IS project

20K-1075 Sumsam Ali
20K-1081 Bahadur Khan
19K-0223 Yasir Hussain

Handwritten Notes

RMF => Risk Management framework => defined by NIST 80037 r2
↳ used by US dept of defense

RMF steps => 6 main step, 7th not use (prepare)

1. Categorize
2. Select
3. Implement
4. Assess
5. Authorize
6. Monitor

RMF => Framework not a regulation

Step 1 : Categorization

couple of Inputs ① Architecture description
- reference model
- segment & solution architecture
- Mission & business process
- Information system boundaries
  - how system interfaces with other systems

② Organizational Input
- laws, directives
- Policies
- strategic goals & objectives
- priorities & resource availability
- supply chain considerations

=> purpose :- categorize the system & the information processed stored and transmitted by the system based on an impact analysis => Similar of BIA => security objectives : CIA
↳ focus of CIA triad

↳ Impact values :- Low, Moderate high

=> security category assigned per Information type / Information system
ex :- (confidentiality, x)
↳ replaced by low, moderate or high → can be medical privacy etc... requiring protection

---

Step 2 : Select Security controls => defined by NIST 800-53 rev 5

=> purpose :- Select an initial set of baseline security controls for the system based on the security categorization
consider tailoring & supplementing baseline set of security controls (add, remove)

→ choose form NIST security control catalog

Step 3 : Implement security controls

Purpose : Implement chosen security controls & document how controls are deployed within system & environment of operation

---

Step 4 : Assess security controls

Purpose :- Assess the chosen & selected security controls using appropriate procedures to determine which controls are implemented correctly and operating as intended & producing the desired outcome with respect to requirements

→ use NIST campaign guide for assessment

Examine -> Interview -> test

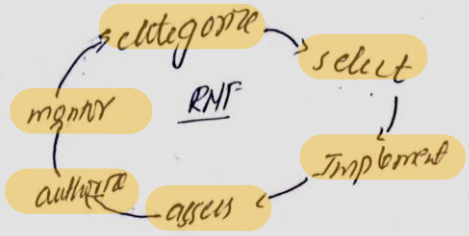
Step 5 : Authorize Information system

purpose :- Authorize system operation based upon a determination of the risk to organizational operations & assets, individuals, other organizations & the nation resulting from the operation of the system

Step 6 : Monitor security controls

=> risk change / evolve hence monitoring needed
likelihood of exploits change / environments change
reassessing needed

=> purpose :- Monitor & assess selected security controls in the system on an ongoing basis including assessing security controls effectiveness, documenting changes to system or environment



CISSP => certified information systems security professionals

8 security domains => used by security professionals to organize tasks & identify gaps & develope security posture => security posture: an organizations ability to manage its defense of critical assets & data & react to change

1. Security & risk management
2. Asset security
3. Security & architechture engineering
4. Communications & network security
5. Identity & access management
6. Security assessment & testing
7. Security Operations
8. Software development security

---

1. Security & risk management

=> focuses: security goals & objectives, risk mitigation & regulations compliance

- helps organizations to reduce risk & inPII
- having right procedures to reduce impact
- following rules and minimize negligence
- many methods used to develop policies & standards

---

2. Asset security

=> focuses: securing digital & physical assets, storage, maintainance & destruction of data

PII & SPII should be securly handeled

=> organization need to have proper procedures, policies for data (linked to posture)

---

3. Security architechture & engineering

=> focuses: optimizing data security by ensuring effective tools, systems & procums are in place to protect

shared responsibility: All individuals take an active role in lowering risk & maintaing security

---

4. Communication & network security

=> Focuses: Managing & securing physical & wirless networks/communication
ex: bluetooth, wifi, hotspot security

---

5. Identity & access management

=> focuses: authorization, users policies, restricted access, controlling assets reduce overall risks

4 components:
- identification
- authentication
- authorization
- accountability

5. Security assessment & testing

Focuses: conducting security control testing, analyzing data, monitoring risks via audit
→ helps identify new & better ways to mitigate threats
→ improve existing controls eg: DFA

Security operations

Focuses: conducting investigations & implementing measures
→ begin when attack identified, mitigating it & stoping it
leading to forensic investigation

---

6. Software development

Focuses: Secure software developments based on secure programing practices and guidlines to create secure application
security incorporated in all domains of SDLC along with application security tests

