IT RISK MANAGEMENT IN BANKING SYSTEM

Project report submitted in partial fulfillment of the requirement for the degree of

BACHELOR OF TECHNOLOGY

IN

ELECTRONICS AND COMMUNICATION ENGINEERING

By

Bhoomika Kandpal(211061)
Harshita Verma(211070)

UNDER THE GUIDANCE OF

Prof. Dr. Rajiv Kumar

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY,
WAKNAGHAT

May 2025

TABLE OF CONTENTS

CAPTION **PAGE NO.**

DECLARATION

We hereby declare that the work reported in the B.Tech Project Report entitled “**IT Risk Management in Banking System**” submitted at **Jaypee University of Information Technology, Waknaghat, India** is an authentic record of our work carried out under the supervision of **Prof. Dr. Rajiv Kumar**. We have not submitted this work elsewhere for any other degree or diploma.

Bhoomika Kandpal	Harshita Verma
211061	211070

This is to certify that the above statement made by the candidates is correct to the best of my knowledge.

Prof. Dr. Rajiv Kumar.

Date:

Head of the Department/Project Coordinator

ACKNOWLEDGEMENT

With profound gratitude, I first and foremost acknowledge the divine grace that enabled the successful culmination of this project.

My deepest appreciation and sincere thanks are extended to my supervisor, Prof. Dr. Rajiv Kumar, esteemed Head of the Department of Electronics and Computer Science at Jaypee University of Information Technology, Waknaghat. His enduring patience, perceptive direction, consistent encouragement, diligent oversight, constructive criticism, helpful insights, and meticulous review of numerous iterations at each phase were crucial to the completion of this work. I am deeply indebted for his generous support and commitment.

I also wish to convey my sincere gratitude to all those who contributed to the triumph of this project, whether directly or indirectly. In these unique times, I particularly recognize the diverse academic and administrative personnel who offered invaluable aid throughout this undertaking.

Lastly, I must express my profound thankfulness for my parents' unwavering support and steadfast patience.

LIST OF ACRONYMS AND ABBREVIATIONS

- **API:** Application Programming Interface
- **CBS:** Core Banking System
- **EKYC:** Electronic Know Your Customer
- **FIS:** Financial Information System
- **HTTP:** Hypertext Transfer Protocol
- **IFSC:** Indian Financial System Code
- **IPS:** Intrusion Prevention System IT: Information Technology
- **KYC:** Know Your Customer
- **MW:** Middleware NBFC: Non-Banking Financial Company
- **NEFT:** National Electronic Funds Transfer
- **NPCI:** National Payments Corporation of India
- **NSDL:** National Securities Depository Limited
- **OIC:** Oracle Integration Cloud
- **PAM:** Pluggable Authentication Modules
- **PAN:** Permanent Account Number
- **PRI:** Primary Rate Interface
- **PSP:** Payment Service Provider
- **RTGS:** Real-Time Gross Settlement
- **SaaS:** Software as a Service
- **UPI:** Unified Payments Interface

ABSTRACT

Our project is centered on an in-depth examination of IT risk management across key digital channels and payment infrastructures of the banking industry. We start with the establishment of the core contribution of information technology and the embedded risks in contemporary banking operations. Later stages of our project explore the particular risk environments and mitigation practices for important technological elements. This entails a close analysis of API (Application Programming Interface) security risks, monitoring techniques, and secure implementation best practices. In addition, our project explores the Unified Payments Interface (UPI) environment, detailing its architecture, transaction process, related security and operational risks, and critical monitoring and mitigation steps. A specific part of our project explains the call flow and architecture of the IVR system and gives a foundational knowledge for the risk assessment of this direct customer contact channel. Last but not least, our project treats the risk management aspects of core payment systems, i.e., NEFT and RTGS, describing their transaction flows, security mechanisms, and particular risk mitigation and monitoring needs. This integral analysis seeks to establish a comprehensive perception of IT risk management within various banking technologies and payment systems, ultimately culminating in the formulation of effective security and operational resilience guidelines for the institution.

CHAPTER 1

INTRODUCTION

1.1 The Critical Role of IT and the Landscape of IT Risk in Banking

1.1.1 The Foundation of Modern Banking: Information Technology

The operational foundation of the banking sector is becoming more and more dependent on information technology (IT). In order to provide a wide range of services, effectively handle intricate financial transactions, and safely store enormous amounts of sensitive data, banks heavily rely on IT systems. Although there are many benefits to the extensive integration of IT into banking operations, these institutions are also exposed to a number of technology-related dangers.

1.1.2 Defining and Understanding IT Risk in the Banking Sector

The operational foundation of the banking sector is becoming more and more dependent on information technology (IT). In order to provide a wide range of services, effectively handle intricate financial transactions, and safely store enormous amounts of sensitive data, banks heavily rely on IT systems. Although there are many benefits to the extensive integration of IT into banking operations, these institutions are also exposed to a number of technology-related dangers.

1.2 The Imperative and Challenges of IT Risk Management in Banking

1.2.1 The Paramount Importance of Proactive IT Risk Management for Banks

- A key component of banks' long-term stability and performance is effective IT risk management, which goes beyond simple operating requirements. Several important factors highlight its significance:
- Keeping private information safe: Large amounts of extremely sensitive consumer data, such as complex financial records, confidential personal information, and comprehensive transaction histories, are held in the custody of banks. To protect this data from unwanted access, data loss, and the constant threat of cyberattacks, strong IT risk management frameworks are essential.
- Making sure that operations are resilient: Modern banking depends on the availability and dependability of IT systems to operate well. These systems are essential to critical operations including safe online banking platforms, precise account administration, and effective payment processing.To keep these crucial operations resilient and continuous, effective risk management techniques are necessary.

- Preserving the confidence and trust of customers: Trust is crucial in the financial industry. Customers expect the highest level of security for the handling of their financial and personal information since they entrust banks with their financial well-being. Long-term loyalty and consumer confidence are greatly increased by an IT risk management framework that is clearly defined and strictly followed.
- Respecting Tough Regulatory Requirements: Global banking regulators enforce strict guidelines for IT risk management because they understand the financial sector's systemic significance. IT risk management is a crucial component of regulatory compliance since these rules are intended to safeguard consumers and maintain the general stability of the financial system.

- **1.2.2 Navigating the Complex Challenges of Managing IT Risks in Banking**

Even though IT risk management is of paramount critical importance, banks are confronted with an ever-changing and ever-more complicated set of challenges:

Emerging cyber threats: The frequency and sophistication of cyberattacks are spiraling out of control. Banks have to keep adapting their security features to counter more and more innovative and persistent threats, and it is always a challenge to remain one step ahead of the malicious players.

Legacy systems: A large proportion of mature banks continue to use older or "legacy" IT systems. These older systems tend to have significant security exposures and can be difficult and expensive to keep running and compatible with newer technology.

Data complexity: The volume of data banks handle, combined with its complexity and demand for real-time analysis and processing, brings substantial levels of complexity to data protection and governance initiatives.

