**INFORMATION SECURTIY CS-3002**

**JS BANK THREAT AND RISK ASSESSMENT**

A picture containing text, gear, metalware

Description automatically generated

**PROJECT REPORT**

**SUBMITTED TO:**

Ms. Yusra Kaleem

**GROUP MEMBERS:**

INSHA SAMNANI **20K-0247**

ISMAIL AHMED ANSARI **20K-0228**

YUSRA ADAM **20K-0207**

**70 QUESTIONS AND ANSWERS**

**FINANCIAL SECTOR (JS BANK)**

**Introduction:**

Established in 2006, JS Bank has evolved significantly since its inception, originating from the acquisition of Citicorp Investment Bank Limited. With a robust presence in both domestic and international markets, the bank has become a dynamic financial institution. Recognized for excellence in digital financial services, SME, and consumer lending, JS Bank, a part of the JS Group, remains dedicated to making a positive impact on the lives of its customers. Committed to a secure financial relationship, the bank emphasizes ongoing efforts to enhance security parameters, acknowledging the prevalent risks in today's digital landscape. In the ever-evolving realm of cyber threats, JS Bank ensures continuous vigilance while providing a safe and secure banking experience for its customers.

**Services provided by JS Bank:**

1. **Security Measures:**

The advisory assures customers that JS Bank prioritizes the protection of personal information. Multiple layers of security are implemented in both mobile and internet banking services to prevent unauthorized access. Importantly, JS Bank emphasizes that it will never request personal information through email, phone, or SMS.

1. **Highlighting of common Types of Internets and Mobile Banking Fraud:**

JS Bank highlights several common types of fraud, including phishing/scamming, malware and viruses, mobile fraud, and text message fraud (smishing). It emphasizes that fraudsters employ sophisticated tools to deceive users and gain access to financial information.

1. **Customer Tips for Security:**

JS Bank provides customers with practical tips to enhance their information security, including avoiding sharing personal information, creating strong passwords, using secure methods on public computers, and promptly reporting lost or stolen mobile phones.

1. **Security Advisory Contacts:**

Customers are urged to report any suspicious emails, websites, or SMS messages to JS Bank through the dedicated helpline at 0800-011-22.

1. **Privacy Guardian Services:**

**5.1- Handling Personal Information:** JS Bank respects the privacy of personal information provided by customers. The Privacy Statement outlines the purposes for which the information may be used, including providing requested services, conducting credit checks, and improving services based on customer feedback.

**5.2- Information Disclosure:** The statement clarifies that customer details may be disclosed to entities within the JS Bank Group, regulatory authorities, service providers, credit reference agencies, and other relevant parties for specified purposes. JS Bank emphasizes secure and confidential treatment of transferred information.

**5.3- Cookies and Internet Communications and Web Tracking:**

JS Bank occasionally uses cookies to enhance internet services. These cookies help recognize users' interests, enable access to online services, and provide statistical information for website improvement.

**5.4- Monitoring Internet Communications:**

To maintain system security and prevent unauthorized activities, JS Bank reserves the right to monitor all internet communications, including web and email traffic.

**ANSWERS TO 70 QUESTIONS**

**Q1: Do you conduct robust and frequent end-user cybersecurity awareness training?**

**A1: Yes,** JS Bank conducts regular and comprehensive cybersecurity awareness training programs for end-users to ensure they are well-informed about potential risks and security best practices.

**Q2: Have you taught everyone how to securely store passwords or passphrases?**

**A2: Yes,** JSBank has implemented training sessions to educate staff and customers on secure password practices, emphasizing the importance of strong, unique passwords or passphrases.

**Q3: Do you conduct quarterly anti-phishing, smishing, and vishing campaigns?**

**A3: Yes,** JS Bank regularly organizes anti-phishing, smishing, and vishing campaigns to simulate real-world scenarios, assess the readiness of employees and customers, and enhance their ability to recognize and respond to potential threats.

