CS668: Practical Cybersecurity
for
Cybersecurity Practitioners

Assignment-4

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 cyber resilience review for the Grameena Vikas Bank, we follow the guidelines outlined in CERT-RMM. The answers to the given questions are discussed below:

For this task, we review the detailed description given, make necessary assumptions about typical functions, and find possible vulnerabilities in this rural bank. The assumptions are stated below, along with a detailed description.

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
G5	**Use of FortiGate 6500F network firewall**	This firewall us susceptible to heap-based buffer overflow vulnerability[8,9]

[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*%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*%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:*

[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

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, 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.
A10	**Encrypted Communication**	Data in transit is encrypted using cryptographic protocols.
A11	**Backup and Recovery Solutions**	Bank has backup servers and recovery solution to aid in the situation of cyber hazards.
A12	**Antivirus Software and Patch Management**	Antivirus softwares are in place to provide first layer of security. Patches are managed appropriately for third party softwares.
A13	**Audit, Review and Compliance management**	Regular audit and reviews are performed to assess security posture of the bank. Bank has complied standards.

I. First thing you need to determine is the scope of the CRR. What business processes are critical for the bank? List the business processes or services that are critical enough that merit a CRR assessment?

Ans: To effectively conduct a Cyber Resilience Review (CRR) for Grameena Vikas Bank, it is crucial to establish a well-defined scope and identify key business processes critical to the bank's operations. This approach ensures a focused assessment, enhancing the bank's ability to safeguard against cybersecurity threats and maintain operational integrity. Below is a table that outlines the scope of the CRR and the critical business processes that aid in systematically enhancing the bank's cyber resilience.

Scope and Critical Business Processes for CRR Assessment

Scope of CRR	Critical Business Process	Description and Importance	Key Services for CRR Assessment	Potential Risks and Why CRR is Needed
Transaction Management	**Transaction Processing System**	Manages all customer transactions, a fundamental operation for the bank's daily functioning and essential for maintaining financial fluidity and customer trust.	**Processing Deposits, Withdrawals, and Transfers**: Ensures these foundational activities are secure and efficient.	**Fraud, Data Breaches, Operational Disruptions**: Critical to review to prevent financial losses and ensure transactional integrity.
Access and Security	**Customer Authentication and Account Management**	Secures login processes and manages account access, crucial for protecting customers from identity theft and unauthorized access.	**Account Logins, Authentication Protocols**: Critical to keep these processes resilient against evolving cybersecurity threats.	**Identity Theft, Phishing, Account Hijacking**: Essential to assess to strengthen defenses against access breaches.
Core Operations	**Core Banking Services**	Involves the software and databases that handle the bank's primary operations, ensuring that financial transactions and customer data are managed accurately and reliably.	**Data Integrity and Transaction Records**: Ensures that the core operations are robust and resistant to attacks.	**Internal/External Breaches, System Failures**: Review needed to protect the heart of banking operations from sophisticated cyber-attacks and failures.
Digital Services	**Digital and Mobile Banking Services**	Provides banking services via digital platforms, increasingly important due to customer demand for remote access, significantly impacting	**Online Banking Transactions, Mobile App Interactions**: Focuses on securing these platforms from cyber threats.	**Cyber-attacks, Software Vulnerabilities, Data Leakage**: Critical for review to secure digital channels and

		customer service and operational efficiency.		protect against data breaches.
Infrastructure	**Network Infrastructure and Internet Connectivity**	Supports critical IT infrastructure for internal operations and customer-facing services, essential for the seamless functioning of banking services.	**Service Connectivity, Branch Communication**: Ensures reliable and secure communication across all bank operations.	**Network Disruptions, DDoS Attacks, Unauthorized Access**: Assessment necessary to safeguard infrastructure from disruptions and unauthorized intrusions.
Security Measures	**Physical and Cybersecurity Measures**	Includes both physical security systems and cybersecurity tools to protect the bank's assets and data, essential for overall security.	**CCTV, Secure Access, Firewalls, Anti-Virus Systems**: Focus on maintaining robust security layers to prevent breaches.	**Physical Breaches, Cyber Intrusions, Data Loss**: Reviewing these measures is crucial to detect vulnerabilities and enhance security protocols.
Compliance and Risk Control	**Compliance and Risk Management**	Ensures the bank adheres to legal and regulatory requirements and manages internal and external risks effectively, crucial for legal compliance and operational integrity.	**Compliance Audits, Risk Assessments, Mitigation Strategies**: Aims to continuously adapt and improve compliance and risk handling.	**Non-compliance Penalties, Operational Disruptions**: CRR is needed to minimize legal risks and optimize risk management practices.