Third-party dependencies: Banks often look to outside third-party vendors to supply them with various IT services and solutions as they seek efficiency and innovation. Though useful, these dependencies create added layers of risk that must be managed carefully and monitored to ensure the security and reliability of the overall ecosystem.

1.3 Effortech's Role in Addressing IT Risk in Banking

Effortech offers end-to-end Technology Risk Management solutions for Banks, Fintechs, NBFCs and other financial institutions in India. Effortech is driven by banking industry experts who appreciate the specific challenges of financial institutions in India.

Comprehensive Risk Assessment - Identify and assess technology risks unique to your organization
Regulatory Compliance - Remain compliant with RBI guidelines and other regulatory norms
Tailored Solutions - Banks, fintechs, and NBFCs have customized risk management solutions.
Continuous Monitoring - Active identification and mitigation of new technology risks

CHAPTER 2

API Risk Management in Banking Systems

2.1 Application Programming Interfaces (APIs) in Banking

2.1.1 Introduction to APIs

Application Programming Interfaces (APIs) are now banking's indispensable gadgets, facilitating interactions and data flow between various applications and systems. Although APIs pose many advantages, they also provide new risks, which banks must address.

An API refers to a set of communication protocols and subroutines employed by numerous programs to communicate back and forth. APIs enable different software programs to work together and share data, allowing banks to provide innovative products and enhance efficiency in operations.

"API full form is an Application Programming Interface that is a set of communication protocols and subroutines which are used by different programs to interact between them. A programmer can utilize different API tools to simplify and make their program easier.".

Additionally, an API helps programmers with an effective method for creating their own software programs. Therefore, Api meaning is where an API makes two programs or applications talk to one another through offering them needed tools and functionalities.

It receives the request from the user, forwards it to the service provider, and forwards the result obtained from the service provider again to the target user.

2.1.2 How APIs Work

How APIs function can be explained in the following way:

"The functioning of an API can be easily understood by a few easy steps. Imagine a client-server model in which the client initiates the request through a medium to the server and gets the response via the same medium.".

An API serves as an interface between two programs or systems for operation. The client is the customer/user (who initiates the request), the medium is the application interface programming, and the server is the back-end (where the request is received, and a response is sent).

Steps taken in the functioning of APIs – The client sends the requests through the APIs URI (Uniform Resource Identifier) The API calls the server upon receiving the request Then, the server sends the response to the API along with the information At last, the API sends the data to the client.

APIs are secure in attack terms as it contains authorization credentials and an API gateway to restrict access to reduce the security threats.

For the purpose of providing extra layers of security to the data, HTTP headers, query string parameters, or cookies are implemented. If we discuss the architectures, API's architectures are: REST (Representational State Transfer) SOAP (Simple Object Access Protocol)"

2.2 API Security Risks

APIs bring certain vulnerabilities into banking systems that need to be managed judiciously. The risks here mainly concern security breaches, data loss, and unauthorized access.

2.2.1 Unauthorized Access

APIs are valuable but a source of weakness if not suitably secured. Security risks mostly encompass:

Unauthorized access refers to the instance when people or systems access APIs without authorization. It can cause breaches of data, fraud, and other ill uses.

2.2.2 Data Breaches

APIs manage sensitive information, and a security breach can release such data to unauthorized sources. This can have dire ramifications for banks, which include financial losses, loss of reputation, and legal fines.

2.3 Monitoring API Vulnerabilities

Monitoring the usage of APIs and performance helps track and mitigate possible vulnerabilities. Mechanisms and techniques such as Oracle Integration Cloud (OIC) Dashboards assist in monitoring API traffic, identifying anomalies, and maintaining security.

2.3.1 Oracle Middleware (MW) Dashboard Monitoring

- Oracle Integration Cloud (OIC) Dashboards facilitate monitoring of Production APIs, i.e., their performance, success rates, and failures.
- Tracking these metrics very closely, we can quickly discover problems and troubleshoot API failure causes. Dashboard Access: - Log into your OIC (Oracle Integration Cloud) account and, on the home page, click on Integration to monitor the Production API.
- Some of these include "Common Audit" and "Finacle Provider". These integrations can be neglected while tracking API hits.
- External Integrations: - There are some integrations which are mapped at OIC end and are typically from other SAAS applications.
- These include CBS APIs as well as third-party services. These need to be tracked with extreme caution.
- The following are the details for some key external integrated APIs:
- **EKYC:** Utilized to process the KYC of the customer (Third Party API).
- **INT_CRIF_INQ:** Utilized to verify the credit score approval for sanction amount of loan.
- **AadharDV:** It is utilized to retrieve/generate Aadhar Token from Aadhar Data Vault.
- **GenericCardDetails:** It is the process of FIS and Paycraft cards APIs (CBS + Third Party API).
- This integration is to FIS card APIs (Third Party API).
- **LoanAccount:** This API is used to open a loan account (CBS API).
- **Collateral:** It is utilized to generate collateral for the customer who has applied for a loan (CBS API).
- **LoanPayOffWF:** It is utilized for payoff the loan amount (CBS API).
- **RetailCustomer:** This API is utilized to create the customer Id (CBS API).
- **Custom_Get:** These are the group of the custom get APIs (CBS API).
- **ExternalPayment:** This is the process to make transactions to beneficiary accounts (CBS API).
- **TermDeposit:** It is utilized to open the Term Deposit Account (CBS API).
- **Int_NSDL_PanValidation:** This API is utilized to validate the PAN Number of the customer (Third Party API).

- **EKYCWithBiometric:** This is the workflow to process the KYC as well as customer creation for partner (BlackBuck) (Third Party and CBS API).
- **InquiryLvl2/InquiryLvl4:** These are the group of DB get Inquiry APIs (CBS API).
- **LoanAccount_IndiaGold:** This API utilized to form a loan account for Partner (India Gold) (CBS API).
- **Custom:** These are the set of the custom APIs (CBS API).
- **SBAAcctAdd:** It opens the Saving Account (CBS API).
- The alert should be triggered for time spans as per hits mentioned in the previous list. It gives details like **primary identifier, Instance Id, status, duration and business identifier.**
- **Primary Identifier:** This field is made up of the Requested (UUID) with embedded API name.
- **Instance Id:** Instance Id is uniquid for middleware that is utilized in OIC to verify and examine the flow for each request.
- **Status:** Status informs us the request is in which step like in progress, succeeded and errored.
- **Duration:** The sum of time consumed in the course of processing API requests.
- **Business Identifier:** This column gives the data of the API request Sources (Partners Source Name, Vendors Source Name).
- The error occurs when the API is failed in the specified duration which is displayed in the Errors column.
- **Primary Identifier:** This column is made up of the **Requested (UUID**) with embedded API name.
- **Instance Id:** Instance Id is uniquid for middleware that is utilized in OIC to validate and examine the flow for each request. **Fault Location:** This field returns the location of the API request Destination (Partners Source Name, Vendors Source Name) where the API failed.
- **Error Time:** Gives the time and cause when the error was found in the request. The traces are made up of the request payload, the API journey through the internal/CBS integrations and the response payload.
- This Response payload will also include the information of scenarios in which the error has happened. The information of the error is presented in this error log. To analyze the errors, we need to check this log.
- This Response payload will also provide the information of situations where the error has been encountered. The information of the error is indicated in this error log. We will have to check this log for the analysis of the errors
- Important metrics for monitoring API health and security are:

  Error rates: Monitoring the number of API calls that lead to errors.