**Q4: Does everyone in your organization understand the risk associated with cybersecurity, the common ploys used by threat actors, and how to report any suspicious activities for further investigation?**

**A4: Yes,** JS Bank ensures that all employees are well-versed in the risks associated with cybersecurity. They are trained to recognize common tactics employed by threat actors and are encouraged to promptly report any suspicious activities for thorough investigation.

**Q5: Are all vendor default accounts changed or disabled?**

**A5: Yes,** JS Bank ensures that default accounts from vendors are either changed or disabled to prevent unauthorized access and enhance the overall security of the system.

**Q6: Are only necessary services, protocols,** **daemons, and functions enabled?**

**A6: Yes,** JS Bank employs a strict policy to enable only essential services, protocols, daemons, and functions, minimizing potential vulnerabilities and reducing the attack surface.

**Q7: Is all unnecessary functionality removed or disabled?**

**A7: Yes,** JS Bank takes measures to remove or disable any unnecessary functionality, reducing the complexity of the system and mitigating the risk of potential security breaches.

**Q8: Are all accounts immediately disabled or deleted upon termination of employment?**

**A8: Yes,** JS Bank follows a robust account management process, ensuring that accounts are promptly disabled or deleted when an employee's tenure terminates, preventing unauthorized access.

**Q9: Are all screen idle times set for 15 minutes, and do they require re-authentication to unlock?**

**A9: Yes,** JS Bank enforces a security policy where screen idle times are set to 15 minutes, and re-authentication is required to unlock, enhancing protection against unauthorized access in case of inactivity.

**Q10. Do you provide end** **users a tool to save all passwords (preferably cloud-based for home and work use)?**

**A10: No,** JS Bank does not provide a specific tool for end users to save passwords, aiming to avoid potential security risks associated with centralized storage of sensitive information.

**Q11: Have you developed an administrator (admin) and user password or passphrase policy that eliminates the use of common or easy-to-guess passwords?**

**A11: Yes,** JS Bank has implemented a robust password policy for both administrators and users, discouraging the use of common or easily guessable passwords to enhance security measures.

**Q12: Are all end point logs being ingested by a smart technology that uses threat intelligence and artificial intelligence (AI) based on threat actor activities and heuristics?**

**A12: Yes,** JS Bank employs a sophisticated system that ingests end point logs using smart technology, integrating threat intelligence and AI to analyze threat actor activities and heuristics for proactive cybersecurity.

**Q13: Do you harden all endpoints and remove everything that is not needed for job functionality?**

**A13: Yes,** JS Bank follows a security practice of hardening all endpoints by eliminating unnecessary components, focusing on job functionality to minimize potential vulnerabilities.

**Q14: Do you have next-generation anti-malware protection (e.g., managed detection and response [MDR], extended detection and response [XDR], endpoint detection and response [EDR])4 on all endpoints that utilizes a threat intelligence-based security analytics platform with built-in security context?**

**A14: Yes,** JS Bank has implemented next-generation anti-malware protection across all endpoints, incorporating technologies like MDR, XDR, and EDR. This system utilizes a threat intelligence-based security analytics platform with built-in security context for enhanced protection.

**Q15: Do you prevent non-enterprise-controlled and secured devices from connecting to any portion of your network?**

**A15: Yes,** JS Bank enforces measures to prevent non-enterprise-controlled and unsecured devices from accessing any part of the network, ensuring a controlled and secure environment.

**Q16: Do all endpoints have personal firewalls for accessing the Internet when not attached to the enterprise network?**

**A16: Yes,** each endpoint at JS Bank is equipped with personal firewalls for secure Internet access when disconnected from the enterprise network, adding an additional layer of protection.

**Q17: Do all endpoints have antivirus software installed that cannot be disabled and is automatically updated when new updates are available?**

**A17: Yes,** JS Bank ensures that all endpoints have antivirus software installed, which cannot be disabled by end users. The software is configured to receive automatic updates whenever new updates are available, maintaining the latest threat protection.

**Q18: Do all endpoints have a next-generation anti-malware application installed?**

**A18: Yes,** JS Bank has deployed next-generation anti-malware applications on all endpoints, enhancing the overall security posture with advanced malware protection measures.