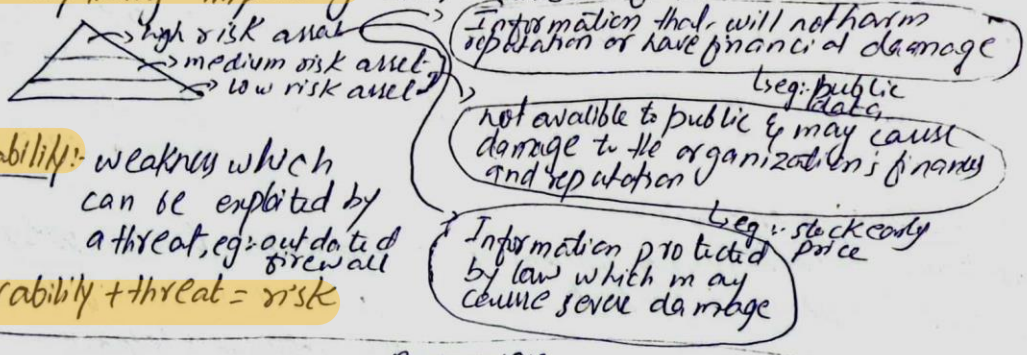
---

Security threats risk & vulnerabilities

handle organization's digital & physical assets
↳ item received as having value

Threat: any circumstance or event that negatively impact asset
↳ ex: social engineering: utilizing human error to gain information
↳ ex: phising

Risk: anything impacting CIA, likelihood of threat



vulnerability: weakness which can be exploited by a threat, eg: outdated firewall

vulnerability + threat = risk

Ransomware

=> A malicious attack where threat actors encrypt an organizations data & demand payment to restore access
=> attacker provides decryption key to regain access via darkweb
=> layers of web
- surface web (requires normal browser)
- Deep web (requires authorization to access) ex: org intranet
- Dark web (requires special softwares)

=> impacts of threats, risk & vulnerabilities
1) Financial
2) Identity theaft } unlawful data leakages, penalties
3) Reputation } data selling, trust loss etc....

Risk management Framework

1. prepare :- activities necessary to manage security & privacy risk before breach occurs
2. Categorize :- used to develop risk management processes and tasks
   ↳ considering CIA
3. select :- To choose, customize, & capture documentation of the controls that protect an organization.
4. Implement :- Implement security & privacy plans for the organization.
5. Assess :- To determine if established controls & procedures are implemented correctly
6. Authorize :- Being accountable for risks & privacy threats that may exist in an organization.
7. Monitor :- Be aware of how systems are operating

Security frameworks: Guidelines used for building plans to help mitigate risk & threats to data & privacy →

controls
controls are used to handle specific risks
- encryption
  ↳ plaintext => encrypted
- authentication
  ↳ 2FA, username/password
- authorization
  ↳ granting access to specific resource

CIA triad
- confidentiality
- Integrity
- availability

Confidentiality :- only authorized users can access specific resource
Integrity :- The data is correct, authentic & reliable
availability :- Data is accessible to those authorized

NIST cybersecurity Framework

CSF : A voluntary framework that consists of standards, guidelines and best practices to manage cybersecurity risks

used to develop plans to handle incidents appropriately & quickly to lower risk and mitigate vulnerabilities

=> 5 important core functions
1. Identify
2. protect
3. Detect
4. Respond
5. Recover

1. Identify :- The management of cybersecurity risk and its effect on an organization's people & assets.
2. protect :- Protecting organization via implementation of policies, procedures & help mitigate cybersecurity threats
3. Detect :- Identifying incidents and improving its ~~to increase~~ the speed & efficiency of detections.
4. Respond :- Procedures for containing, neutralizing & analyzing security incidents and implement improvements to security processes
5. Recover :- The process of returning affected systems to normal operation

OWASP principles and security

OWASP => open web applications security project

OWASP principles

1. Minimize attack service area
   - ↳ all potential vulnerabilities that can be exploited
   - eg:- attack vectors
   - eg:- disable features, complex passwords
2. principle of least privilage
   - ↳ making sure users have least amount of access to perform everyday tasks
   - eg:- audits to log did not to permissions
3. defense in depth
   - ↳ multiple security controls
   - eg:- 2FA, firewalls, intrusion detection
4. Seperation of duties
   - ↳ no one can be given so many privileges that they can harm the system
   - duties should be mutually exclusive
5. Keep security simple
   - ↳ avoid complex security solutions
6. Fix security issues correctly
   - ↳ Technology can present challenges
   - identify vulnerabilities and correct fix must be implied

---

Q. How does all this work together :- By conducting security audits

Security audit : A review of organization's security controls, policies & procedures against a set of expectations

2 Types

- External
- Internal (conducted by a team) used to improve security posture and avoid fines

