IS PROJECT

Members:

19K-0214 Ahmed Memon

20K-0297 Usaid Bin Rehan

20K-0409 Mukand Krishna

Handwritten Notes.

Used by Dept of Defense & US Govt
Defined in NIST 800-37 r2 (version 2)

RMF Steps

#1 Categorize Information System

Input: Architecture Description

- Architecture Reference Model
- Segment and Solution Model
- System Boundaries
- Mission & Robustness Processes

Organizational Inputs

- Laws
- Directives
- Policies
- Governance
- Strategic Goals
- Priority & Availability
- Supply Chain

eg HIPAA

Similar to Business Impact Analysis

#2 Select Security Controls

eg max tolerable downtime
Recovery Point Objective

BUT
CIA Trial in this case:

- Confidentiality
- Integrity
- Availability

Impact Values: Low, Moderate, High

Security Category = (c, value)(I, value)(A, value)
info type/info sys

eg SC_{PHI} = (C, high)(I, high)(A, low)

'protected health info' domain — not important to provide access all the time

#2 Select Security Control

Select initial set of baseline security controls for system based on security categorization, tailor and supplement security control baseline as needed based on organization assessment of risk and local conditions

eg Drone has baseline security controls that needed to be incremented when it flies into enemy country

#3 Implement and Document Security Controls

Implement then document how they are deployed within system and operation environment

#4 Assess Security Controls

Assess using appropriate procedures to determine extent to which

- controls are implemented correctly
- operating as intended
- producing desired outcome

eg reducing risk typically

NIST 800-53A gives guidance how to do it

#5 Authorize Info Sys

Authorize operations based on

Risk to: organizational ops and assets

- people
- other organizations
- Nation

Decide if that risk is acceptable formally

#6 Monitor Security Controls

Monitor and assess ongoing basis

- Assessing control effectiveness
- Documenting changes to system or env
- Conducting Security Impact Analysis
- Reporting Security State to appropriate

#7 Preparation (Optional)

Can't fully prepare for risks but some is better than none

Roll NO:

20K-0297

20K-0409

19K-0214

Roll no: 20K-0409

Why perform a Security Risk Assessment?

- Importance: Organizations regularly address security concerns due to legal requirements protecting data and public safety expectations. The goal is to identify and measure risks to information assets.

- Rational for Risk assessment

1) Cost Justification:- Extra security costs more money, but it's essential. Assessment educates manager or critical tech, risks, justifying security expenses. For example, Investing in cyber security prevents costly data breaches, saving money in the long run.

2) Productivity Improvement: Assessment enhance IT productivity, formalizing reviews, structuring information, and implementing self analysis, make everything run smoother. For example, Better security measures reduce interruptions from cyber threats, makes business operations efficient.

3) Breaking Barriers: Security decisions involve both organizational management and IT staff. Leaders decide security levels, and IT staff implements specific requirements. For example, Leaders decide on data security levels, and IT ensures transactions are secure.

4) Self Analysis: Assessment system should be simple for every one, even without security or IT expertise. This encourages ownership of security and integrates it into the organization's culture. For example, employees can follow security guidelines without advanced IT knowledge, making security a part of organization's / company's culture.

5.) Communication Boost: Assessments gather information from different parts of the organization, improving communication and decision making. For example, Sharing knowledge and potential security risks helps the whole company stay informed and respond quickly to threats.

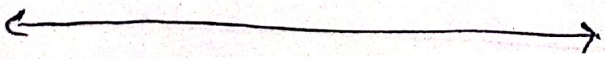
Key Procen in Info Sec.

- risk mgmt core: enterprise risk assessment and risk management processes are central to information Security.
- tailoring to org. size: Depending on the organization's size and complenity, a general prioritization might be more suitable than a detailed assessment of precise values and risks.

Frequency and Continuity

- continous activity: Security risk assessment should be ongoing.
- recommended frequency: Comprehensive Assessment should be done atleast every 2 years to explore risks. For mission-critical systems, more frequent assessments, if not continous, are highly recommended.

- Regular updates in security measure help adapt to new ~~features~~ threats and protect important information over time.



How To Manage Security Risks & Threats

Date:

What you'll learn:

Roll no: 19K-0214

- CISSP's eight security domains (Certified Information Systems security Professionals)
- Security frameworks and controls (NIST) -> (National Institute of standards & Technology)
- Security audits
- Basic Security tools
- Threats, risks and vulnerabilities
- Layers of the web

Note:

There are 8 security domains or categories identified by CISSP. Security teams use them to organize daily tasks and identified gaps in security that can cause negative consequences for an organisation and to establish their security posture.