**Q19: Are all logs stored for at least 2 years?**

**A19: Yes**, JS Bank ensures that all logs are stored for a minimum of 2 years, meeting regulatory requirements and providing an extensive historical record for analysis.

**Q20: Are all devices generating logs?**

**A20: Yes,** all devices within JS Bank's network generate logs, ensuring comprehensive coverage for monitoring and analysis of activities across the entire infrastructure.

**Q21: Are all logs being reviewed daily by inside and/or outside sources?**

**A21: Yes,** JS Bank conducts daily reviews of logs by both internal and external sources, enhancing the detection of any suspicious activities and ensuring a proactive response to potential security incidents.

**Q22: Do you have a mature and well-organized cybersecurity incident response (in-house or in conjunction with third parties) that thoroughly investigates all incidents?**

**A22: Yes,** JS Bank has established a mature and well-organized cybersecurity incident response system. It includes both in-house capabilities and collaboration with third parties to ensure thorough investigations of all incidents, enhancing the overall resilience of the security infrastructure.

**Q23: Do you only give employees the tools and access needed to perform their job functions, and nothing else?**

**A23: Yes,** JS Bank strictly adheres to the principle of least privilege, providing employees with only the tools and access required for their job functions. This approach minimizes the attack surface and reduces the risk of unauthorized access or activities.

**Q24: Do you utilize the principle of least privilege?**

**A24: Yes**, JS Bank utilizes the principle of least privilege. This means that access rights and permissions are assigned at the minimum levels necessary for employees to perform their job functions, reducing the risk of unauthorized access and potential security breaches.

**Q25: Do you deploy a zero-trust model?**

**A25: Yes**, JS Bank deploys a zero-trust model. This approach ensures that trust is never assumed and that every user and device, both inside and outside the network, is continuously verified before granting access. This enhances overall security by minimizing the risk of unauthorized access and potential security threats.

**Q26: Do you require multifactor authentication (MFA) for all connections outside network?**

**A26: Yes**, JS Bank requires multifactor authentication (MFA) for all connections outside the network. This additional layer of security helps verify the identity of users accessing the network from external sources, reducing the risk of unauthorized access, and enhancing overall cybersecurity.

**Q27: Do you require MFA for internal authenticated network users to access key infrastructure and data inside the network (i.e., the crown jewels)?**

**A27: Yes**, JS Bank requires multifactor authentication (MFA) for internal authenticated network users to access key infrastructure and sensitive data inside the network, including the crown jewels. This ensures an extra layer of protection against unauthorized access and enhances the security of critical assets within the organization.

**Q28: Do you manage all credentials in an order that allows you to quickly conduct a password reset for every account on your network? (This includes service accounts.)**

**A28: Yes**, JS Bank manages all credentials in an organized manner that enables the quick conduct of a password reset for every account on the network, including service accounts. This proactive approach ensures efficient credential management and enhances the overall security of the network by promptly addressing any potential security threats related to passwords.

**Q29: Have you recently assessed your Active Directory to ensure that it is properly configured and secured?**

**A29: Yes**, JS Bank recently assessed its Active Directory to ensure proper configuration and security. Regular assessments help identify and address any vulnerabilities or misconfigurations, enhancing the overall security posture of the network and ensuring the robustness of the Active Directory environment.

**Q30: Are you actively monitoring the security of your Active Directory?**

**A30: Yes**, JS Bank is actively monitoring the security of its Active Directory. Continuous monitoring is crucial for promptly detecting and responding to any security incidents or anomalies, contributing to the overall cybersecurity resilience of the organization.

**Q31: Do your perimeter firewalls have a deny-all rule unless otherwise authorized?**

**A31:** **Yes,** JS Bank has implemented a deny-all rule on its perimeter firewalls unless otherwise authorized. This practice enhances network security by restricting unauthorized access and potential threats at the network perimeter.

**Q32: Is your demilitarized zone (DMZ) secured?**

**A32: Yes**, JS Bank has implemented security measures to ensure the demilitarized zone (DMZ) is secured. This enhances the protection of the network by establishing a secure intermediary zone that adds an extra layer of defense against potential threats.

