operational impacts, the bank faces long-term reputational damage that can be difficult to recover from.	Critical Servers like HTTP Server and Database Servers, Network and Access Control Infrastructure, CCTV Surveillance System, Core Banking Software, Employee Devices, Customer Interface Platforms like online banking
19		Strategic Impacts	Long-term strategic impacts may include increased security expenditures, loss of competitive edge, and potential shifts in business strategy to recover from or prevent future attacks.	Across Multiple Assets, Employee Devices
20		Legal and Compliance Issues	Breaches often lead to legal challenges, including lawsuits from affected parties and scrutiny from regulators, leading to further financial and reputational damage.	Critical Servers like HTTP Server and Database Servers, Network and Access Control Infrastructure, Core Banking Software,

				Employee Devices, Customer Interface Platforms like online banking
--	--	--	--	---

Understanding these impacts underscores the importance of a comprehensive cybersecurity strategy that not only aims to prevent attacks but also prepares the bank to respond effectively should a compromise occur.

V. What are the cyber risk levels of various cyber assets? Are the controls described helping in lowering the risks? If not, what controls do you need to recommend reducing the risks to various assets.

To determine the cyber risk levels of various assets in Grameena Vikas Bank and assess whether the described controls help in mitigating these risks, we first categorize the assets based on their criticality and exposure to threats, then evaluate the effectiveness of current controls, and finally recommend additional controls as necessary.

Cyber Risk Levels of Various Assets

- **Internet-Facing Servers (HTTP Servers)**
 - **Risk Level: High.** These servers are exposed to the internet, making them prime targets for attacks.
 - **Current Controls:** Use of a network firewall (FortiGate 6500F).
 - **Recommendations:**
 - **Web Application Firewall (WAF):** To specifically protect against web application attacks such as SQL injection and cross-site scripting (XSS).
 - **Regular Vulnerability Scanning and Penetration Testing:** To identify and mitigate vulnerabilities before they can be exploited.
 - **DDoS Protection Measures:** To ensure availability during volumetric attacks.
 - Employ HTTPS rather than HTTP.
- **Database Servers**

- **Risk Level: High.** Contains critical and sensitive financial data.
- **Current Controls:** Segmented network architecture, limiting direct internet access.
- **Recommendations:**
 - **Encryption of Data at Rest and in Transit:** To protect data confidentiality and integrity.
 - **Database Activity Monitoring:** To detect and alert on suspicious activities.
 - **Access Controls and Authentication:** Implement strong authentication methods and enforce the principle of least privilege.
- **Employee Devices (Windows 11 and Windows 10 Machines)**
 - **Risk Level: Medium to High.** The endpoint devices could be exploited to gain entry into the network.
 - **Current Controls:** Unknown specific controls for endpoint protection.
 - **Recommendations:**
 - **Endpoint Detection and Response (EDR) Solutions:** To monitor and respond to threats on endpoints.
 - **Regular Patch Management:** To keep operating systems and applications up to date.
 - **Phishing Awareness Training:** To reduce the risk of social engineering attacks.
- **Core Banking Software**
 - **Risk Level: High.** Central to banking operations and financial transactions.
 - **Current Controls:** Deployed on highly secured network segments.
 - **Recommendations:**
 - **Application Whitelisting:** To ensure only approved software can run.
 - **Secure Development Practices:** If developed in-house, apply secure coding standards and regular security assessments.
 - **Multi-factor Authentication (MFA):** For accessing the application, especially for administrative functions.
- **CCTV Surveillance System**
 - **Risk Level: Medium.** Primarily poses a physical security risk but could be leveraged for further cyber-attacks if compromised.
 - **Current Controls:** Operated on a separate network.
 - **Recommendations:**
 - **Network Segmentation and Firewalls:** Ensure strict segmentation from critical digital assets.

- **Regular Firmware Updates:** To patch vulnerabilities in CCTV hardware.
 - **Secure Access Controls:** Restrict and monitor access to CCTV management interfaces.
- **Customer Interface Platforms (e.g., Online Banking)**
 - **Risk Level: High.** Directly accessible by customers and exposed to the internet.
 - **Current Controls:** Unknown specific controls.
 - **Recommendations:**
 - **MFA for Customers:** To enhance security beyond just passwords.
 - **Customer Education Programs:** On securing their accounts and recognizing phishing attempts.
 - **Regular Security Audits and Compliance Checks:** Ensuring adherence to financial industry security standards and regulations.
 - Implied use of **HTTPS** for encryption.
- **Employee Authentication System**
 - **Risk Level: High.** This system is critical for ensuring that only authorized personnel can access the bank's digital resources. Its compromise could lead to unauthorized access to sensitive areas of the bank's network.
 - **Current Controls:** Use of biometric details for system access.
 - **Recommendations:**
 - **MFA:** Implement multi-factor authentication (MFA) to add an extra layer of security.
 - **Regular assessment:** Regularly update and review authentication protocols and consider behavioral biometrics for continuous authentication.
- **Transaction Approval Process**
 - **Risk Level: Medium to High.** This process is crucial for preventing unauthorized financial transactions, which could lead to significant financial losses.
 - **Current Controls:** Requirement for managerial approval for large transactions.
 - **Recommendations:**
 - **Anomaly Detection Systems:** Deploy systems that automatically flag transactions deviating from normal patterns for further review.
 - **Automated Risk Scoring:** Use software to assign risk scores to transactions based on multiple factors, requiring additional verification for high-risk transactions.

- **Machine Learning for Fraud Detection:** Implement advanced machine learning algorithms to detect potentially fraudulent activity more effectively.
- **Network and Access Control Infrastructure**
 - **Risk Level: High.** This infrastructure underpins the security of the entire banking operation, controlling who accesses what within the bank's network.
 - **Current Controls:** Network segmentation, with different levels of access for staff and critical systems placed in a highly secured network segment.
 - **Recommendations:**
 - **Enhanced Monitoring:** Adopt tools for real-time monitoring of network traffic to detect and respond to unusual activity swiftly.
 - **Zero-Trust Architecture:** Apply a zero-trust framework, requiring verification for every access request, regardless of origin.
 - **Robust Encryption:** Ensure strong encryption standards for all data transmitted within and between network segments.

General Recommendations Across Various Assets

- **Patch Management Program:** Regularly update and patch all systems and software to protect against exploitation of known vulnerabilities.
- **Enhanced Intrusion Detection and Prevention:** Implement advanced IDS/IPS solutions to detect and prevent attacks on the network perimeter and within segmented networks.
- **Security Awareness Training:** Conduct regular, comprehensive training for all employees on recognizing phishing attempts, social engineering tactics, and safe internet practices.
- **Encryption for Data at Rest and in Transit:** Ensure that all sensitive data, especially customer information, is encrypted both when stored and transmitted over networks.
- **Regular Penetration Testing:** Engage in periodic penetration testing to identify and address security weaknesses proactively.
- **Application Security Review:** Conduct security reviews and vulnerability assessments on all critical software applications, focusing on secure coding practices and dependency management.
- **Incident Response and Recovery Plan:** Develop and regularly update an incident response plan to ensure preparedness for detecting, responding to, and recovering from security incidents.
- **Vendor Risk Management:** Assess and monitor the security postures of third-party vendors, especially those with access to the bank's networks or data.

By implementing these recommendations, Grameena Vikas Bank can enhance its cybersecurity posture, protect its assets from potential threats, and ensure the integrity and availability of its banking services. It's important to continually assess and adjust these controls as threats evolve and new vulnerabilities are discovered.