

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.
- 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 ~~are~~ 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)

- Step 1: Plan the Penetration Test: Plan the project's scope, objectives & stakeholders
- Step 2: Gather Information: Conduct Network surveys & identify the No. of Reachable systems.
- Step 3: Scan for vulnerabilities: Identify the vulnerabilities that exist in Networks & systems.
- Step 4: Attempt the penetration: Estimate How long a pen-test will take on set targets and begin.
- Step 5: Analyze the report: → Analyze & highlight critical vulnerabilities in our assets.
- Step 6: Clean up the MESS. → clean up the compromised hosts without disturbing Normal operations.

RECENT SECURITY INCIDENT REPORT:

↳ According to ICD'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:

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 criminals 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 : → els-india.org / [Internet-governance.org](https://internet-governance.org/) / Tools: laptop / Desktop-PC
→ resources / security - standards
2. → pcisecuritystandards.org /
3. → financialit.net/blog /
4. → crest-approved.org/wp-content/
5. → windows-10 (os)
6. → Chrome web browser
7. → Stable Internet connection

4. What skills did you acquire ?

1. WHY abt { Penetration Test & Penetration Testing }
2. Performing Penetration Test in
3. Real world on multiple - Cap 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 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.

IT GOVERNANCE

INFORMATION SECURITY GOVERNANCE

↳ (CISO)

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

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:

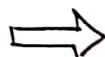
↳ Indian Banks follow the RBI guideline for Reporting all frauds above ₹1 Cr to their respective Audit Committee of the Board. The Board for Final Supervision (BFS) of RBI has observed that in terms of higher governance standards, the Fraud Risk Management & Fraud Investigation must be owned by the bank's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

Components of Fraud Risk Management:

- Fraud Prevention Practices
- Fraud Vulnerability Assessments
- Review of New Products & 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

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

Fraud Risk Management Ap
Specific Committee
External Agencies



↳ Fraud Reporting

- ↳ a) Frauds in
 - ↳ Merchant Acquiring Business
 - ↳ ATM acquiring Business
 - ↳ Etc
- ↳ 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 USE CASE SOLUTION FOR FRAUD MANAGEMENT BY MC-KINSEY BANK

→ Banks often focus on 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