  Response time: Calculating the amount of time that the API responds to requests.

Traffic volume: Measuring the volume of API requests over a period of time.

Authentication failures: Monitoring failed attempts to authenticate API requests.

2.4 Best Practices for API Risk Mitigation

In order to properly address API risks, banks must institute the following best practices:

2.4.1 Secure API Design

Design APIs securely, including input validation, encryption, and rate limiting.

2.4.2 Strong Authentication and Authorization

Institute strong authentication and authorization processes to confirm the identity of API consumers and to govern access to resources.

2.4.3 Continuous Monitoring and Testing

Monitor API traffic continually for abnormal patterns and regularly test for security vulnerabilities.

CHAPTER 3

UPI (Unified Payments Interface) Risk Management

3.1.1 Introduction to UPI

The Unified Payments Interface (UPI) is a National Payments Corporation of India (NPCI)-developed real-time payment system that makes instant transfers from one bank account to another on a mobile platform. UPI has transformed Indian digital payments for its convenience, interoperability, and instant speeds. UPI enables one mobile application to support multiple bank accounts and to accept payments via Virtual Payment Address (VPA).

3.1.2 UPI Architecture

The UPI architecture has multiple important participants:

NPCI: The regulatory authority that created and operates the UPI ecosystem.

PSPs (Payment Service Providers): Parties (banks or third-party companies) that offer UPI apps to customers.

Banks: The financial entities that maintain the customers' accounts and enable the transfer of funds.

Customers/Merchants: The users that make and accept payments using UPI.

UPI transactions are facilitated mainly by APIs that allow efficient communication among the participants.

3.2 UPI Transaction Flow and Security

3.2.1 UPI Transaction Flow in General

The typical UPI transaction flow is as follows:

The payment request is initiated by the payer using his UPI app.

The PSP application of the payer sends the transaction information to NPCI.

NPCI validates the transaction and triggers payer authentication (through UPI PIN).

The amount is debited from the account of the payer by the payer's bank.

The amount is credited to the payee's account by the payee's bank.

Transaction confirmation is sent to both the payer and payee.

3.2.2 Data Security in UPI

UPI transactions entail the exchange of sensitive information, such as:

Account information,

Transaction value,

User authentication (UPI PIN),

Protecting the security and confidentiality of such information is crucial. UPI utilizes a number of security protocols, including encryption, authentication schemes, and secure APIs, to safeguard data during transmission and storage.

3.3 UPI-Related Risks

3.3.1 Security Threats

Phishing and Social Engineering: The attackers can try to trick users into sharing their UPI PIN or other confidential details through fake messages or websites.

Mobile Device Compromise: Malware or unauthorised access of mobile devices can compromise UPI apps and result in fraudulent transactions.

API Vulnerabilities: Security vulnerabilities within the APIs employed for UPI transactions can be targeted by the attackers to intercept or manipulate transactions.

Transaction Fraud: Unauthorized transactions may be created because of identity theft, account takeover, or fraud.

3.3.2 Operational Risks

System Failures: Technical issues or system failure can hinder UPI services and stop users from receiving or sending payments.

Processing Errors: Processing errors in transactions can result in debiting or crediting wrong amounts, resulting in user's or bank's financial loss.

3.4 UPI Risk Mitigation and Monitoring

3.4.1 Security Practices

- **Strong Authentication:** Transaction authorization in UPI is dependent on the UPI PIN. Strong PIN policies and other modes of authentication, such as biometric authentication, must be imposed by PSPs and banks.
- **Encryption:** Data being transmitted while performing UPI transactions must be end-to-end encrypted to keep sensitive information safe.
- **Fraud Monitoring Systems:** Banks and PSPs must put in place stringent fraud monitoring systems that can catch and block suspicious UPI transactions in real time.
- **API Security:** Secure API design, authentication, and authorization procedures are required to secure UPI APIs from exposure.
- **User Awareness:** Raising user awareness on UPI security best practices is necessary to avoid phishing and other social engineering attacks.

3.4.2 Monitoring UPI Infrastructure

UPI infrastructure monitoring is crucial for the security, reliability, and performance of UPI. This may include:

Server Monitoring: Employing tools such as PuTTY to remotely access and monitor servers that host UPI applications and systems.
Authentication Management: Using PAM (Pluggable Authentication Modules) to authenticate server access and implement strict authentication policies.
API Monitoring: Monitoring API traffic, error rates, and response times to identify anomalies and suspected security threats.
Transaction Monitoring: Monitoring transaction patterns for detecting fraudulent activity.

Chapter 4:

IVR System Architecture and Call Flow

4.1 Introduction

This chapter describes the architecture and end-to-end call flow of the Interactive Voice Response (IVR) system. It is important to understand this flow for Level 1 (L1) monitoring because it gives a guideline for recognizing the various phases of a customer interaction and possible points of failure. This chapter specifies the events from the customer making a call to the multiple backend systems that handle the request.

4.2 Initiation of call by IVR

The customer makes contact with the IVR system by calling the Toll-Free Number, as designated.

4.3 Reception by IVR System

Once the toll-free number has been dialed, the IVR System (Interactive Voice Response) picks up the call. This is the initial step where the automated system gains possession of the interaction.

4.4 Request to Google Cloud

When the call is received by the IVR system, it sends a Request to Google Cloud. This establishes that the IVR platform used takes advantage of Google Cloud services for processing and routing of the call.