**Q33: Has it been ensured that there are no data, databases or stored accounts on the DMZ?**

**A33: Yes**, JS Bank ensures that there are no data, databases, or stored accounts on the DMZ. This practice enhances security by minimizing potential points of vulnerability in the demilitarized zone.

**Q34: Do you deploy anti-spoofing technology to prevent forged IP addresses from entering the network?**

**A34: Yes**, JS Bank deploys anti-spoofing technology to prevent forged IP addresses from entering the network. This measure enhances the network's security by mitigating the risk of unauthorized access through IP address manipulation.

**Q35: Do you prevent the disclosure of internal IP address and routing information on the Internet?**

**A35: Yes**, JS Bank implements measures to prevent the disclosure of internal IP addresses and routing information on the Internet. This practice helps enhance security by minimizing the exposure of sensitive network details to potential attackers.

**Q36: Do you segment key infrastructure from other parts of the network with restrictive firewalls (e.g., segmenting Wi-Fi, confidential data, virtual machines and printers away from crown jewels)?**

**A36: Yes**, JS Bank employs network segmentation with restrictive firewalls to separate key infrastructure from other parts of the network. This segmentation enhances security by isolating critical components such as Wi-Fi, confidential data, virtual machines, and printers, reducing the risk of unauthorized access to crown jewels.

**Q37: Are procedures defined and implemented to protect cryptographic keys used to protect stored data against disclosure and misuse?**

**A37: Yes**, JS Bank has well-defined procedures and implementations to protect cryptographic keys used to safeguard stored data. These measures are in place to prevent the unauthorized disclosure and misuse of cryptographic keys, ensuring the security of stored data.

**Q38: Are cryptographic keys stored in the fewest possible locations with at least dual custodians?**

**A38: Yes**, cryptographic keys at JS Bank are stored in the fewest possible locations, and the bank follows a dual custodian approach to enhance the security of these keys. This ensures a robust and secure management of cryptographic keys.

**Q39: Do you utilize full disk encryption on all appropriate drives?**

**A39: Yes**, JS Bank utilizes full disk encryption on all appropriate drives. This security measure helps protect sensitive data in case of unauthorized access to physical devices.

**Q40: Do you use secure encryption in motion-at least Transport Layer Security (TLS) 1.1 or higher?**

**A40: Yes**, JS Bank uses secure encryption in motion, specifically Transport Layer Security (TLS) 1.1 or higher. This ensures the secure transmission of data over networks, safeguarding customer information during online transactions and communications.

**Q41: Is all non-console administrative access encrypted using strong cryptography?**

**A41: Yes**, all non-console administrative access at JS Bank is encrypted using strong cryptography. This security measure ensures that unauthorized access attempts are thwarted, protecting sensitive administrative information.

**Q42: Do you perform periodic targeted threat hunts?**

**A42: Yes**, JS Bank conducts periodic targeted threat hunts to proactively identify and mitigate potential threats. This approach enhances the bank's cybersecurity posture by staying vigilant against evolving security risks.

**Q43: Do you ingest current threat intelligence (preferably from more than one source) and have a procedure to implement rapid countermeasures based on good threat intelligence?**

**A43: Yes**, JS Bank regularly ingests current threat intelligence from multiple sources and has established procedures to implement rapid countermeasures based on this information. This proactive approach helps enhance the bank's ability to respond effectively to emerging threats.

**Q44: Does it include performing routine dark web reconnaissance to learn what exists on the dark web about your brand and enterprise structures?**

**A44: Yes**, JS Bank includes routine dark web reconnaissance as part of its cybersecurity strategy to gain insights into what information exists on the dark web related to its brand and enterprise structures. This practice helps the bank stay informed about potential threats and vulnerabilities.

**Q45: Do you closely monitor all vendor and third-party supply-chain connections for compliance and untoward issues?**

**A45: Yes**, JS Bank closely monitors all vendor and third-party supply-chain connections for compliance and untoward issues as part of its cybersecurity and risk management practices. This ensures that the bank's partners adhere to security standards and do not pose potential risks to the organization.