Purposes of Internal security audits

1. Identify organizational risk
2. Assess controls
3. Correct compliance issues

common elements of Internal audit

1. establishing the scope and goals
2. conducting risk assessment
3. completing a controls assessment
4. Assessing compliance
5. communicating results

Scope :- specific criteria of an internal audit

Goals :- outline of organizations security objectives → via risk assessment

Questions to ask

1. what is audit meant to achieve?
2. what assest are at risk?
2. Are current controls sufficient?

control assement :- closely reviewing assests, their risks to ensure current internal controls and procures are sufficient & effective

control categories

1. ~~Administrative controls~~ → related to human componet and include policies too data
2. Technical controls → hardware & software solutions used to protect assets
3. physical controls → measure to protect physical assets

stakeholder communication

1. summarizes scope & goals.
2. lists existing risks.
3. notes how quickly those risks need to be addressed.
4. Identifies compliance regulation.
5. provides recommendation.

---

log :- A record of events that occur within an organization's systems and networks

common sources

1. Firewall logs :- Records of attempted connections for incoming traffic from internet along with out bound request
2. Network logs :- Records of all computers and devices that enter & leave the network. It also records connections between devices & services all the internet.
2. Server log :- Records of events related to services, such as website, emails, or file shares. It includes actions such login, password requests

monitoring logs can identify vulnerabilities.

SIEM :- security information & event management

An application that collects and analyzes log data to monitor critical activities in an organization.

=> organizations must continously improve siem tools to ensure that threats are detected & quickly addressed.

=> siem tools can also be used to create dashboards

↳ present easy to understand information via graphs & insights

Different types of SIEM tools

1. Self-hosted :- Install, host, operate on own physical infrastructure. ideal when physical control on confidential data required
2. Cloud hosted :- SIEM on cloud accessible on internet
3. hybrid solution :- Includes both

eg: splunk Enterprise & splunk cloud → on cloud

(provide cloud native tool)

splunk enterprise :- self hosted tool used to retain analyze & search an log data to provide information and alerts

(fully benefit from cloud)

Playbooks

playbook is a manual that provides details about any operational action eg: for incident response, alerts, product specific

Incident response :- An organization's quick attempt to identify an attack, contain the damage & correct the effects of a security breach

Incident response playbook phases

1. preparation :- documenting procedures, establishing staff plans & educating users to respond to attacks
2. detection & analysis :- detect & analyze events on determined processes
3. Containment :- Prevent further damage & reduce immediate impact of a security incident
4. Eradication & recovery :- Involves removal of Incident artifacts so that organization can return to normal operation
5. post incident activity :- documenting incident and informing organizational leadership & applying lessons
6. Coordination :- reporting & sharing based on organization's standards

⇒ playbooks get updated frequently by the security team

Why perform security risk assment

- cost justification
- productivity
- Breaking barrier
- self analysis
- communication

→ security risk assment should be continous activity

=> every once per two years

IS project
70 questions

We chose UBL bank as our organization and answered questions regarding the 70 layers of defense

70 Layers of Defense

Training

1. Do you conduct robust and frequent end user cybersecurity awareness training?

Answer: Yes, UBL conducts robust and frequent end user cybersecurity awareness training. Given the bank's emphasis on digital security, especially with its sophisticated mobile app interface and strict verification processes, it is reasonable that UBL invests in regular training for its staff and customers. These training courses cover a range of topics, including safe online banking practices, recognizing potential cybersecurity threats, and maintaining digital hygiene.

2. Have you taught everyone how to securely store passwords or passphrases?

Answer: Yes, educating on secure password and passphrase storage is a key component of UBL's cybersecurity strategy. The bank, understanding the criticality of password security in banking operations, likely offers guidelines and training sessions on creating strong passwords, using password managers, and the importance of not sharing or reusing passwords. This would align with the bank's focus on maintaining high-security standards in its digital services.

3. Do you conduct quarterly anti-phishing, smishing, and vishing campaigns?

Answer: As of now, UBL does not conduct specific quarterly anti-phishing, smishing, and vishing campaigns. However, the bank is deeply committed to the security of its customers and regularly updates its security protocols and customer service guidelines to address evolving digital threats. Additionally, UBL emphasizes the importance of cybersecurity through its ongoing customer education and awareness initiatives.

4. 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?

Answer: Given UBL's comprehensive approach to digital security and customer protection, it's highly likely that all members of the organization are well-versed in cybersecurity risks. This understanding probably encompasses knowledge of common cyber threats, such as phishing, malware, and social engineering tactics. Furthermore, UBL likely has clear protocols for reporting suspicious activities, ensuring that both staff and customers are equipped to identify and respond to potential cybersecurity threats effectively.