The above table describes each critical business process, explains the importance and essential services involved, details the potential risks, and justifies why a CRR is particularly necessary for each area. This helps understand the scope and depth of the CRR, guiding the bank in prioritizing regions that require focused attention to enhance cyber resilience.

II. What are the critical assets in the organization? What would you ask the person in charge of asset inventory regarding the maturity level of their asset management process?

Ans: For this bank, safeguarding critical assets is paramount to maintaining operational integrity and regulatory compliance. These assets, ranging from financial data to physical and technological resources, form the backbone of the bank's daily operations and security strategies. Identifying and prioritizing these assets helps implement focused protective measures and maintain continuous service delivery. Below is a detailed table categorizing the critical assets essential for the robust functioning of the bank.

Critical Assets in Grameena Vikas Bank

Asset Category	Critical Asset	Description	Importance
Physical Assets (Technology)	**Database Servers**	Linux-based servers hosting core banking databases.	Central to banking operations, holding critical financial data.
	Network Infrastructure Components	Includes the FortiGate 6500F firewall, routers, and switches.	Essential for secure and reliable data flow within and outside the bank.
	Banking Terminals and Workstations	30 Windows 11 and 20 Windows 10 machines used by employees.	Primary interfaces for employees, critical for daily banking operations.
	Physical Security Systems	CCTV systems and biometric access controls.	Provide security to the physical premises, monitor for unauthorized access.
Digital Assets (Technology)	**Core Banking Software**	Software platform managing all major banking functions.	Backbone of banking operations, handling customer accounts and backend data processing.
	Customer Data and Privacy Information	Includes personal data, account details, transaction history.	Highly sensitive, requiring strict security to maintain privacy and comply with laws.

	Internet-Facing Services	Official website, online banking portals, and mobile apps.	Critical for customer interaction and service delivery, vulnerable to cyber-attacks.
Intangible Assets (Process)	**Software and Data Integrity**	Integrity and correctness of software applications and data.	Ensures smooth operation and reliable financial transactions.
	Brand Reputation and Trust	Public perception of the bank as secure and reliable.	Key to customer confidence and competitive advantage.
	Regulatory Compliance	Adherence to financial and data protection regulations.	Mandatory for legal operation, avoiding penalties, and maintaining operational integrity.
People (People)	**Cybersecurity Team and IT Staff**	Employees responsible for managing and securing IT systems.	Crucial for implementing, maintaining, and improving the security measures and technologies.
	Employee Training and Awareness	Training programs and awareness initiatives for all bank staff.	Key to ensuring that all employees understand their role in safeguarding bank assets and preventing breaches.
	Management and Leadership	Leadership roles that define security policies and procedures.	Important for strategic decision-making and prioritizing cybersecurity investments and practices.

To thoroughly assess the maturity of the asset management process, it is essential to ask targeted questions to the person responsible for asset inventory. These questions are designed to evaluate the asset management system's completeness, effectiveness, and integration within the bank's broader operational framework. The following table lists the key questions that will help us understand the robustness of the bank's asset management practices to ensure that critical assets are well-managed and protected.