4.5 Google Cloud Processing

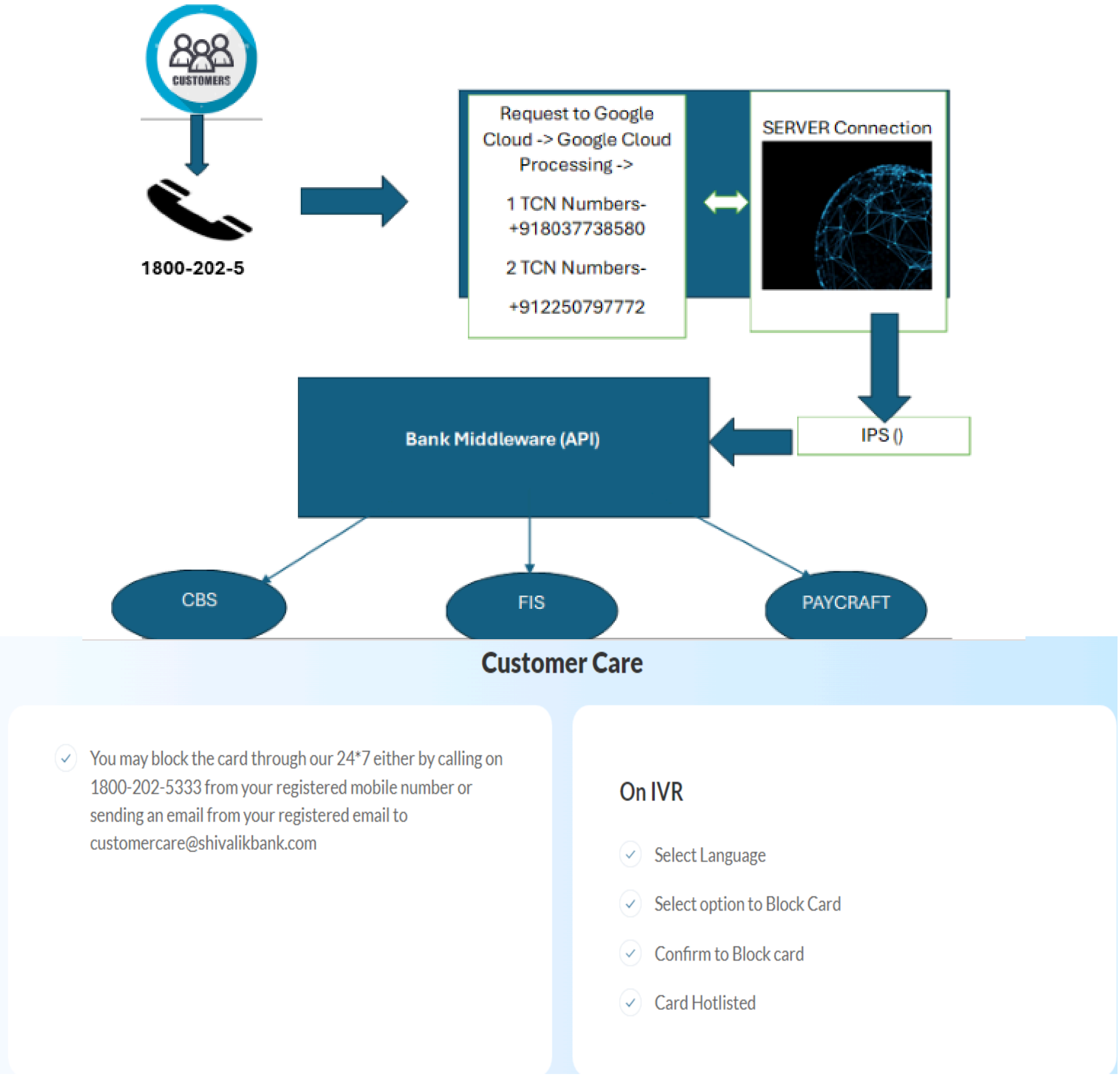
The Google Cloud Processing step entails the cloud infrastructure performing the initial processing of the call. Interestingly, the diagram shows handling of 2 TCN (Telephone Communication Number) numbers. These TCNs are special numbers linked to the telephone communication being processed in the Google Cloud setup.

4.6 Server Connection

After processing by Google Cloud, a SERVER Connection is made. This means the Google Cloud environment connects to the internal servers of the bank in order to proceed with further processing of the customer's request.

4.7 IPS (Intrusion Prevention System)

This specific flow demonstrates how the general architecture is utilized for a particular service.



Customer Care

✓ You may block the card through our 24*7 either by calling on 1800-202-5333 from your registered mobile number or sending an email from your registered email to customercare@shivalikbank.com

On IVR

- ✓ Select Language
- ✓ Select option to Block Card
- ✓ Confirm to Block card
- ✓ Card Hotlisted

Fig 1

Chapter 5

NEFT and RTGS Risk Management

5.1 Introduction to NEFT and RTGS

The National Electronic Funds Transfer (NEFT) and Real-Time Gross Settlement (RTGS) systems are core to the payment infrastructure of India, supported by the Reserve Bank of India (RBI). The systems support electronic transfer of funds between branches of banks in the country and play a central role in the support of economic activities and financial transactions. Effective management of risks is essential to secure the safety, efficiency, and reliability of the national payment systems.

5.1.1 Overview of NEFT

NEFT is a deferred batch-based net settlement system. [As per common knowledge about NEFT] Payments instructed till a given cut-off period are pooled in batches and executed at intervals during the day. Payment to the beneficiary's account is made either on the same day or next business day based on initiation timing and the batching schedule of execution. NEFT finds extensive usage in a range of payment applications such as salary payments, bill payments, and interbank transfers. Its extensive use and the huge volumes of transactions handled necessitate strong risk management.

5.1.2 Overview of RTGS

Unlike in NEFT, in the Real-Time Gross Settlement (RTGS) system, funds transfer is settled continuously and in real-time on an individual transaction basis. [General knowledge of RTGS] As soon as the transaction has been authenticated and approved, the transfer becomes irrevocable and conclusive. RTGS is mostly employed to clear and settle high-value transactions in real-time, including interbank transactions and money market transactions. The high values and real-time nature require strict risk management procedures to reduce the likelihood of systemic risks.

5.2 NEFT and RTGS Transaction Flow and Security

The smooth and secure processing of NEFT and RTGS transactions is dependent on well-documented processes and strong security controls applied at every phase of the transaction life cycle. A proper understanding of these processes and security controls is critical to effective risk management.

5.2.1 Typical NEFT Transaction Flow

The NEFT fund transfer process takes the form of a sequence of sequential steps having definite responsibilities as well as security aspects:

Initiation: Starting with the remitter, who is the initiator of the transfer of funds, the first step is placing a transaction order with his/their bank. [As presented earlier] It includes vital details required for transfer, such as:

- The beneficiary's name is a clear identification of the payee.
- The account number of the beneficiary, where the credit needs to be done.
- Bank name and branch of the beneficiary, which determines the destination financial institution.
- The Indian Financial System Code (IFSC), an 11-character unique code that serves to identify every bank branch that is part of the NEFT scheme, facilitating correct routing of the transaction.
- The amount to transfer, determining the financial value of the transaction.
- The account details of the remitter, determining the account from which the amount will be deducted. [Based on general knowledge of NEFT]

This initiation may be done through a number of channels, including:

- Physical branch visits, where the remitter completes a NEFT request form.
- Online banking sites, offering convenient access to account holders.
- Mobile banking apps, allowing fund transfers on the move. [General knowledge of NEFT]
- The originating bank ensures the authenticity of the remitter and the correctness of the information provided.

Validation: On receiving the request for transaction, the initiating bank conducts a series of crucial validations to check the integrity and viability of the transfer. [As defined earlier] These include:

- Verifying the remitter's account details to confirm the existence and status of the account.

- Checking the beneficiary's account information, including IFSC code and account number, to check for its validity.
- Verifying the remitter's account balance to ensure that there are adequate funds available to meet the transfer value and any charges that may be incurred.
- Applying any transaction limits or restrictions that are applicable. [Assuming general knowledge of NEFT]
- These checks are essential to avoid errors, fraud, and unauthorized transactions.