Security Posture: An organisations ability to manage its defense of critical assets and data, and react to change.

~~The video discusses of the first four domain...~~

~~Other domains.~~

1. Security and Risk management
2. Asset security.
3. Security architecture and engineering
4. Communications and network security.
5. Identity and access management.
6. Security assesment and ~~testing~~ testing
7. Security operations.
8. Software development security.

Date: _____

Security and risk management:

Focused on defining security goals and objectives, risk ~~management~~ - mitigation, compliance, business continuity, and legal regulations.

defining security & objectives: organisations reduces risks to their critical assets and data, like PII (Personally identifiable information).

Risk mitigation: The process of having the right procedures and rules in place to quickly reduce the impacts of a risk like a breach.

Compliance: Primary method used to develop an organization's internal ~~security~~ security policies, regulatory requirements, and independent standards.

Business continuity: An organizations ability to maintain their everyday productivity by establishing risk disaster recovery plans.

legal regulations: This means following rules and expectations for ethical - behaviour to minimize negligence, abuse or fraud.

Date: _____

Asset Security: Focused on securing digital and physical assets. It's also related to the storage, maintenance, retention, and destruction of data.

Security Architecture and Engineering: Focused on optimizing data security by ensuring effective tools, systems, and processes are in place to protect an organization's assets and data.

Note: One of the core concepts of secure design architecture is "shared responsibility"

Shared responsibility: All individuals within an organisation take an active role in lowering risk and maintaining both physical and virtual security.

Communication and network security: Focused on managing and securing physical networks and wireless communications.

- Secure Networks keep an organization's data and communications safe, whether on site, or in the cloud, or when connecting to services remotely.

For example: employees working remotely in public spaces need to be protected from vulnerabilities that can occur when they use insecure bluetooth connections or public Wi-Fi hotspots. By having security team member remove access to those types of communication channels at the organizational level, employees may be discouraged from practicing insecure behavior that could be explained by threat actors.

Date: _____

Identity and access management: Focused on access and authorization to keep data secure, by making sure users follow established policies to control and manage assets.

for example: If everyone at a company is using the same administration login, there is no way to track who has access to what data. In the event of a breach, seperating valid user activity from the threat actor would be impossible.

Components of IAM (Identity and Access Management).

- Indentification
- Authentification
- Authorization
- Accountability
- Security Assesment and Testing

Security Assesment and Testing: Focused on conducting security control testing, collecting and analyzing data, and conducting security audits to monitor for risks, threats, and vulnerabilities.

Security Operations: Focused on conducting investigations and implementing preventative measures.

Software development security: Focused on using secure coding practices

Date: _____

→ As an entry level security analyst, one of your many roles will be to handle an organization's digital and physical ~~environment~~ assets.

Types of assets:
• Physical office • computers • customers' PII • Intellectual properties; such as, patents or copyrighted data and so much more.

∴ Unfortunately organizations ~~are~~ operate in an environment that presents multiple security threats, risks & vulnerabilities to their assets.

Threat: Any circumstance or event that can negatively impact assets.

e.g: Social Engineering Attack: A manipulation technique that exploits human error to gain private information, access or valuables.

Risk: Anything that can impact the ~~confidentiality~~ confidentiality, integrity, or availability of an asset.

- Low Risk asset: Information that would not harm the organization's reputation or ongoing operations, and would not cause financial damage if compromised.

- Medium Risk asset: Information that's not available to the public and may cause some damage to the organization's finances, reputation, or ongoing operations.

- High Risk asset: Information protected by regulations or laws, which if compromised would have a severe negative impact on an organization's finances, ongoing operations, or reputation. This could include leaked assets with SPII, PII, or intellectual property.

Date:

Vulnerabilities: A weakness that can be exploited by a threat

* Important point: both, a vulnerability and threat must be present for there to be a risk.

Examples:
- Outdated firewall.
- Software or Applications
- weak passwords
- Un-protected confidential data.

Ransomware: A malicious attack where threat actors encrypt an organization's data and demand payment to restore access.

Layers of the web:
- Surface web
- Deep web
- Dark web

~~Surface layer.~~

Surface web: It is the layer that most people use. It contains content that can be accessed using a web browser.