**Q46: Do you conduct at least 1 penetration test annually, performed by a third party?**

**A46: Yes**, JS Bank conducts at least one penetration test annually, which is performed by a third party. This practice helps identify vulnerabilities and assess the effectiveness of the bank's security measures against potential cyber threats.

**Q47: Do you conduct routine vulnerability scans and remediate all vulnerabilities a Common Vulnerability Scoring System (CVSS) score of 4 or more within 30 days, and all other vulnerabilities within 90 days?**

**A47: Yes**, JS Bank conducts routine vulnerability scans and follows a remediation process. Vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 4 or more are addressed within 30 days, and all other vulnerabilities are remediated within 90 days. This approach ensures a timely response to identified security weaknesses, contributing to the overall cybersecurity of the bank.

**Q48: Do you routinely scan your Internet-facing infrastructure for penetration and vulnerabilities?**

**A48:** **Yes,** JS Bank routinely conducts scans on its Internet-facing infrastructure to identify and address potential penetration and vulnerabilities. This proactive measure contributes to the ongoing security assessment of the bank's external-facing systems.

**Q49: Do you perform an annual business impact analysis/risk analysis report with insider and outside auditors?**

**A49:** **Yes,** JS Bank performs an annual business impact analysis and risk analysis report in collaboration with both insider and outside auditors. This comprehensive assessment helps identify potential risks and impacts on the business, contributing to strategic decision-making and ongoing improvements in risk management.

**Q50: Do you have an enterprise security policy that is at least updated annually and understood by all the parties to which it applies?**

**A50:** **Yes,** JS Bank has an enterprise security policy that is updated annually, and efforts are made to ensure that all relevant parties, including employees and stakeholders, understand and comply with the policy. This regular updating and communication enhance the effectiveness of security measures across the organization.

**Q51: Do you have a formal change control policy?**

**A51: Yes,** JS Bank has implemented a formal change control policy. This policy outlines structured procedures for initiating, reviewing, approving, and implementing changes within the organization's IT infrastructure. The formal change control policy helps maintain the stability and security of the bank's systems.

**Q52: Are processes and mechanisms for restricting physical access to servers, consoles, backup, and network equipment in place and properly safeguarded?**

**A5**2: **Yes**, JS Bank has established processes and mechanisms to restrict physical access to servers, consoles, backup, and network equipment. These measures are in place to ensure the physical security and safeguarding of critical infrastructure components.

**Q53: Are physical and/or logical controls implemented to restrict the use of publicly accessible network jacks within the facilities?**

**A53:** **Yes**, JS Bank has implemented both physical and logical controls to restrict the use of publicly accessible network jacks within its facilities. These controls contribute to the overall security of the network infrastructure and help prevent unauthorized access.

**Q54: Do you have a robust cyber incident response plan (CIRP) that is reviewed and practiced yearly? The CIRP should be routinely updated, and the core and extended incident response teams should practice responses at least annually using tabletop or functional cybersecurity exercises.**

**A54:** **Yes**, JS Bank has a comprehensive cyber incident response plan (CIRP) that undergoes regular reviews and annual practice sessions. Both core and extended incident response teams participate in tabletop or functional cybersecurity exercises to ensure preparedness and effectiveness in responding to potential cyber incidents

**Q55: Do you have playbooks with technical instructions for handling common cybersecurity incidents?**

**A55: Yes**, JS Bank has developed playbooks containing technical instructions for handling common cybersecurity incidents. These playbooks serve as valuable resources for incident response teams, providing structured guidance to effectively address and mitigate specific types of cyber threats.

**Q56: Do you have thorough diagrams of the entire network, including Wi-Fi?**

**A56:** **Yes**, JS Bank maintains thorough diagrams of the entire network, encompassing both wired and Wi-Fi components. These diagrams provide a visual representation of the network architecture, aiding in understanding and managing the overall infrastructure effectively.

**Q57: Do you have a complete inventory of all assets that includes business criticality levels, owners, co-owners, and restoration? Does this inventory include instructions with time periods to recover?**

**A57:** **Yes**, JS Bank maintains a comprehensive inventory of all assets, including business criticality levels, owners, co-owners, and restoration instructions. This inventory provides essential information for effective asset management and includes instructions with defined time periods for recovery in case of disruptions.