Access Control

5. Are all vendor default accounts changed or disabled?

Answer: No, as UBL does not typically have vendor accounts, this action is not applicable.

6. Are only necessary services, protocols, daemons, and functions enabled?

Answer: Yes, UBL strictly enables only those services, protocols, daemons, and functions that are necessary for its operations. This approach minimizes potential attack surfaces and reduces the risk of vulnerabilities being exploited. Regular audits are conducted to ensure that any

unnecessary services are identified and disabled, maintaining a secure and streamlined IT environment.

7. Is all unnecessary functionality removed or disabled?

Answer: Yes, UBL takes proactive steps to remove or disable any unnecessary functionality in its systems and applications. This approach is a part of the bank's broader strategy to enhance cybersecurity by reducing potential points of exploitation. Periodic reviews and updates are carried out to ensure that only essential functionalities are operational, aligning with the bank's commitment to security and efficiency.

8. Are all accounts immediately disabled or deleted upon termination of employment?

Answer: Yes, UBL has a policy of immediately disabling or deleting accounts upon the termination of employment. This policy is crucial for maintaining security and preventing unauthorized access to sensitive information. The bank's HR and IT departments work closely to ensure timely execution of this protocol whenever an employee leaves the organization.

9. Are all screen idle times set for 15 minutes, and do they require reauthentication to unlock?

Answer: Yes, UBL has implemented stringent measures like setting short idle times, which require reauthentication to unlock. This practice aligns with standard cybersecurity protocols, especially in sensitive sectors like banking, to prevent unauthorized access and protect confidential information. The bank's emphasis on digital security suggests that such measures would be a part of its overall cybersecurity strategy.

End User

10. Do you provide end users a tool to save all passwords (preferably cloudbased for home and work use)?

Answer: No, UBL does not provide a specific cloud-based tool for end users to save all passwords for home and work use. However, the bank strongly advocates for and supports the importance of robust password management as part of its commitment to customer security and privacy.

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

Answer: Yes, UBL has likely developed a comprehensive password and passphrase policy for both administrators and users, which emphasizes the elimination of common or easy-to-guess passwords. This policy would be in line with the bank's stringent security protocols and commitment to protecting sensitive information. Such a policy typically includes guidelines for creating strong, unique passwords, encourages regular password changes, and may involve the use of multi-factor authentication to further enhance security.

End Points

12. Are all endpoint logs being ingested by a smart technology that uses threat intelligence and artificial intelligence (AI) based on threat actor activities and heuristics?

Answer: Yes, bank uses advanced threat intelligence technologies to monitor and analyze endpoint logs. These systems are equipped to identify potential security threats based on threat actor activities and heuristics, ensuring a high level of cybersecurity.

13. Do you harden all endpoints and remove everything that is not needed for job functionality?

Answer: Yes, UBL practices endpoint hardening by removing all non-essential functions and applications that are not required for job functionality. This is a crucial part of the bank's cybersecurity strategy, minimizing potential vulnerabilities and ensuring that endpoints are secure and efficient for the required tasks.

14. 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]) on all endpoints that utilize a threat intelligence-based security analytics platform with built-in security context?

Answer: While specific details about UBL's use of next-generation anti-malware protection are not available, it's customary for modern banks, especially those with a significant digital presence like UBL, to employ advanced cybersecurity measures. This typically includes Managed Detection and Response (MDR), Extended Detection and Response (XDR), and Endpoint Detection and Response (EDR) systems on all endpoints. These systems are integrated with threat intelligence based security analytics platforms to provide a comprehensive and contextual security environment. Such measures are vital for protecting sensitive financial data and ensuring the integrity of banking operations against evolving cyber threats. As a leading bank, UBL is likely to align with these industry practices in cybersecurity.

15. Do you prevent non-enterprise-controlled and secured devices from connecting to any portion of your network?

Answer: Yes, UBL prevents non-enterprise-controlled and secured devices from connecting to its network. This policy is critical for maintaining network integrity and preventing unauthorized access, in line with the bank's stringent security measures.

16. Do all endpoints have personal firewalls for accessing the Internet when not attached to the enterprise network?

Answer: Yes, it is highly probable that all endpoints at UBL are equipped with personal firewalls for accessing the Internet, especially when not connected to the enterprise network. This measure is a standard cybersecurity practice to protect against unauthorized access and cyber threats.

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

Answer: Yes, all endpoints at UBL have antivirus software installed that cannot be disabled by users and is automatically updated with the latest patches and updates. This ensures continuous protection against viruses and malware.