- **Batching and Forwarding:** NEFT uses a batch-processing system, under which transactions placed within a window of time are bunched together. [As introduced earlier] The originating bank accumulates these transactions and sends them to the NEFT Service Centre, run by the Reserve Bank of India (RBI). [As introduced earlier] These batches are normally processed half-hourly. [Based on general knowledge about NEFT processing] This batching is done to maximize the system's efficiency by processing several transactions at one go.

- **Processing at NEFT Service Centre:** The NEFT Service Centre is the focal point of the transaction process. [As introduced earlier] It accepts batches of transactions from originator banks, categorizes them based on the destination bank, and sends the individual transactions to the specific destination banks. [As introduced earlier] Sorting and routing of transactions ensures transactions are sent to the right recipient financial institutions.

- **Settlement:** Settlement is the essence of the process of fund transfer, wherein the actual transfer of funds between banks takes place. [As introduced earlier] In NEFT, there is settlement on a net basis. [As introduced earlier] It implies that the RBI accounts for the originating bank and credits the destination bank account with the net amount due or received for all the transactions in a batch. [On general knowledge of NEFT settlement] This netting procedure decreases the total amount of funds to be transferred between banks.

- **Credit to Beneficiary:** On receiving the NEFT Service Centre funds, the destination bank credits the account of the beneficiary. [As defined earlier] Depending on the destination bank's processing time, the time taken for the beneficiary to receive the funds may differ. [On general knowledge of NEFT processing]

- **Confirmation:** To give assurance and transparency to the remitter, the beneficiary bank can send a confirmation of the credit to the originating bank. [As introduced earlier] The originating bank, in turn, notifies the remitter of the successful completion of the transfer. [As introduced earlier] This process of confirmation gives a record of the transaction.

5.2.2 Typical RTGS Transaction Flow

- The RTGS transaction process is defined by its promptness and irrevocability, intended for high-value, time-sensitive payments.
- **Initiation:** Like NEFT, the RTGS transaction is initiated by the remitter requesting a fund transfer from their bank. [As explained earlier] The request includes the same basic details of the beneficiary, the amount, and the account of origin. [From general knowledge of RTGS] RTGS transactions are initiated, however, through bank branches or dedicated online banking sites because of the high amounts involved.
- **Validation:** The originator bank carries the intense validations to ensure the validity of the information and that there is enough fund available. [As introduced earlier] Due to the high value of RTGS transactions, such validations tend to be more intense compared to those conducted for NEFT transactions.
- **Authorization and Forwarding:** Once authenticated successfully, the originating bank makes the authorization for the transaction. [As explained earlier] Authorized transaction in RTGS is, thereafter, delivered directly and outright to the RTGS system provided by the RBI. [As explained earlier] Direct transmission forms a significant differentiation from the batch-processing mechanism employed by NEFT.
- **Settlement and Processing:** The RTGS system settles the transaction on a gross basis, i.e., every transaction is settled separately and in real-time. [As introduced earlier] The RBI debits the account of the originating bank and credits the account of the destination bank with the RBI for the entire value of the transaction. [As introduced earlier] This real-time and gross settlement makes the transfer final and irrevocable, removing settlement risk.
- **Credit to Beneficiary:** The credit is received by the destination bank and credited to the beneficiary's account immediately. [As introduced earlier] The RTGS transaction's near-instant settlement ensures that the beneficiary receives the funds without delay.

- **Confirmation:** The RTGS system and the beneficiary bank send confirmations to the originating bank and the remitter, giving immediate notice of successful transfer. [As introduced earlier]

5.2.3 Data Security in NEFT and RTGS

Data security in data being sent and processed through NEFT and RTGS systems is of utmost significance. There is a multi-layered method for securing the confidentiality, integrity, and authenticity of financial data.

- **Encryption:** Encryption is a basic security feature employed to shield sensitive information while in transit. [As was previously discussed] Cryptographic functions are used to convert information into an unreadable form so that it cannot be deciphered by an unauthorized party if intercepted. [Based on general knowledge of cryptography] Symmetric as well as asymmetric encryption methods can be employed, as per the particular requirements of the communication channel.
- **Secure Communication Channels:** Secure and dedicated communication channels are set up for the message exchange between participating banks and the RBI. [As explained earlier] These are typically private networks or virtual private networks (VPNs) with high security protocols to avoid unauthorized entry and eavesdropping. [General knowledge of network security]
- **Authentication and Authorization:** Robust authentication and authorization processes are put in place to authenticate the identities of banks and authorized staff using the NEFT and RTGS systems. [As already discussed]

  Authentication provides assurance that only valid parties are permitted to use the system. This can include the use of passwords, digital certificates, or multi-factor authentication, which involves two or more independent authentication factors.

  Authorization controls limit what authenticated users can do according to their roles and responsibilities. This least privilege principle reduces the likelihood of unauthorized activity
- **Message Integrity Checks:** To maintain the integrity of transaction messages, checks are made to identify any unauthorized changes or tampering while in transit. [As above] These checks can be done through the use of digital signatures or message authentication codes (MACs), which give confidence that the received message is identical to the sent message.
- **Auditing and Logging:** Detailed audit trails and transaction logs are carefully kept to capture all activity within the NEFT and RTGS systems. [As mentioned earlier] These logs create a detailed history of who used the system, what was done, and when it was done. This is extremely useful for tracking system activity, identifying unusual activity, investigating incidents, and maintaining accountability.

5.3 NEFT and RTGS-Related Risks

The functioning of NEFT and RTGS systems, although bringing substantial advantages in terms of efficiency and speed of fund transfer, also poses financial institutions to a variety of possible risks. Proper risk management is essential to counter these risks and provide for the sustained stability and reliability of these key payment systems. These threats can be generally classified into security threats, which pose a risk to the confidentiality, integrity, and availability of information and systems, and operational threats, which are caused by mistakes or breakdowns in processes, systems, or human elements.

5.3.1 Security Risks

Security threats in NEFT and RTGS systems are a primary concern for banks. Such threats can result in huge financial losses, reputational damage, and loss of customer confidence.

- **Unauthorized Access:** Unauthorized access to NEFT and RTGS systems is a critical security risk. [As discussed previously] This can occur through various means, including:
    - **Compromised Credentials:** Invalid login credentials can be accessed by attackers via phishing, malware attacks, or social engineering. This enables them to masquerade as legitimate users and access the system.
    - **Insider Threats:** Authorized employees may misuse their access privileges to conduct fake transactions or pilfer confidential data. They might be driven by monetary rewards or other malicious motivations.
    - **Access Control Mechanism Vulnerabilities:** Flaws in authentication or authorization mechanisms can be used by attackers to bypass security controls and obtain unauthorized access. This underlines the need for strong access control systems.
    -
- The consequences of unauthorized access can be severe, including:
    - **Fraudulent Transactions:** Attackers may commandeer unauthorized fund transfers, causing immediate financial losses for the bank and customers.
    - **Data Breaches:** Illegal access can allow attackers to steal confidential data, including customer account information and transaction history.

    - **System Disruption:** Attackers are able to disrupt the functioning of NEFT and RTGS systems, leading to delays in transferring funds and affecting the overall payment system.