Deep web: It generally requires authorisation to access it. An organisation's internet is an example of deep web, since it can only be accessed by employees or others who have been granted access.

Dark web: It can only be accessed by using special software. The dark web generally carries a negative ~~connection~~ connotation. Since it is the prefered web layer for criminals because of the secrecy that it provides.

Date:

Key impacts of Risks, Threats & Vulnerabilities

- Financial
- Identity
- Reputation

National Institute of Standards & Technology.

NIST provides many frameworks that are used by security professionals to manage risks, threats and vulnerabilities.

NIST's "Risk Management framework" or "RMF".

7 steps in "RMF"
- Prepare
- Categorize
- Select
- Implement
- Assess
- Authorize
- Monitor

RMF step 1: Prepare
Activities that are necessary to manage security and privacy risks before a breach occurs.

RMF step 2: Categorize.
Used to develop risk management processes and tasks.

RMF step 3: Select
Choose, Customize, and capture documentation of the controls that protect an organization.

RMF step 4. Implement
Implement security and privacy plans for the organisation.

RMF step 5: Assess
Determine if established controls are implemented correctly.

RMF step 6: Authorize
Being accountable for the security and privacy risks that may exist in an organization

RMF step 7. Monitor: Be aware how systems are ~~monitoring~~ operating.

Date:

What you'll Learn

- Frameworks
- Controls
- Design principales
- Security audits.

Security Frameworks: Guidelines used for building plans to help mitigate risk and threats to data and privacy. Such as ~~social~~ social engineering attacks and ransomware.

Security Controls: Safeguards designed to reduce specific security risks.

- Three ~~co~~ common types of controls:

Encryption: The process of converting data from a readable format to an encoded format.

Authentication: Process of verifying who someone or something is.

- more advance methods of authentication, such as Multi-Factor Authenticat, or 'MFA', challenge the user to demonstrate that they are who they claim to be by requiring both a password and an additional form of authentication, like a security code or biometric, such as a fingerprint, voice, or face-scan.

Biometrics,

Unique physical characterstics that can be used to verify a person's ~~entity~~. identity.

e.g: finger-print, an eye scan, ~~and~~ or palm scan.

Date: _____

An example of social engineering attack that can exploit biometrics is "vishing"

Vishing: The ~~exploitation~~ exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source.

e.g. It can be used to impersonate a person's voice to steal their identity. and then commit a crime.

Another important security control...

Authorization: The concept of granting access to specific resources within a system.

~~CIA triad~~

CIA triad: A model that helps inform how organizations consider risks when setting up systems and security policies.

Confidentiality: Only authorized users can access specific assets or data.

Integrity: The data is correct, authentic, and reliable

Availability: Data is accessible to those who are authorized to ~~[redacted]~~ access it.

NIST Frameworks:

NIST Cybersecurity Framework (CSF): A voluntary framework that consists of standards, guidelines, and best ~~practices~~ practices to manage cybersecurity risk.

- It consists of 5 important core functions,
  - Identify, Protect, Detect, Respond, Recover

NIST S.P. 800 - 53

A unified framework for protecting the security of information systems within the federal government.

Identify: The management of cybersecurity risk and its effect on an organizations people and assets.

Protect: The strategy used to protect an organization through the implementation of policies, procedures, training and tools that help mitigate cybersecurity threats.

Detect: Identifying potential security incidents and improving monitoring capabilities to increase the speed and efficiency of detections.

Respond: Making sure that the proper procedures are used to contain, neutralize, and analyze security incidents, and implement improvements to the security process.

Recover: The process of returning affected systems back to normal-operation.

Date:

OWASP (Open Web Application security projects). principles

- Minimise the attack surface area:
- Principle of least privilege
- Defense in depth
- Seperation of duties
- Keep security simple
- Fix Security issues correctly.

- how they all work together?
- by conducting Security audits.

Security audit: A review of an organisation's security controls, policies, and, procedures against a set of expectations.

Purposes of internal security audits:

- Identify organizational risk
- Assess controls
- Correct compliance issues

Common elements of internal audits:

- Establishing the scope and goals
- Conducting a risk assessment
- Completing a controls assesment.
- Assessing compliance
- Communicating results.

Date:

1. Establishing scope and goals:
   - Scope refers to the specific criteria of an internal security audit.
   - Goals are an outline of the organization's security objectives.