Questions to Assess Asset Management Maturity

Area of Focus	Questions to Ask	Purpose of Evaluation
Inventory Completeness	Are there automated systems in place for asset tracking, and how	To evaluate the use of technology in maintaining an up-to-date and accurate asset inventory.

	are they integrated with other IT management systems?	
	How frequently is the asset inventory updated, and what mechanisms are in place to ensure its accuracy and completeness?	To assess the effectiveness and reliability of the inventory management process.
Asset Classification	How are assets classified according to their criticality and sensitivity? What criteria are used for this classification?	To understand the criteria and process for prioritizing assets, which impacts how security resources are allocated.
	How do you ensure that critical assets receive the highest level of protection and regular reviews?	To determine if there's a structured approach to asset protection based on risk and criticality.
Risk Management	How is the asset inventory integrated with the organization's broader risk management framework?	To understand the role of asset management in overall risk mitigation strategies.
	How frequently are risk assessments conducted on critical assets, and how do these assessments influence security practices?	To evaluate proactive measures taken to identify and mitigate risks associated with critical assets.
Security Measures and Controls	What security controls are associated with high-risk or critical assets?	To identify specific security controls implemented to protect high-risk assets and evaluate their effectiveness.
	How do you ensure these controls are effectively implemented and maintained?	To assess the operational effectiveness and maintenance of security controls over time.
Compliance and Regulation	How does the asset management process ensure compliance with relevant regulatory requirements?	To confirm that asset management practices align with legal and regulatory frameworks, minimizing compliance risks.
	Are there regular audits or reviews to verify compliance with these standards?	To gauge the thoroughness and frequency of compliance verification processes.
Documentation and Reporting	What documentation is maintained for asset management, and how is this information secured?	To check for the availability and security of documentation, which is crucial for audits and historical analysis.
	Who has access to this documentation, and how is this access controlled?	To assess control measures in place for sensitive asset management information, preventing unauthorized access.

Training and Awareness	What training do staff receive regarding asset management responsibilities?	To assess the level of knowledge and competency in asset management among staff.
	How is awareness about the importance of asset management maintained across the organization?	To understand how ongoing awareness and importance of asset management are promoted within the bank.
Incident Response and Asset Recovery	What processes are in place for responding to security incidents related to asset compromise?	To understand the readiness and procedural steps for addressing security incidents affecting assets.
	How do you manage the recovery or replacement of critical assets in the event of a failure or security incident?	To evaluate the plans and capabilities in place for the timely recovery or replacement of critical assets.

The questions outlined in the table are crucial for understanding the bank's asset management maturity. By addressing these areas, the bank can identify opportunities for enhancement, ensure compliance with regulatory standards, and strengthen its overall cybersecurity posture to safeguard critical assets effectively.

(iii) What are the most likely controls present in the cyber infrastructure of the bank? What would you look for in their control management practices to determine the maturity level of their control management?

Ans: Grameena Vikas Bank employs robust cybersecurity controls to safeguard its operations and sensitive data. These controls are designed to protect against various cyber threats, secure critical information, and ensure the integrity of the bank's IT infrastructure. The table below categorizes and details these essential controls, explaining their roles and importance in maintaining the security of the bank's systems and operations. This structured overview is crucial for understanding how Grameena Vikas Bank mitigates potential security risks and maintains compliance with regulatory standards.

Cybersecurity Controls in Grameena Vikas Bank

Control Category	Likely Controls	Purpose and Functionality
Network Security	**Firewalls (FortiGate 6500F)**	To monitor and control incoming and outgoing network traffic based on predetermined security rules.
	Intrusion Detection Systems (IDS)	To detect unauthorized access or anomalies in network traffic and alert the security team.
Access Control	**Multi-Factor Authentication (MFA)**	To enhance security by requiring multiple forms of verification from users when accessing sensitive systems.
	Role-Based Access Control (RBAC)	To limit access to information based on the individual user’s role within the organization.
Data Protection	**Data Encryption**	To protect data at rest and in transit, making it unreadable without the correct decryption key.
	Backup and Recovery Solutions	To ensure data continuity by regularly backing up data and providing means for data recovery in case of loss.
Endpoint Security	**Antivirus/Antimalware Software**	To protect against viruses, malware, and other malicious software threats.
	Patch Management	To keep software up to date and secure by regularly applying patches and updates to eliminate vulnerabilities.
Physical Security	**Biometric Access Controls**	To restrict physical access to critical infrastructure, using biometric indicators like fingerprints.
	Surveillance Cameras (CCTV)	To monitor physical premises and deter unauthorized access or detect intruders.
Compliance and Standards	**Regular Security Audits**	To evaluate the effectiveness of security measures and ensure compliance with regulatory requirements.
	Compliance Management Software	To help manage and maintain records of compliance with standards like GDPR, PCI DSS, etc.