- Mitigating unauthorized access requires a multi-layered approach, including:

    - **Strong Authentication:** Including the use of strong authentication techniques, like multi-factor authentication, to confirm the users' identities.
    - **Access Control:** Implementing stringent access control rules adhering to the least privilege principle.
    - **Intrusion Detection**: Installing intrusion detection systems to scan system activity and alert on suspect behavior.
    - **Regular Security Audits:** Performing regular security audits to detect and resolve vulnerabilities in access control mechanisms.

- **Data Breaches:** Data breaches are yet another major security threat in NEFT and RTGS systems. [As was already discussed] These systems deal with a great amount of sensitive information, including:
- Customer account details
- Transaction sizes
- Beneficiary information
- Bank routing details
- A data breach can occur due to various factors, such as:

    - **Cyberattacks:** Hackers can exploit malware or hacking methods to penetrate systems and harvest information.
    - **Insider Threats:** Sensitive information can be inadvertently or deliberately shared by employees.
    - **System Vulnerabilities:** Flaws in hardware or software may be used by intruders to access information.
- The consequences of a data breach can be severe:

    - **Financial Losses:** Both customers and banks can incur financial losses because of fraud and identity theft.
    - **Reputational Harm:** Data breaches can harm the reputation of a bank and destroy customer trust.
    - **Legal Liabilities:** Banks can be legally penalized for not keeping customer information secure.

- Protecting data requires a comprehensive strategy:

  - **Encryption:** Encrypting data in transit and at rest to avoid unauthorized access.
  - **Access Control:** Limited access to information based on the least privilege principle.
  - **Data Loss Prevention (DLP):** Installing DLP solutions to ensure sensitive data does not escape the organization's control.
  - **Regular Security Assessments:** Conducting regular assessments to identify and address vulnerabilities in data security practices.
  -
- **Malware Attacks:** Malware attacks pose a significant threat to NEFT and RTGS systems. Malware can infect systems through various means, including:

  - **Email Attachments:** Malware attachments in email can install when opened.
  - **Downloaded Files:** Malware infection can result from downloading infected files from the internet.
  - **Software Vulnerabilities:** Software vulnerabilities can be targeted by malware to gain entry into systems.

The impact of malware attacks can be severe:

- **System Disruption:** Malware can interfere with the functioning of NEFT and RTGS systems, leading to fund transfer delays.
- **Data Corruption:** Malware has the potential to delete or corrupt data, causing business losses and operational issues.
- **Fraudulent Transactions:** Malware can be employed to enable fraudulent transactions by altering transaction information.
- Protecting against malware requires a multi-layered approach:

  Anti-Malware Software: Having installed and running up-to-date anti-malware software on all systems.
  Firewalls: Utilizing firewalls to prevent unauthorized access to systems.
  Intrusion Prevention Systems (IPS): The use of IPS to identify and block malicious network traffic.
  Periodic Security Patches: Installing security patches on operating systems and software to fix weaknesses.
  Employee Training: Educating employees on the dangers of malware and avoiding infection.

Phishing and Social Engineering: Phishing and social engineering attacks are designed to deceive individuals into revealing sensitive information or performing actions that compromise security. [As discussed previously] These attacks often target:

- **Bank Employees:** Attackers may impersonate colleagues or supervisors to trick employees into providing credentials or initiating fraudulent transactions.

- **Customers:**Attackers can send false emails or text messages that seem to be from the bank, requesting customers to give their login credentials.
-

The consequences of successful phishing and social engineering attacks can be:

- **Unauthorized Access:** The attackers can gain unauthorized access to NEFT and RTGS systems through stolen credentials.

- **Fraudulent Transactions:** The attackers can make fraudulent fund transfers.
- **Data Breaches:** The attackers can steal sensitive data.

Prevention of these risks involves:

- **Employee Training:** Educating employees on the methods used in phishing and social engineering attacks and how to detect them.
- **Awareness Campaigns:** Organizing regular awareness campaigns to promote security best practices.
- **Technical Controls:** Putting technical controls, including email filtering and website authentication, in place to identify and block phishing attempts.
- **API Vulnerabilities:** Application Programming Interfaces (APIs) are employed to enable communication between disparate systems within the NEFT and RTGS infrastructure. [As already discussed] Flaws in these APIs can be taken advantage of by attackers to:
- **Gain Unauthorized Access:** Attackers could circumvent authentication controls and access sensitive data or functionality.
- **Manipulate Transactions:** Malicious actors might alter transaction information or create phony transactions.
- **Launch Denial-of-Service Attacks:** Attackers can clog APIs with traffic, bringing down systems.

Securing APIs involves:

- **Secure API Design:** Secure coding practice and authentication and authorization controls.
- **API Testing:** Performing frequent security testing to locate and fix weaknesses.
- **API Monitoring:** Tracking API traffic for odd behavior.
- **Internal Fraud:** Internal fraud is a serious issue in any financial institution, including ones running NEFT and RTGS systems.

Authorized staff can conduct fraudulent acts such as:

- Embezzlement: Theft of money from the bank.
- Fraudulent Transactions: Conducting unauthorized fund transfers for personal benefits.
- **Data Manipulation:** Changing transaction records to hide fraudulent transactions.

Prevention of internal fraud involves:

- **Segregation of Duties:** Allocation of duties to employees to ensure that no single person has excessive control.
- **Background Checks:** Running detailed background checks on employees.
- **Forced Vacations:** Forcing employees to go on forced vacations to identify any fraud that might be taking place when they are not around.
- **Periodic Audits:** Performing periodic audits to identify any internal fraud indicators.
- **Whistleblower Systems:** Providing systems for the employees to report suspicious behavior without fear of persecution.

5.3.2 Operational Risks

Operational risks in NEFT and RTGS systems are the ones that happen due to mistakes or breakdowns in internal processes, systems, or human nature. These risks can interrupt operations, result in financial losses, and harm the reputation of the bank.

- **System Failures:** System failure may happen for a number of reasons, including:

- **Hardware Failures:** Malfunctioning of servers, network devices, or other hardware parts.

    - **Software Errors:** Glitches or bugs in the software employed to run NEFT and RTGS systems.
    - **Network Outages:** Communication network breakdowns that hinder the transmission of transaction information.
    - **Power Outages:** Electrical power supply disruptions to systems.
    - **Natural Disasters:** Natural occurrences like earthquakes, floods, or fires that destroy infrastructure.

The effects of system failures can be:

    - **Transaction Delays:** Delay in processing and settling transactions.
    - **System Downtime:** Failure to access or utilize NEFT and RTGS systems.
    - **Financial Losses:** Financial losses due to non-executed transactions or an inability to execute business.
    - **Reputational Damage:** Reputation loss of the bank as a reliable organization.

To counter system failure, one needs:

    - **Redundancy:** Siting redundant systems and components in place to have the capability of maintaining operations if a failure happens.
    - **Failover Mechanisms:** Siting protocols for automatic switch over to the back-up systems on failure.
    - **Disaster Recovery Plans:** Creating full plans to restore systems and data in the face of catastrophic loss.
    - **Regular Maintenance:** Carrying out periodic maintenance on systems in order to prevent breakdown.
    - **Capacity Planning:** Insuring systems are adequately equipped with capacity to maintain transactional loads.