Scope: The internal IT audit will assess the following:
- Assess user permissions
- Identify existing controls, policies and procedures
- Account for technology currently in use

Goals: The goals for the internal IT audit are:
- Adhere to the NIST Cybersecurity Framework (CSF)
- Establish policies and procedures to ensure compliance with regulations.
- Fortify system controls

2. Conducting a risk assessment.

Risk description: There is a lack of proper management of physical and digital assets; equipment used to store data is not properly secured; and access to private information in the organization's internal network needs more robust controls in place.

Control categories

- Administrative controls
- Technical controls
- Physical controls

Date: _____

Administrative Controls			
Control name	Control type and explanation	Needs to be implemented (X)	Priority
Password-policies	Preventative; establish password strength rules to improve security / reduce likelihood of account compromise through brute force or dictionary attack techniques	X	high

Technical Controls			
Control name	Control type and explanation	Needs to be implemented (X)	Priority
Intrusion-Detection system (IDS)	Detective; allows IT team to identify possible ~~functions~~ intrusions (i.e: anomalous traffic) quickly.	X	High
Encryption.	Deterrent; makes confidential information/data more secure (i.e, website payment transactions)	X	High

Date: _____

Physical controls			
Control-name	Control type and explaination	Needs to be implemented (X)	Priority
Closed-circuit television (CCTV) surveillance	Preventative / detective; can reduce risk of certain events; can be used after event for investigation	X	High
Locks	Preventative; physical and digital assets are more secure	X	High

Note: Compliance regulations are laws that organizations must follow to ensure private data remain secure.

The final common element of an internal security audit is ~~"communication"~~. "communication"

Once the internal security audit is complete, results and recommendations need to be communicated to stakeholders.

Stakeholder communication

- Summarizes scope and goals
- Lists existing risks.
- Notes how quickly those risks need to be addressed
- Identifies compliance regulations.
- Provides recommendations.

Date:

What you'll Learn

- Logs
- SIEM dashboards
- Common SIEM tools

Log: A record of events that occur within an organization's systems and networks.

Common log sources:

- Firewall logs
- Network logs
- Server logs

A Firewall log is a record of attempted or established connections for incoming traffic from the internet. It also includes outbound requests to the internet from within the network.

A network log is a record of all computers and devices that enter and leave the network. It also records connections between devices and services on the network.

A server log is a record of events related to services, such as websites, emails, or file shares. It includes actions such as login, password, and username requests.

SIEM dashboard:

SIEM solutions rely on dashboards to collect and analyze log data from various sources, providing actionable insights for analysis and normalization.

Date: _____

Security Information and event management (SIEM)

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

Different types of SIEM tools

- Self-hosted
- Cloud-hosted
- Hybrid

Note: Splunk Enterprise, Splunk cloud, and chronicle are common SIEM tools that many organisations use to help protect their data and systems.

Splunk Enterprise: A self-hosted tool used to retain, analyze, and search an organisation's log data to provide security information and alerts in real-time.

Splunk cloud: A cloud-hosted tool used to collect, search and monitor log data.

Chronicle: A cloud native tool designed to retain, analyze, and search-data.

Date:

What you'll learn

- Playbooks
- Six phases of incident response

Playbook: A manual that provides details about any operational action.

It also clarify what tools should be used in response to a security incident.

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

Incident response playbook phases:

- Preparation
- Detection and analysis.
- Containment
- Eradication and recovery
- Post incident activity
- Coordination

Preparation: Organizations must prepare to mitigate the likelihood, risk, and impact of a security incident by documenting procedures, establishing staffing plans, and educating users.

Detection and analysis: This phase detect and analyze events using defined processes and technology.

Date: _____

Containment: Its goal is to prevent further damage and reduce the immediate impact of a security incident.

Eradication and recovery: It involves the complete removal of an ~~incident~~ incidence artifacts, so that an organization can return to normal operations.

Post incident activity: It includes documenting the incident, informing organizational leadership, and applying lessons learned to ensure that an organisation is better prepared to handle future incidents.

Coordination: It involves reporting incidents and sharing information throughout the incident response process based on the organization's established standards.

Note: SIEM tools and playbooks work together to provide a structured and efficient way of responding security incidents.

PROJECT BASED ON RISK ASSESSMENT AND THREAT MANAGEMENT

Company: Avanza Solutions

Sector: Digital Technology and Automation

Training ~ PDF # 1

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

Yes: They conduct cybersecurity awareness training regularly, although resource limitations may impact the extent of training. Recognizing its importance, the organization invests in educating employees to maintain a strong security posture within budget constraints.