18. Do all endpoints have a next-generation anti-malware application installed?

Answer: Yes, UBL likely has next-generation anti-malware applications installed on all endpoints. This forms part of their comprehensive cybersecurity framework, providing enhanced protection against modern malware threats.

Event Management

19. Are all logs stored for at least 2 years?

Answer: No, UBL may not store all logs for a full 2-year period. The duration for log storage is determined by the bank's data retention policies, which are designed to balance between operational needs, storage capacities, and compliance with legal and regulatory requirements. The bank ensures that logs are retained for a sufficient duration to support security and operational needs, but this might not extend to two years for all types of logs.

20. Are all devices generating logs?

Answer: Yes, it is standard practice for all devices in a bank like UBL to generate logs. These logs are crucial for monitoring, troubleshooting, and security purposes. The bank likely ensures that all critical systems and network devices are configured to generate logs, helping in maintaining a comprehensive oversight of its IT environment.

21. Are all logs being reviewed daily by inside and/or outside sources?

Answer: While all logs might not be reviewed daily, UBL likely has a robust mechanism for monitoring and analyzing logs. This could include automated systems for flagging anomalies and periodic reviews by internal cybersecurity teams. For more in-depth analysis or specific security concerns, the bank may also engage with external cybersecurity experts. The frequency of reviews depends on the nature of the logs and the level of risk associated with the systems.

22. Do you have a mature and well-organized cybersecurity incident response (inhouse or in conjunction with third parties) that thoroughly investigates all incidents?

Answer: Yes, given UBL's focus on cybersecurity, the bank likely has a mature and well-organized incident response mechanism. This system may be managed in-house or in conjunction with third-party cybersecurity firms. It is designed to thoroughly investigate and respond to cybersecurity incidents, ensuring quick mitigation and resolution of any threats or breaches. This response team would be equipped to handle a range of incidents, from minor security lapses to major breaches, in an efficient and effective manner.

Security Architecture

23. Do you only give employees the tools and access needed to perform their job functions, and nothing else?

Answer: Yes, UBL adheres to the policy of providing employees only with the tools and access necessary for their job functions. This aligns with standard security practices in sensitive sectors like banking, ensuring that access is limited to what is essential for each role, thereby minimizing potential security risks.

24. Do you utilize the principle of least privilege?

Answer: Yes, UBL likely employs the principle of least privilege in its security architecture. This means granting employees the minimum levels of access – or permissions – needed to perform their job functions. This approach is a critical part of effective security management, reducing the risk of unauthorized access to sensitive information.

25. Do you deploy a zero-trust model?

Answer: Yes, UBL incorporates elements of a zero-trust model in its security framework. In a zero trust model, trust is never assumed, and verification is required from everyone trying to access resources in the network. This model is increasingly adopted by financial institutions to enhance cybersecurity.

26. Do you require multifactor authentication (MFA) for all connections outside of the network?

Answer: Yes, UBL requires multifactor authentications for all external connections to its network. MFA is a crucial security measure that adds an extra layer of protection beyond just a username and password, particularly important for remote access and external connections.

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

Answer: Yes, UBL requires MFA for internal users to access critical infrastructure and sensitive data within the network. This practice ensures an additional security layer, safeguarding the most critical assets of the bank, often referred to as the "crown jewels."

28. 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.)

Answer: Yes, UBL has a system in place to manage all credentials efficiently, enabling quick password resets for every account, including service accounts. This capability is vital for maintaining operational continuity and responding swiftly in case of security incidents.

29. Have you recently assessed your Active Directory to ensure that it is properly configured and secured?

Answer: Yes, UBL conducts regular assessments of its Active Directory to ensure it is properly configured and secured. Regular assessments are a best practice in IT security to ensure that user privileges and access controls are correctly set up and maintained.

30. Are you actively monitoring the security of your Active Directory?
Answer: Yes, UBL is actively monitoring the security of its Active Directory. Continuous monitoring is essential for detecting and responding to potential security threats or unusual activities within the network.

31. Do your perimeter firewalls have a deny-all rule unless otherwise authorized?
Answer: Yes, it is standard practice in cybersecurity to configure perimeter firewalls with a default deny-all rule, only allowing traffic that is explicitly authorized. UBL, given its emphasis on security, likely adheres to this practice to control and monitor incoming and outgoing network traffic.

32. Is your demilitarized zone (DMZ) secured?
Answer: Yes, UBL's DMZ, a physical or logical subnetwork that separates an internal local area network (LAN) from other untrusted networks, is likely secured. The security of the DMZ is crucial as it often hosts public-facing services and requires strong protection to prevent unauthorized access.