To thoroughly assess the maturity level of control management practices, evaluating a range of specific elements demonstrating how effectively the bank implements and maintains its cybersecurity controls is crucial. The evaluation should encompass various aspects, from policy documentation to compliance, ensuring a comprehensive understanding of the bank's ability to safeguard its operations against cyber threats. The table below outlines key evaluation areas and the specific elements within those areas to examine, providing a structured approach to determine the robustness and sophistication of the bank's control management practices.

Evaluating Maturity in Control Management Practices

Aspect of Control Management	What to Look For	Purpose of Evaluation
Policy and Procedure Documentation	Written policies and procedures detailing control management practices.	To ensure there are formal, documented policies guiding the implementation and management of controls.
	Regular updates and reviews of these documents.	To verify that policies and procedures are kept current with evolving threats and technology.
Control Implementation	Implementation strategies for various controls (e.g., firewalls, encryption).	To assess the effectiveness and appropriateness of control deployment within the bank's infrastructure.
	Integration of controls with existing systems and processes.	To determine how well controls are integrated into the organizational workflow and IT systems.
Training and Awareness	Training programs for staff on the importance and usage of controls.	To evaluate the level of awareness and understanding among employees regarding control measures.
	Continuous education on new threats and control updates.	To ensure staff are continually updated on the latest security threats and how controls mitigate these risks.
Monitoring and Review	Regular audits and reviews of control effectiveness.	To check the efficiency and effectiveness of existing controls in real-time operations.
	Incident response testing and adjustments based on findings.	To test how controls perform under simulated breach scenarios and how the system adapts based on these tests.

Compliance and Reporting	Alignment with industry standards and regulatory requirements.	To confirm that control management practices meet required compliance standards (e.g., GDPR, PCI DSS).
	Reporting mechanisms for control failures and security incidents.	To assess the robustness of the bank’s reporting system in tracking and documenting security lapses.
Performance Metrics and Monitoring	Tools and technologies used for monitoring control effectiveness.	To evaluate the technical capabilities used to monitor and measure the performance of security controls.
	Metrics for measuring response times and effectiveness during security incidents.	To assess the responsiveness and effectiveness of the incident response plan and control mechanisms.
Testing and Audits	Frequency and methodology of testing (e.g., penetration testing, security audits).	To determine the thoroughness and frequency of proactive security testing and evaluations.
	Insights and actions from recent audit reports.	To understand how audit findings are used to improve security practices and control implementations.
Incident Management and Response	Established and tested incident response plans.	To verify the readiness and efficacy of plans to manage and mitigate security incidents effectively.
	Processes for recovery from security incidents and system restoration.	To evaluate the bank's ability to quickly recover and restore normal operations after a security incident.
Feedback Mechanisms	Internal mechanisms for staff to report issues or suggest improvements.	To assess how well the organization captures and integrates internal feedback for continuous improvement.
	Integration of feedback from external audits into the control management process.	To determine the effectiveness of incorporating external insights into refining control management practices.

This table provides a comprehensive overview of the aspects of the control management practices at Grameena Vikas Bank that need to be examined to assess their maturity. These factors cover everything from the foundational policies and procedures through the implementation and regular review of controls to the integration of advanced technologies and compliance adherence. Such a thorough evaluation helps determine the bank's control management system's robustness, responsiveness, and effectiveness.

(iv) What would you check in their configuration management practice to determine the maturity level of configuration management?