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

Yes: They provide training on secure password storage practices, acknowledging the challenge of enforcing consistent application across diverse systems. Despite difficulties, the organization emphasizes security education to enhance overall awareness and practices.

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

No: They face operational challenges that lower the frequency of anti-phishing campaigns. Resource and time constraints impact the ability to conduct these campaigns quarterly, though they are recognized as crucial for cybersecurity.

4. Does everyone in your organization understand the risk associated with cybersecurity?

No: Universal awareness is lacking Avanza, and reporting procedures may lack clarity. The organization recognizes the variability in employee backgrounds and the complexity of cybersecurity topics, contributing to inconsistent awareness levels.

Access Control ~ PDF # 3

5. Are all vendor default accounts changed or disabled?

No: Changes to vendor default accounts are inconsistently applied across systems at Avanza. Decentralized IT management and oversight contribute to disparities in security practices.

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

Yes: They maintain a policy of minimal exposure to reduce potential vulnerabilities. The organization enables only essential services, protocols, daemons, and functions, emphasizing continuous monitoring and updates.

7. Is all unnecessary functionality removed or disabled?

No: They face challenges in removing all non-essential functionality due to operational requirements and system interdependencies. Balancing security with operational needs is a complex task.

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

Yes: They take immediate action upon employee departure, ensuring account disablement or deletion to prevent unauthorized access. This proactive measure safeguards against potential security breaches.

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

No: Uniform implementation of screen idle times is challenging Avanza. Device variations and user needs contribute to difficulties in standardizing this security measure.

End User ~ PDF # 9

10. Do you provide end-users a tool to save all passwords?

No: They do not uniformly provide tools for password management to end-users. The organization acknowledges the diversity of user preferences and the complexity of implementing a unified system, contributing to this limitation.

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

Yes: They have implemented a password policy to enhance security. However, the enforcement of this policy might not be consistent across all users and systems. This inconsistency arises due to factors like user awareness, password change requirements and system limitations.

End Points ~ PDF # 9

12. Are all endpoint logs ingested by smart technology using threat intelligence and AI?

Yes: They employ advanced technology to analyze endpoint logs, utilizing threat intelligence and AI. This enhances threat detection and response capabilities, fostering a proactive security approach.

13. Do you harden all endpoints and remove unnecessary functionalities?

No: Complete hardening of all endpoints is challenging for Avanza. This is due to the diverse requirements of job functionalities, varying applications, and potential limitations in removing non-essential components without impacting job performance.

14. Do you have next-generation anti-malware protection on all endpoints with a threat intelligence-based platform?

No: Implementation challenges arise for They due to compatibility issues with existing systems. The organization acknowledges the importance of advanced protection but faces difficulties in ensuring uniform deployment across all endpoints.

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

Yes: They endeavor to control access to its network by preventing non-enterprise devices from connecting. However, the organization faces limitations in maintaining strict control over all external devices attempting to access the network. Like varied device types, evolving technologies, and the diverse locations from which devices connect.

17. Do all endpoints have non-disabling antivirus with automatic updates?

Yes: They ensure uniform antivirus deployment on all endpoints. The antivirus is designed to be non-disabling, and automatic updates are implemented, ensuring up-to-date threat protection.

18. Do all endpoints have next-generation anti-malware applications?

No: Limited implementation on all endpoints is due to compatibility issues faced by Avanza. Despite recognizing the importance of advanced malware protection, achieving widespread deployment is hindered by compatibility challenges with existing systems.

Event Management ~ PDF # 20

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

No: The duration of log storage Avanza may vary. Achieving uniform storage for a minimum of two years poses challenges, considering factors such as resource constraints, evolving compliance requirements, or the nature of the logged information.

20. Are all devices generating logs?

No: Logging capabilities across devices may not be uniform at Avanza. The organization faces challenges in ensuring that all devices consistently generate logs, with non-uniformity arising from differences in device types,

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

No: Daily log reviews present a challenging task for them. Achieving daily analysis is difficult due to factors such as resource constraints, the volume of generated logs, or the need for specialized expertise in log analysis.

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

Yes: They maintain a mature and well-organized cybersecurity incident response system, demonstrating a commitment to thorough investigations of all incidents. This preparedness is crucial for promptly addressing and mitigating potential cybersecurity threats, ensuring a resilient security posture.