**Q58: Do you have a full set of data flow diagrams?**

**A58:** **Yes**, JS Bank has a complete set of data flow diagrams that illustrate the flow of information within the organization's systems. These diagrams help visualize the movement of data, enhancing the understanding of data processes and aiding in the implementation of effective security measures.

**Q59: Do you utilize file integrity monitoring (FIM) of the crown jewels of the organization?**

**A59:** **Yes**, JS Bank utilizes file integrity monitoring (FIM) specifically for the crown jewels of the organization. This proactive measure helps detect and respond to any unauthorized changes or alterations to critical files, ensuring the integrity and security of essential assets.

**Q60: Is storage of confidential data kept to a minimum and securely deleted after it's no longer needed?**

**A60:** **Yes**, JS Bank follows a data minimization approach, keeping the storage of confidential data to a minimum. Additionally, the bank ensures secure deletion of confidential data when it is no longer needed, aligning with best practices for data privacy and security.

**Q61: Do you require data classification throughout the network?**

**A61:** **Yes**, JS Bank implements data classification throughout its network. This ensures a structured approach to handling and protecting different types of data based on their sensitivity and importance.

**Q62: Do you deploy a network and cloud-based data loss prevention (DLP) program where confidential data resides?**

**A62:** **Yes**, JS Bank deploys a comprehensive data loss prevention (DLP) program both in the network and cloud environments where confidential data resides. This program helps monitor, detect, and prevent unauthorized access or leakage of sensitive information.

**Q63: Do you prevent confidential data from being copied to external devices and external devices from being attached to endpoints?**

**A63:** **Yes**, JS Bank implements measures to prevent the unauthorized copying of confidential data to external devices. Additionally, controls are in place to restrict external devices from being attached to endpoints, minimizing the risk of data exfiltration, and enhancing overall data security.

**Q64: Are processes and mechanisms for developing and maintaining secure systems and software defined and understood?**

**A64:** **Yes**, at JS Bank, processes, and mechanisms for developing and maintaining secure systems and software are well-defined and understood. The organization follows best practices and standards in secure software development to ensure the integrity and resilience of its systems.

**Q65: Are software engineering techniques or other methods defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in all software?**

**A65:** **Yes**, JS Bank incorporates software engineering techniques and other methods to prevent or mitigate common software attacks and vulnerabilities in all software. This proactive approach is part of the organization's commitment to building secure and resilient software.

**Q66: With regard to public-facing web applications, are new threats and vulnerabilities addressed on an ongoing basis?**

**A66:** **Yes**, JS Bank addresses new threats and vulnerabilities related to its public-facing web applications on an ongoing basis. Regular assessments and updates are conducted to ensure the security of these applications against evolving cyber threats.

**Q67: Are these applications protected against attacks?**

**A67:** **Yes**, JS Bank ensures that its public-facing web applications are protected against various cyber attacks. Security measures such as firewalls, intrusion detection systems, and regular monitoring are in place to safeguard these applications.

**Q68: Are preproduction environments separated from production environments, and is separation enforced with access controls?**

**A68:** **Yes**, JS Bank enforces the separation of preproduction environments from production environments, and this separation is rigorously enforced with access controls. This practice helps maintain the integrity of production systems and minimizes the risk of unauthorized access or changes during the development and testing phases.

**Q69: Are all mobile devices governed by effective mobile (MDM) policies?**

**A69:** **Yes**, all mobile devices at JS Bank are governed by effective Mobile Device Management (MDM) policies. These policies ensure the secure and compliant use of mobile devices within the organization.

**Q70: Do you disallow any enterprise device management connectivity of mobile devices not controlled by security mechanisms?**

**A70:** **Yes**, JS Bank disallows enterprise device management connectivity for mobile devices that are not controlled by security mechanisms. This policy helps maintain a secure and controlled environment, ensuring that only authorized and secure mobile devices have access to enterprise device management functionalities.

**HANDWRITTEN NOTES**