Operational risks under NEFT and RTGS are those which happen due to blunders or default in internal functions, systems, or human factors. These would cause interruption of operations, give rise to economic losses, as well as put the reputation of the bank into jeopardy.

- **System Failures:** System failures happen due to the following reasons:
- **Hardware Failures:** Hardware defects in servers, network devices, or other pieces of hardware.
- **Software Glitches:** Errors or bugs in the software used to run NEFT and RTGS systems.

- **Communication Network Breakdowns:** Network breakdowns disrupting communication networks which hinder the exchange of transactional data.
- **Electricity Blackouts:** Electrical power supply failures in systems.
- Natural Disasters like earthquakes, flooding, or burning down buildings destroy infrastructure.

Effects of system downtime can be:

- **Transaction Lagging:** Delaying processing and settlement of transactions.
- **System Failure:** Inaccessibility or usability of NEFT and RTGS systems.
- **Financial Losses:** Losses associated with failed transactions or inability to do business.
- **Reputational Damage:** Losses to the bank's reputation for dependability.

Mitigating system failures involves:

- **Redundancy:** Creating redundant systems and components so that operations can be continued in the event of a failure.
- **Failover Mechanisms**: Defining procedures to automatically switch to backup systems in the event of a failure.
- **Disaster Recovery Plans:** Creating detailed plans for system and data recovery in the case of a significant disruption.
- **Regular Maintenance:** Conducting regular maintenance on systems to avoid failures.
- **Capacity Planning:** Making sure systems have enough capacity to process transaction volumes.
- **Processing Errors:** Processing errors may result from:
- **Data Entry Mistakes:** Mistakes made during the entry of transaction data.
- **Software Bugs:** Software defects used to process transactions.
- **Miscommunication:** Miscommunication between various systems or departments.
- **Lack of Training:** Lack of proper training of employees on NEFT and RTGS processes.

The effects of processing errors can be:

- **Incorrect Transactions:** Transferring funds to the wrong account or in the wrong quantity.
- **Financial Losses:** Loss of money due to incorrect transactions or rectification of errors.
- **Customer Dissatisfaction:** Discontent due to delays or mistakes in fund transfers.

Preventing processing errors involves:

- **Data Validation:** Putting controls in place to ensure the validity of transaction information.
- **Automated Processing:** Processing in an automated manner to minimize the opportunity for human error.
- **Reconciliation:** Frequent reconciliation of transaction records in order to detect and remove errors.
- **Staff Training:** Giving thorough training to staff in regard to NEFT and RTGS procedures.
- **Clear Procedures:** Having clear and well-documented procedures for processing transactions.
- **Settlement Risk:** Settlement risk exists as a likelihood that a settlement in a funds transfer system doesn't occur when it is due to happen. [As is the case already discussed] Settlement risk is, however, heightened in systems basing their settlements on a net settlement deferred basis, like that of NEFT. In the case of RTGS, it is reduced through real-time gross settlement.
- **Liquidity Risk:** Liquidity risk is the risk that a bank is unable to meet its payment obligations when they fall due. [As discussed previously] This can arise in NEFT and RTGS if a bank experiences unexpected outflows of funds or is unable to obtain sufficient funds to settle its transactions.

- **Legal and Regulatory Risk:** Legal and regulatory risk is the risk of non-compliance with laws and regulations governing NEFT and RTGS operations.These may comprise:
- Anti-Money Laundering (AML) rules
- Know Your Customer (KYC) rules
- Data privacy rules
- Regulations of payment systems

Non-compliance may lead to:

- Financial penalties
- Sanctions by law
- Damage to reputation
- **Managing legal and regulatory risk involves:** Keeping abreast of relevant legislation and rules.Having compliance programs in place. Carrying out regular audits to confirm compliance.

Chapter 6

EFRM (Electronic Funds Risk Management)

6.1 Introduction to EFRM

Electronic Funds Risk Management (EFRM) is a pillar of operational resilience and security in today's banking system. The digital payment channels of mobile banking, internet banking, and payment gateways have changed the way financial transactions are done. This digital revolution, as much as it has brought with it unprecedented convenience and efficiency, has also created a sophisticated and dynamic environment of risks that need to be scrupulously managed by banks. EFRM embraces an integrated, comprehensive, and flexible framework comprising policies, procedures, technological controls, and surveillance measures to ensure the security of electronic fund transfer systems, defense against sensitive financial information, and perpetuation of the confidence and trust of stakeholders and customers. The success of a bank's EFRM system is not just an operational requirement but a key driver of its long-term stability, regulatory compliance, and reputation in an increasingly globalized and digitally enabled financial environment.

6.1.1 Overview of EFRM

In essence, EFRM is an ongoing and iterative process that revolves around actively managing the risks involved in the electronic transfer of funds. It entails a formal method that starts with an all-inclusive enumeration of all risks that may affect electronic fund transfer operations. Risks may have various sources and may be represented by advanced cyber threats, internal weaknesses, human mistakes, as well as outer dependencies. After risk identification, a thorough analysis is carried out to assess the potential effect of each identified risk on the financial well-being, continuity of operations, legal position, and reputation of the bank, as well as the probability of its occurrence. This assessment process is essential for risk mitigation effort prioritization and resource allocation.

Depending on the result of the risk assessment, an arsenal of suitable mitigation measures and controls are developed and put in place. These controls can range from broad, including technical measures like stringent encryption protocols, multi-factor authentication systems, and sophisticated intrusion detection systems; operational practices like segregation of duties, transaction cutoffs, and reconciliation procedures; and physical security measures to safeguard essential infrastructure. The activation of these controls is not a one-time occurrence but an ever-present process that must be continually refined and adapted to counter changing threats and technology.

6.1.2 EFRM Architecture (Conceptual)

EFRM's conceptual design offers a systematic method of comprehending the different elements and the interrelationship among them in an overall electronic funds risk management system. Though not a physical plan, it may be envisioned as a set of interconnected levels, each adding to the general robustness and efficiency of EFRM:

- **Governance and Policy:** This is the base layer that sets the overall framework for EFRM. It defines the strategic objectives for managing electronic fund transfer risks, articulates the bank's risk appetite in this domain, clearly delineates roles and responsibilities across different organizational units, and sets forth the comprehensive policies, standards, and procedures that govern all electronic fund transfer activities. Sound governance ensures that EFRM is integrated into the bank's overall risk management culture and strategic objectives, and that responsibility for managing these risks is clearly allocated.

- **Control Framework:** This level consists of the precise controls that are developed and put in place to counteract the risks uncovered in the risk assessment process. These controls are the operational core of EFRM and can be generally divided into:

- **Technical Controls:** These are used through technology for prevention or detection of unauthorized access, data exposure, or fictitious transactions. Some examples are encryption algorithms used for maintaining the confidentiality of the data, firewall systems for limiting network traffic, intrusion detection and prevention systems to detect and exclude malicious activity, and multi-factor authentication to ensure the identity of users.