Security Architecture

~PDF 8

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

Yes: They provide employees with access only to the tools and resources necessary for their specific job functions. They achieve this through a robust access control system that evaluates the job requirements and assigns access rights, accordingly, ensuring that each employee has just what they need to perform their duties effectively.

24. Do you utilize the principle of least privilege?

Yes: They practice the principle of least privilege across its network. This means that employees are granted only the minimum levels of access or permissions they need to carry out their job functions. The company manages this by regularly reviewing user roles and access rights, ensuring that privileges are aligned with job requirements and are not excessive.

25. Do you deploy a zero-trust model?

Yes: They have limited implementation of the zero-trust model. Implements some elements in place, the model is not fully integrated across the organization.

~ PDF # 13

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

Yes: But it's implementing multifactor authentication (MFA) for all external connections is limited.

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

Yes: But its enforcement varies within Avanza, especially when accessing critical infrastructure and data.

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.)

Yes: They effectively manage all credentials on their network, including the ability to quickly conduct password resets for every account. Managed through a centralized credential management system that tracks and controls access credentials, ensures efficient and secure handling of password resets and account management, even for service accounts.

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

Yes: They regularly assess their Active Directory to ensure it is properly configured and secured. They conduct these assessments periodically to identify and rectify any security vulnerabilities, ensuring that the Active Directory remains robust and resistant to potential cyber threats.

30. Are you actively monitoring the security of your Active Directory?

Yes: They actively monitor the security of their Active Directory. This involves continuous oversight using specialized security tools and protocols to detect and respond to any irregularities or potential breaches, thereby maintaining the integrity and security of their directory services.

31. Do your perimeter firewalls have a deny-all rule unless otherwise authorized?

Yes: Perimeter firewalls are configured with this rule unless specific authorization is provided. This strict approach ensures that only verified and necessary traffic is allowed through the network, significantly enhancing the company's network security.

32. Is your demilitarized zone (DMZ) secured?

No: Securing the demilitarized zone (DMZ) is a significant challenge for Avanza. The complexity of maintaining security in these intermediate areas between the internal network and the external internet is a reason for this difficulty.

33. Has it been ensured that there are no data, databases, or stored accounts on the DMZ?

No: Ensuring that the DMZ is free of data, databases, or stored accounts is challenging for Avanza. This might be due to the complexities involved in managing and segregating network traffic and data storage in these zones.

34. Do you deploy anti-spoofing technology to prevent forged IP addresses from entering the network?

Yes: They deploy anti-spoofing technology to protect their network. Which helps prevent forged IP addresses from entering the system, which protects against certain types of cyber-attacks based on IP spoofing.

35. Do you prevent the disclosure of internal IP addresses and routing information on the Internet?

Yes: They take measures to prevent the disclosure of internal IP addresses and routing information on the Internet. They employ various security protocols and configurations to ensure that sensitive internal network details are not exposed to external parties.

Threats ~ PDF # 10

42. Do you perform periodic targeted threat hunts?

Yes: They conduct targeted threat hunts periodically. These hunts are designed to proactively identify and mitigate potential cyber threats but are not frequent. They use a combination of manual expertise and automated tools to execute these hunts effectively.

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?

Yes: They actively use threat intelligence from various sources to stay ahead of potential cyber threats. They utilize specialized tools for analyzing this intelligence, helping them quickly identify and respond to emerging security risks.

44. Does it include performing routine dark web reconnaissance to learn what exists on the dark web about your brand and enterprise structures? ~ PDF # 11

No: They do not regularly monitor the dark web for information about their brand. This is mainly because dark web monitoring requires specialized tools and expertise, which can be challenging to maintain in-house.

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

Yes: They maintain a robust monitoring system for their vendor and third-party connections. This includes regular audits and automated systems to ensure compliance and detect any security issues, safeguarding their supply chain. ~ **PDF # 7**

Testing ~ PDF # 9

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

Yes: They conduct at least one penetration test annually with the help of a third-party service. This approach ensures an objective evaluation of their network and systems' security. The third-party experts bring a fresh perspective and specialized skills to identify vulnerabilities that internal teams might overlook.

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?

Yes: They routinely perform vulnerability scans and stick to a strict protocol to remediate identified issues. They prioritize fixing vulnerabilities with a CVSS score of 4 or more within 60 days and address all other vulnerabilities within 120 days. This systematic approach helps in maintaining a strong defense against potential cyber threats.