Ans: To effectively assess the maturity level of configuration management practices, it's essential to review several key areas that reflect their thoroughness, security, and efficiency. A structured evaluation of these areas ensures that the bank's IT configurations align with best practices, support security measures, and facilitate smooth operational continuity. The following table outlines specific elements to examine across various aspects of configuration management, providing a clear framework for a comprehensive maturity assessment.

Evaluating Maturity in Configuration Management Practices

Aspect of Configuration Management	What to Check	Purpose of Evaluation
Standardization	Whether there are standardized configuration baselines for all hardware and software.	To ensure that all systems are configured according to industry best practices and internal standards to minimize risks.
Change Management	Procedures for making changes to system configurations, including approval processes.	To verify that all changes are controlled and documented, reducing the risk of unauthorized changes that could introduce security vulnerabilities.
Automation	Use of automation tools to manage configurations and ensure consistency.	To assess the extent to which the bank reduces human error and enhances efficiency in configuration management.
Version Control	Systems in place for version control of configuration changes.	To check that all changes are tracked over time, allowing for rollback if necessary and understanding the evolution of the configuration landscape.

Compliance Monitoring	Regular checks to ensure configurations comply with security policies and standards.	To confirm that configurations remain in compliance with regulatory requirements and best security practices over time.
Security Features	Security measures integrated into configuration management, such as encryption.	To evaluate how security is embedded in configuration practices to protect data and maintain system integrity.
Audit and Review	Frequency and methodology of audits to assess configuration settings and compliance.	To determine how thoroughly and frequently the configuration settings are audited to ensure ongoing compliance and security.
Documentation	Quality and accessibility of documentation for configuration management practices.	To ensure there is clear, detailed, and easily accessible documentation that supports the configuration management process and training.
Training and Awareness	Training programs available for staff involved in configuration management.	To evaluate if staff are adequately trained to manage configurations securely and respond to related issues effectively.
Incident Response Integration	Integration of configuration management in the incident response plan.	To check if configuration management is considered during incident response to quickly mitigate risks and restore services.
Disaster Recovery and Backup Configurations	Regular testing and updating of backup configurations.	To ensure that backup configurations are always current and effective, enhancing the ability to restore systems quickly after an incident.
	Inclusion of configuration restoration in disaster recovery plans.	To verify that configuration restoration is an integral part of disaster recovery, ensuring continuity and resilience in crisis situations.

This table provides a comprehensive approach to evaluate the maturity of configuration management at Grameena Vikas Bank. Each aspect focuses on ensuring that configuration practices are robust, secure, and capable of effectively supporting the organization's overall cybersecurity posture.

(v) What would you check in their service continuity management practices to determine the maturity level of service continuity management?

Ans: To thoroughly assess the maturity level of service continuity management practices at Grameena Vikas Bank, it is crucial to scrutinize several key areas. These areas provide insight into how well-prepared the bank is to handle disruptions and recover operations efficiently. Understanding these elements will help determine the bank's continuity strategies' robustness and alignment with best practices. The following table offers a structured approach detailing specific areas and elements to examine, ensuring a comprehensive evaluation of the bank's preparedness to sustain services during unforeseen events.

Evaluating Maturity in Service Continuity Management Practices

Aspect of Service Continuity Management	What to Check	Purpose of Evaluation
Business Continuity Plan (BCP)	Existence, accessibility, and comprehensiveness of the BCP.	To ensure the BCP is formalized, readily available, and covers all critical functions and resources.
Disaster Recovery Plan (DRP)	Specificity of recovery strategies for IT systems and data, and alignment with business needs.	To verify that the DRP includes detailed and applicable recovery strategies that match the bank's operational requirements.
Plan Testing and Updates	Frequency and effectiveness of BCP/DRP testing; regularity of updates and revisions.	To assess how regularly and effectively the plans are tested and kept up-to-date with organizational needs.
Employee Training and Awareness	Training programs and awareness initiatives related to continuity roles and procedures.	To evaluate the extent and effectiveness of training and ongoing awareness programs for staff.
Incident Response Team	Existence of a dedicated team, team training, and readiness.	To check the preparedness and specific training of the incident response team for managing disruptions.