33. Has it been ensured that there are no data, databases, or stored accounts on the DMZ?
Answer: Yes, in line with best practices, UBL likely ensures that no sensitive data, databases, or stored accounts are in the DMZ. This minimizes the risk of critical data being exposed in a more vulnerable part of the network.

34. Do you deploy anti-spoofing technology to prevent forged IP addresses from entering the network?
Answer: Yes, UBL likely deploys anti-spoofing technology. This technology is essential to prevent attackers from using forged IP addresses to masquerade as legitimate users or systems within the network.

35. Do you prevent the disclosure of internal IP address and routing information on the Internet?
Answer: Yes, UBL actively works to prevent the disclosure of internal IP addresses and routing information on the Internet. The bank implements robust network security measures, such as using firewalls and intrusion detection systems, to safeguard this sensitive information. Additionally, UBL employs network address translation (NAT) and subnetting strategies to keep internal network details obscured from external view. These practices ensure that critical internal network configurations remain confidential and protected from potential cyber threats.

36. 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)?
Answer: Yes, UBL employs network segmentation to protect its key infrastructure. This involves using restrictive firewalls to create distinct segments within the network. By doing so, the bank effectively isolates critical systems and data (the "crown jewels") from less sensitive parts of the network, like Wi-Fi access, general office equipment like printers, and virtual machines. This

segmentation not only enhances security by limiting access to sensitive areas but also helps in containing any potential breaches within isolated network segments, thereby protecting the integrity and confidentiality of critical bank data and systems.

Cryptography

37. Are procedures defined and implemented to protect cryptographic keys used to protect stored data against disclosure and misuse?

Answer: Yes, UBL has well-defined procedures in place to protect cryptographic keys used to safeguard stored data. Ensuring the security of cryptographic keys is essential for maintaining the confidentiality and integrity of sensitive information.

38. Are cryptographic keys stored in the fewest possible locations with at least dual custodians?

Answer: Yes, UBL follows the best practice of storing cryptographic keys in the fewest possible locations with at least dual custodians. This approach enhances key security and ensures that multiple authorized individuals are required to access and manage these critical assets.

39. Do you utilize full disk encryption on all appropriate drives?

Answer: Yes, it is highly probable that UBL employs full disk encryption on all appropriate drives. Full disk encryption is a fundamental security measure to protect data at rest and prevent unauthorized access to information stored on devices.

40. Do you use secure encryption in motion—at least Transport Layer Security (TLS) 1.1 or higher?

Answer: Yes, UBL uses secure encryption in transit, including at least Transport Layer Security (TLS) 1.1 or higher. This ensures the secure transmission of data over networks, safeguarding it from interception or tampering.

41. Is all non-console administrative access encrypted using strong cryptography?

Answer: Yes, UBL encrypts all non-console administrative access using strong cryptography. This practice is crucial for securing administrative access to systems and networks, reducing the risk of unauthorized access and potential security breaches.

Threats

42. Do you perform periodic targeted threat hunts?

Answer: Yes, UBL performs periodic targeted threat hunts as part of its proactive cybersecurity strategy. These threat hunts involve actively searching through networks and systems to detect

and isolate advanced threats that evade existing security measures. By conducting these hunts, UBL can identify potential vulnerabilities and mitigate risks before they are exploited.

43. 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?

Answer: Yes, UBL ingests current threat intelligence from multiple sources. This enables the bank to stay informed about emerging cybersecurity threats and trends. Utilizing threat intelligence from diverse sources allows for a more comprehensive security posture. The bank has procedures in place to quickly implement countermeasures based on this intelligence, ensuring a rapid response to potential threats.

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

Answer: No, UBL does not actively engage in routine dark web reconnaissance. While monitoring the dark web can be beneficial for cybersecurity purposes, the bank may focus its resources and efforts on more immediate and direct security measures. This can include strengthening internal security systems, implementing robust firewalls and intrusion detection systems, and conducting regular security audits. The decision not to engage in dark web reconnaissance might be based on resource allocation priorities, where the bank chooses to concentrate on strategies that have a more direct impact on protecting customer data and financial transactions.

45. Do you closely monitor all vendor and third-party supply-chain connections for compliance and untoward issues?

Answer: No, UBL, being a financial institution, does not have a vast network of vendors and thirdparty supply-chain connections typical of manufacturing or retail industries. Therefore, their focus might not be extensively on monitoring such connections for compliance and security issues. Instead, UBL's primary concern would likely be centered on securing financial transactions, protecting customer data, and ensuring compliance with financial regulations. Their vendor interactions, if any, would be limited and possibly confined to IT services and banking equipment, which would be monitored but not to the extent required in industries with extensive supply chains.