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

Yes: They conduct scans of their Internet-facing infrastructure, but these scans may not be as frequent or comprehensive as required. Regular and thorough scanning is crucial for detecting potential vulnerabilities and penetration risks, and there might be a need for more frequent or detailed assessments.

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

Yes: They attempt to perform annual business impact analyses and risk analysis reports with the help of internal and external auditors. However, they encounter challenges in conducting these analyses annually, due to the complexity of the process and sometimes the need for more in-depth collaboration with auditing experts.

Data Management ~ PDF # 3

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

Yes: They maintain strict practices for storing confidential data. They keep such data storage to a minimum and ensure it is securely deleted once it's no longer needed. This approach is part of their broader data management and security strategy, aiming to reduce the risk of data breaches and comply with data protection regulations.

61. Do you require data classification throughout the network?

No: The company strives for data classification throughout their network, but implementing a universal system is challenging. The complexity arises from the diverse nature of data and the need for detailed categorization to ensure appropriate handling and security measures for different data types.

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

Yes: They have deployed data loss prevention programs in some areas where confidential data resides, but the coverage may be inconsistent. This variation in deployment could be due to differing levels of risk assessment, resource allocation, or the complexity of integrating DLP solutions across various network and cloud environments.

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

Yes: They have implemented robust measures to prevent the copying of confidential data to external devices and restrict external devices from being connected to endpoints. This is achieved through a combination of technical controls, such as device management software, and policy enforcement, ensuring that sensitive data remains secure and is not exposed to risks associated with external device usage.

Software Development ~ PDF # 3

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

Yes: Processes and mechanisms for secure software development are defined at Avanza, but their universal understanding and adoption may be limited. The organization emphasizes secure development practices, although challenges in ensuring widespread implementation exist.

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?

No: They face challenges in achieving universal adoption of prevention techniques by software development personnel. While techniques are defined, ensuring consistent implementation across all software remains challenging due to various factors, including resource constraints and evolving technologies.

67. Are these applications protected against attacks?

Yes: They have implemented measures to protect public-facing web applications against attacks. The organization is proactive in addressing security concerns, employing various strategies to enhance the resilience of these applications against potential threats.

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

Yes: They maintain separation between preproduction and production environments, although enforcement with access controls may face challenges. The organization recognizes the importance of environment separation but acknowledges ongoing efforts to strengthen and ensure consistent enforcement.

For a fintech service-based company like Avanza Solutions, the following five threats are particularly critical due to their potential impact on financial operations, customer trust, and regulatory compliance:

1. Data Breaches:

Unauthorized access to sensitive customer and financial data, leading to potential identity theft, financial fraud, and reputational damage.

Impact: Financial losses, regulatory penalties, damage to customer trust.

Mitigation Approach: Implement robust encryption, conduct regular security audits, monitor network traffic, and ensure compliance with data protection regulations.

2. Phishing Attacks:

Attempts to trick employees into disclosing sensitive information or credentials through deceptive emails or messages.

Impact: Unauthorized access, data compromise, potential financial fraud.

Mitigation Approach: Conduct regular phishing awareness training, implement email filtering systems, use multi-factor authentication (MFA), and regularly update security policies.

3. Ransomware Attacks:

Malicious software encrypts data, demanding payment for its release.

Impact: Disruption of operations, financial losses, potential data loss.

Mitigation Approach: Regularly update and patch software, employ advanced antivirus solutions, conduct regular backups, and educate employees about cybersecurity best practices.

4. Regulatory Compliance Risks:

Failure to comply with financial regulations and data protection laws.

Impact: Regulatory penalties, legal consequences, reputational damage.

Mitigation Approach: Stay informed about regulations, conduct regular compliance audits, implement controls to adhere to industry standards, and establish a robust governance framework.

5. Insider Threats:

Malicious actions or negligence by employees or contractors.

Impact: Unauthorized access, data breaches, potential financial fraud.

Mitigation Approach: Enforce the principle of least privilege, monitor employee activities, conduct background checks, establish clear security policies, and educate employees about the consequences of insider threats.

These threats require a holistic approach that combines technological solutions, employee education, and continuous monitoring. By prioritizing efforts to mitigate these critical threats, Avanza Solutions can enhance its overall cybersecurity resilience in the dynamic fintech landscape.