Communication Plans	Internal and external communication strategies during disruptions.	To ensure all stakeholders are effectively informed during a crisis, maintaining trust and operational integrity.
Resource Availability	Availability of backup and financial resources to support recovery and continuity efforts.	To confirm the availability of critical resources like alternative sites, hardware, and financial means for recovery.
Integration with Third Parties	Vendor dependencies, integration of vendor continuity plans, and specifics in SLAs.	To assess risks associated with third-party services and ensure their continuity plans align with the bank's strategies.
Continuous Improvement	Mechanisms for feedback and continuous improvement in continuity practices.	To ensure the plan evolves based on lessons learned and changing organizational needs.
Audit and Review	Regular audits of the service continuity practices and effectiveness of implementations.	To confirm the plan's effectiveness and identify areas for improvement, ensuring it meets compliance and business needs.

The structured assessment provided in the table offers a comprehensive framework to evaluate the maturity of service continuity management practices at Grameena Vikas Bank. By meticulously reviewing these critical areas, the bank can identify strengths and potential areas for improvement in its preparedness strategies. This ensures that Grameena Vikas Bank is ready to handle unexpected disruptions and maintain essential operations effectively, minimizing service impact and preserving customer trust during challenging times.

vi) What would you check in their situational awareness practices to determine the maturity level of situational awareness domain?

To effectively assess the maturity level of situational awareness practices at Grameena Vikas Bank, it is crucial to examine various components that determine how well the bank monitors, understands and responds to changes and threats in its operational environment. This assessment involves reviewing the bank's capabilities in gathering threat intelligence, managing incidents, and maintaining continuous communication, among other key areas. The following table categorizes these components into specific evaluation areas, providing a detailed and structured approach to understanding how prepared the bank is to identify and manage emerging security challenges. This analysis is essential for ensuring that Grameena Vikas Bank remains vigilant and responsive to cybersecurity threats in the dynamic landscape.

Evaluating Maturity in Situational Awareness Practices

Aspect of Situational Awareness	What to Check	Purpose of Evaluation
Threat Intelligence Gathering	Diversity and reliability of sources for threat intelligence; Timeliness of integration.	To assess the scope and speed at which new intelligence is integrated into security measures, ensuring rapid response to emerging threats.
Security Information and Event Management (SIEM)	Integration across networks and critical assets; Real-time monitoring capabilities.	To verify the extent of SIEM integration and its capability for immediate analysis of alerts, ensuring comprehensive coverage and swift action.
Regular Security Assessments	Frequency and comprehensiveness; Adaptiveness to new threats and changes.	To determine how frequently and thoroughly security landscapes are reviewed and how quickly the bank adapts its assessments to new information.
Employee Training and Drills	Regularity and content of cybersecurity training; Frequency and effectiveness of drills.	To evaluate the thoroughness and impact of training and simulated threat scenario drills on employee preparedness and responsiveness.
Communication of Threat Information	Effectiveness of internal communication channels; Clarity and actionability of information.	To ensure that threat information is communicated effectively within the organization, allowing timely and appropriate responses.

Incident Response and Escalation Procedures	Detail and existence of response plans; Escalation processes.	To check the readiness and detailed planning for different types of security incidents and the effectiveness of escalation procedures.
Collaboration with External Entities	Engagement with industry groups; Partnerships with security firms.	To assess the level and effectiveness of external collaborations that enhance the bank's security capabilities and situational awareness.
Feedback and Improvement Mechanisms	Presence of internal and external feedback loops; Continuous improvement practices.	To determine how feedback is utilized to refine situational awareness and response strategies, fostering a culture of continuous improvement.

The assessment in the table offers a comprehensive framework to evaluate the maturity of situational awareness practices at Grameena Vikas Bank. By systematically reviewing these critical areas, the bank can identify areas of strength and opportunities for improvement, ensuring that it is fully equipped to detect and respond to potential security threats proactively. This thorough evaluation is crucial for maintaining the bank's resilience, safeguarding its assets, and upholding the trust of its customers in an ever-evolving threat landscape.