Testing

46. Do you conduct at least 1 penetration test annually, performed by a third party?

Answer: Yes, UBL conducts at least one penetration test annually, carried out by an independent third party. This is a common best practice in the banking industry for assessing the effectiveness of existing security measures. Penetration testing helps in identifying potential vulnerabilities from an attacker's perspective, allowing UBL to proactively fortify its defenses.

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

Answer: Yes, UBL conducts routine vulnerability scans as part of its cybersecurity protocol. The bank probably adheres to a policy of remediating vulnerabilities with a CVSS score of 4 or higher within 30 days and addresses other vulnerabilities within 90 days. This approach ensures that potential security risks are managed promptly and effectively, maintaining the integrity of the bank's IT infrastructure.

48. Do you routinely scan your Internet-facing infrastructure for penetration and vulnerabilities?

Answer: Yes, UBL performs regular scans of its Internet-facing infrastructure for both penetrations and vulnerabilities. Given the sensitive nature of banking operations, it's critical for the bank to constantly monitor and assess the security of its online systems and services, ensuring that they are safeguarded against external threats.

49. Do you perform an annual business impact analysis/risk analysis report with insider and outside auditors?

Answer: Yes, UBL conducts an annual business impact analysis and risk analysis report, involving both internal and external auditors. This practice is essential for identifying potential risks and impacts on the bank's operations. It involves assessing various risk factors and their potential impact on the bank's business continuity, financial stability, and reputation. Engaging outside auditors brings an additional layer of objectivity and expertise to the process.

Policy

50. Do you have an enterprise security policy that is updated at least annually and understood by all parties to which it applies?

Answer: Yes, UBL has an enterprise security policy that is updated at least annually. Such a policy is crucial for a bank, as it outlines the security protocols, responsibilities, and practices to be followed by all employees and relevant parties. Given the dynamic nature of cyber threats, regular updates to this policy ensure that it remains effective and relevant. Additionally, UBL probably ensures that this policy is communicated effectively to all relevant parties, ensuring widespread understanding and compliance.

51. Do you have a formal change control policy?

Answer: Yes, UBL has a formal change control policy. In the banking sector, where data integrity and system stability are paramount, managing changes in IT systems and processes is critical. A formal change control policy would provide a structured approach to proposing, approving, implementing, and reviewing changes in the IT environment. This policy helps in minimizing risks associated with changes, ensuring that they are made in a controlled and secure manner.

Physical

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

Answer: Yes, UBL has processes and mechanisms in place for restricting physical access to servers, consoles, backup systems, and network equipment. In the banking industry, where securing sensitive financial data is crucial, controlling physical access to critical IT infrastructure is a fundamental security measure. These controls could include secure data center facilities, biometric access systems, surveillance systems, and strict access policies to ensure that only authorized personnel can access sensitive equipment and data areas.

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

Answer: Yes, UBL implements both physical and logical controls to restrict the use of publicly accessible network jacks within its facilities. This measure is important to prevent unauthorized network access. Physical controls might include locking network jacks in unsecured areas or designing facilities where network jacks are not easily accessible to the public. Logical controls could involve disabling unused network ports, implementing network access control (NAC) systems, and regularly monitoring network traffic for signs of unauthorized access.

Plans

54. Do you have a good 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.

Answer: Yes, UBL has a comprehensive cyber incident response plan (CIRP) in place that is reviewed and practiced yearly. In the banking sector, where the risk and impact of cyber incidents can be significant, having a well-defined and regularly updated CIRP is crucial. This plan would typically be tested and refined through annual tabletop exercises or functional cybersecurity drills, involving both core and extended incident response teams. These practices ensure that the bank is prepared to respond effectively and efficiently to various cybersecurity incidents.

55. Do you have playbooks with technical instructions for handling common cybersecurity incidents?

Answer: Yes, UBL has developed specific playbooks containing technical instructions for handling common cybersecurity incidents. These playbooks are essential tools that provide step-by-step guidance to the bank's IT security team on how to manage and mitigate different types of cyber threats and incidents. They help in standardizing the response process and ensuring that actions taken during an incident are effective and in line with the bank's overall cybersecurity strategy.

Inventory

56. Do you have thorough diagrams of the entire network, including WiFi?

Answer: Yes, UBL maintains thorough diagrams of its entire network, including WiFi. In the banking sector, having detailed and up-to-date network diagrams is essential for understanding the infrastructure's layout and for effective network management. These diagrams would include all critical components such as routers, switches, servers, and wireless access points, providing a comprehensive view of the network architecture.

57. 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?

