SKILL ACTIVITY NO: 5 Date: 22/04/2022

(To be filled by the Student)

Title: Application of Security Tools in Banking Sector

1. What is the purpose of this activity ? (Explain in 3 – 4 lines)

The purpose of this activity is to :-

<a> Understand what are FINTECH SECURITY GUIDELINES mandatory by MHA, GOI.

<b> what are mandatory SECURITY-STANDARDS for Fintech startups / Banks.

<c> what SECURITY-TOOLS used for performing Penetration Tests in Banking Application ?

<d> CISO → Post mandatory to form inside any FINTECH ORGANISATION.

<e> what are multiple INFOSEC SECURITY GOVERNANCE guidelines.

All above points objective is to make Banking System (ROBUST)

2. Step performed in this activity (Explain in 5 – 6 lines)

Steps performed in this skill activity are as follows :-

(FOR PERFORMING PENETRATION TESTS)

Step1: Plan the Penetration Test : Plan the project's scope, objectives & stakeholders.

Step2: Gather Information: Conduct Network surveys & Identify the No. of Reachable systems.

Step3: Scan for vulnerabilities: Identify the vulnerabilities that exist in Network & systems.

Step4: Attempt the penetration: Estimate How long a pen-test will take on set targets and begin.

Step5: Analyze the report: → Analyze & highlight critical vulnerabilities in our assets.

Step6: Clean up the MESS. → Clean up the compromised hosts without disturbing Normal operations.

RECENT SECURITY INCIDENT REPORT:

↳ According to ICO's survey → the financial services sector has the highest Number of cybersecurity incidents at any industry.

DEFINITION OF A PENETRATION TEST:

↳ A Penetration Test involves the use of a variety of manual & automated techniques to simulate an attack on an organisation's information security arrangements. A Penetration Test is typically an assessment of IT infrastructure, networks & business applications to identify attack vectors, vulnerabilities & control weaknesses.

COMMON FORM OF PENETRATION TESTING IN BANKS:

- Application Penetration Testing ← (Typically, web applications, which finds technical vulnerabilities)
- Infrastructure Penetration Testing → (which examines servers, firewalls & other Hardware for security vulnerabilities)

WHY PEN-TEST IS IMPORTANT?

↳ Pen-Test are conducted with the aim of identifying & helping to address security weaknesses that criminal might seek to exploit in order to compromise assets and steal data.

↳ Regular Pen-Test is crucial to not only exposing and remediating vulnerabilities but achieving compliance with the latest data & information security requirements, including those mandated by the FCA, PRA, GDPR, NIS Directive, SWIFT & MIFID II.

FINTECH SECURITY GUIDELINES:

Every Qualified Fintech Entity shall put in place procedures and processes to ensure robust information security procedures as specified below:—

3. What resources / materials / equipments / tools did you use for this activity ?

1. Resources :→ eis-india.org/Internet-governance/resources/security-standards
2. → pcisecuritystandards.org/
3. → financialit.net/blog/
4. → crest-approved.org/wp-content/
6. Tools: laptop/Desktop-PC
→ Windows-10 (os)
→ Chrome web Browser
7. → Stable Internet Connection

4. What skills did you acquire ?

1. Whether abt (Penetration Test & Penetration Testing)
2. Performing Penetration Test in
3. Real world on multiple-Gap companies.
4. Difference between Fintech & Infosec Security Guidelines
5. What are the Fintech Security Guidelines issued by RBI?
6. Different mandatory Security Standards
7. Different Security Tools used by companies for Intrusion/Fraud Prevention.
8. Role of CISO in any Banking Organization.

5. Time taken to complete the activity ? 02:00 (hours)

Signature of Student

FINTECH SECURITY GUIDELINES

IT GOVERNANCE

- It lay down standards for Hardware or software prescribed by proposed Architecture.
- It detail Operational procedures for IT infrastructure
- Implement appropriate measures to ensure adherence to customer privacy.

Critical components of Information Security

- Risk Assessment
- Defining Roles & Responsibilities
- Access Control
- Design Controls
- Personnel Security
- Physical security
- User Training & Awareness
- Incident Management
- Migration Controls
- Encryption
- Data Security
- Vulnerability Assessment
- Security measures against Malware
- Patch Management
- Change Management
- Audit Trails

INFORMATION SECURITY GOVERNANCE

↳ (CISO) → A senior level official, of the Rank of GM/DGM/AGM should be designated as 'Chief Information Security officer' responsible for articulating & enforcing the policies that banks use to protect their Information Asset apart from coordinating the security related issues/ implementation within the organization as well as Relevant External Agencies.

CYBER FRAUDS

↳ Which fraud will come under the category of cyber fraud as per RBI ?

DEFINITION PROVIDED BY RBI (INDIA)

"A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank."

↳ Roles & Responsibilities & Organizational Structure for Fraud Risk Management:

↳ Indian Banks follow the RBI guideline for Reporting all frauds above ₹1 Cr to their respective Audit Committee of the Board. The Board for Final Supervision (BFS) of RBI Has observed that in terms of higher governance standards, the Fraud Risk Management & Fraud Investigation must be owned by the bank's CEO.

↳ Components of Fraud Risk Management:

- Fraud Prevention Practises
- Fraud Vulnerability Assessments
- Review of New Product & Processes
- Fraud Loss Limits
- Root Cause Analysis
- Data/ Information/ System Security
- KYC & KYE/Vendor Procedures
- Physical Security
- Creation of Fraud Awareness Amongst Staff & Customers

↳ Fraud Detection
- ↳ a) Detection of Fraud
- ↳ b) Transaction Monitoring
- ↳ c) Alert Generation & Redressal Mechanisms
- ↳ d) Dedicated Email ID & Phone Number for Reporting Suspected Frauds
- ↳ e) Mystery Shopping & Reviews
- ↳ f) Importance of Early Detection of Frauds.

⇒

↳ Fraud Investigation
- Fraud Risk Management Grp
- Specific Committee
- External Agencies

- ↳ a) Fraud Investigation Function
- ↳ b) Recovery of Fraud losses
- ~~↳ c)~~

⇓

↳ Fraud Reporting
- ↳ a) Frauds in
  - Merchant Acquiring Business
  - ATM acquiring Business
  - Bill
- b) Filing of Police Complaints

SOLN → (i) Customer Awareness on Frauds
- ↳ a) Creation of Customer Awareness on Frauds

(ii) Employee Awareness & Training
- ↳ a) Creation of Employee Awareness
- ↳ b) Rewarding Employee on Fraud Prevention

REAL-WORLD USECASE SOLUTION FOR FRAUD MANAGEMENT BY MC-KINSEY BANK

→ Banks often focus only a FRACTION of Total Financial-Crime, Fraud & Cyber Security Costs,

→ Many Banks identify partial Integration as their target state with a view that full AML Integration is an aspiration.

→ Ways to prevent fraud as per Mc-Kinsey & Company
- a) Collaborative Model
- b) Partially Integrated Model
- c) Unified Model