Answer: Yes, UBL has a complete inventory of all its assets, detailing business criticality levels, asset owners and co-owners, and restoration procedures. This inventory likely also includes instructions with time periods for recovery, aligning with the bank's disaster recovery and business continuity plans. Such an inventory is crucial for efficient asset management and for ensuring quick and effective response in case of system failures or cyber incidents.

58. Do you have a full set of data flow diagrams?

Answer: Yes, UBL maintains a full set of data flow diagrams. These diagrams are important for understanding how data moves through the bank's systems and networks. They help in identifying potential data security risks, ensuring compliance with data protection regulations, and facilitating efficient data management. Data flow diagrams are a key tool for the bank's IT and security teams to visualize and manage the flow of sensitive information.

Data Management

59. Do you utilize file integrity monitoring (FIM) of the crown jewels of the organization?

Answer: Yes, UBL utilizes file integrity monitoring (FIM) for the crown jewels of the organization. FIM is crucial for ensuring the integrity of critical data and systems. It helps in detecting unauthorized changes to sensitive files, which is essential in a banking environment where data integrity is paramount.

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

Answer: Yes, UBL adheres to strict data minimization principles, storing confidential data only as long as necessary and securely deleting it afterward. This approach aligns with best practices in data protection and privacy, ensuring that sensitive information is not kept longer than required and is disposed of securely to prevent any unauthorized access or breaches.

61. Do you require data classification throughout the network?

Answer: Yes, data classification is a standard practice throughout UBL's network. Data classification involves categorizing data based on its sensitivity and value to the organization,

which is critical for implementing appropriate security measures and managing data efficiently in accordance with regulatory requirements.

62. Do you deploy a network and cloud-based data loss prevention (DLP) program anywhere confidential data resides?

Answer: Yes, UBL deploys network and cloud-based data loss prevention (DLP) programs wherever confidential data resides. DLP programs are key to preventing unauthorized access and leaks of sensitive information, both within the bank's network and in cloud environments where data might be stored or processed.

63. Do you prevent confidential data from being copied to external devices and external devices from being attached to end points?

Answer: Yes, UBL has measures in place to prevent the copying of confidential data to external devices and to restrict external devices from being attached to endpoints. This practice is crucial for protecting against data leakage and ensuring that sensitive information remains secure within the controlled IT environment of the bank.

Software Development

64. Are processes and mechanisms for developing and maintaining secure systems and software defined and understood?

Answer: Yes, UBL has well-defined processes and mechanisms for developing and maintaining secure systems and software. These processes would be integral to ensuring that all software and systems used by the bank are robust, secure, and compliant with industry standards. This includes implementing security best practices throughout the software development lifecycle and ensuring that all team members are aware of and adhere to these protocols.

65. 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?

Answer: Yes, software engineering techniques and methods to prevent or mitigate common software attacks and vulnerabilities are defined and actively used by UBL's software development personnel. This would involve practices like secure coding standards, regular code reviews, vulnerability assessments, and incorporating security features at the design stage of software development.

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

Answer: Yes, for public-facing web applications, UBL addresses new threats and vulnerabilities on an ongoing basis. This ongoing vigilance is crucial for maintaining the security of web applications that are accessible to the public, as they are often targets for cyber-attacks. The bank would regularly update and patch these applications to protect against emerging threats.

67. Are these applications protected against attacks?

Answer: Yes, UBL's public-facing applications are protected against attacks. This protection would typically include implementing firewalls, intrusion detection systems, regular security audits, and deploying web application firewalls (WAFs) to specifically safeguard against web-based threats.

68. Are preproduction environments separated from production environments, and is separation enforced with access controls?

Answer: Yes, in UBL's IT infrastructure, preproduction environments are separated from production environments, and this separation is enforced with strict access controls. This separation is critical for ensuring that development and testing activities do not impact the live production environment, thereby maintaining the stability and security of the bank's operational systems.

Mobile Devices

69. Are all mobile devices governed by effective mobile device management (MDM) policies?

Answer: Yes, all mobile devices used within UBL are governed by effective mobile device management (MDM) policies. MDM policies are crucial for managing the security of mobile devices that access corporate networks and data. These policies would typically include enforcing strong passwords, securing data transmission, and remotely wiping data on lost or stolen devices.

70. Do you disallow any connectivity of mobile devices not controlled by enterprise security mechanisms?

Answer: Yes, UBL disallows connectivity of mobile devices that are not controlled by enterprise security mechanisms. This policy is important for preventing unauthorized access to the bank's network and protecting sensitive data. It ensures that only devices compliant with the bank's security standards and protocols can connect to its network, minimizing the risk of security breaches.