- **Operational Controls:** These are measures based on processes that aim to minimize the likelihood of error, fraud, and other failure in operations. Segregation of duties to preclude any individual from having inordinate control is an example, as is requiring dual authorization of high-value transactions, limiting transactions to limit the amount of funds transferred, and routine reconciliation procedures to ensure accuracy of transaction records.

- **Physical Controls:** These include physical steps taken to secure the physical infrastructure underlying electronic fund transfer systems, like safe data centers with controlled access, environmental protection, and redundant power facilities.

- **Monitoring and Detection:** This critical layer is designed to continuously monitor electronic fund transfer systems, networks, and transactions for the purpose of detecting anomalies, suspicious patterns, and possible security incidents in real-time or near real-time. Successful monitoring takes advantage of different technologies and methods, such as Security Information and Event Management (SIEM) systems that consolidate and examine security logs from different sources, real-time transaction monitoring systems that scan transaction data for signs of fraud or money laundering, and anomaly detection tools that pick up on deviations from normal user or system behavior.

- **Incident Response and Recovery:** This level identifies the pre-arranged incident response procedures and plans for the effective response and recovery from security breaches or operations disruptions affecting electronic fund transfers. An incident response plan with defined steps involves steps for detecting the incident, containing to restrict the damage scope, eradicating the threat, recovering damaged systems and data, and post-incident analysis of lessons learned for future prevention enhancements. Business continuity planning and disaster recovery plans are also key elements of this layer, which guarantees the robustness and prompt recovery of electronic fund transfer operations in the case of a major disruption.

- **Audit and Compliance:** This last layer offers third-party assurance of the efficacy of the EFRM framework and ensures continuous compliance with applicable legislation, regulation, and internal policies. Internal and external audits are performed regularly to evaluate the adequacy and effectiveness of EFRM controls, detect weaknesses or gaps, and suggest improvement. Monitoring of compliance ensures adherence to legal and regulatory requirements associated with electronic fund transfers, such as anti-money laundering rules, data privacy acts, and payment system standards.

- This extended introduction and overview sets out a clearer picture of the significance, reach, and conceptual structure of Electronic Funds Risk Management within banking, setting the stage for the following sections describing unique risks, mitigation methods, and monitoring procedures.

6.2 EFRM Processes and Security

EFRM relies on a combination of well-defined processes and robust security measures.

6.2.1 Typical EFRM Processes

- **Risk Assessment:** This is the process of identifying and analyzing possible risks related to electronic fund transfers. It involves assessing the probability and possible effect of different risk scenarios.
- **Control Design and Implementation:** On the basis of the risk assessment, proper controls are designed and put into place to reduce identified risks.
- **Transaction Monitoring:** It encompasses real-time or near real-time monitoring of electronic fund transfers to identify suspicious behavior, including fraud or money laundering.
- **Fraud Management:** It covers prevention, detection, and handling of fraudulent transactions against electronic fund transfers.
- **Security Incident Management:** It encompasses response processes for security incidents, including data breach or cyberattacks, including containment, eradication, and recovery.
- **Change Management:** This function assures that electronic fund transfer processes and systems changes are executed securely and in a controlled environment.
- **Vendor Risk Management:** This includes evaluation and control of the risk tied up with third-party vendors of electronic fund transfer services.
- Data protection is integral to EFRM.
- **Encryption:** This refers to encoding data so that they cannot be accessed without permission at the time of transmission and storage.
- **Access Controls:** These controls limit access to electronic fund transfer systems and information to authorized individuals only.
- **Authentication and Authorization:** Authentication confirms the identity of users, and authorization regulates what they can do.
- **Data Loss Prevention (DLP):** DLP software prevents sensitive information from exiting the organization's control.
- **Secure Storage:** This entails putting in place controls to secure stored data from unauthorized accessing, modification, or destruction.
- **Data Masking and Tokenization:** Both of these methods secure sensitive information by substituting it with masked or tokenized values.

6.3 EFRM-Related Risks

EFRM addresses a wide array of risks that can disrupt or compromise electronic fund transfers.

6.3.1 Security Risks in EFRM

- Risk Assessment: This entails the identification and analysis of possible risks related to electronic fund transfers. It comprises the analysis of the likelihood and possible effect of different risk situations.

- Control Design and Implementation: Appropriate controls are designed and implemented based on the risk assessment to curb identified risks.

- Transaction Monitoring: This is monitoring electronic fund transfers in near real-time or real-time to identify suspicious activity, including fraud or money laundering.

- Fraud Management: This function is concerned with preventing, detecting, and responding to fraudulent behavior involving electronic fund transfers.
- Security Incident Management: This entails procedures for managing security incidents, including data breaches or cyberattacks, such as containment, eradication, and recovery.
- Change Management: This procedure makes sure that changes to electronic fund transfer systems or processes are carried out in a secure and controlled environment.
- Vendor Risk Management: This is evaluating and managing risks linked to third-party vendors participating in electronic fund transfer services.
-

6.2.2 Data Security in EFRM

- Data protection is the core of EFRM.
- **Encryption:** This is encrypting data to keep it away from unauthorized use when being sent and stored
- These threats endanger the confidentiality, integrity, and availability of EFRM systems and information.
- **Cyberattacks:** These are numerous malicious acts, including hacking, malware infection, and denial-of-service attacks.
- **Data Breaches:** Unauthorized access to and release of sensitive information, including customer account data.
- **Insider Threats:** Risks presented by employees or other insiders who might misuse their access rights.
- **Fraud:** This includes different kinds of fraudulent behavior, including unauthorized transactions, account takeover, and payment fraud.

- **Mobile and Online Banking Risks:** Risks related to electronic fund transfers carried out through mobile and online banking channels, including phishing and account takeover.
- **API Security Risks:** APIs for electronic fund transfers can be attacked by hackers.

6.3.2 Operational Risks in EFRM

- These threats are due to breakdowns in internal processes, systems, or human mistakes.
- System Disruptions: Disruptions in the availability or performance of electronic fund transfer systems.
- Processing Errors: Errors or mistakes in processing electronic fund transfers, resulting in incorrect transactions.
- Capacity Issues: Failure of systems to process the volume of electronic fund transfers.
- Model Risk: Risks that occur due to the application of incorrect or unsuitable models for risk measurement or decision-making.
- Third-Party Risk: Risks related to dependence on third-party providers of electronic fund transfer services.

6.3.3 Compliance Risks in EFRM

- These risks entail breaches of laws, regulations, or internal guidelines.
- Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) Regulations: Failure to comply with regulations to prevent money laundering and terrorist financing.
- Data Privacy Regulations: Breaches of regulations for collecting, using, and disclosing customer information.
- Payment Card Industry Data Security Standard (PCI DSS): Failure to comply with security standards for the processing of cardholder data.
- Consumer Protection Regulations: Breaches of regulations meant to safeguard consumers in electronic funds transfers.
- 6.4 EFRM Risk Mitigation and Monitoring
- Mitigation and monitoring of risks are critical to a successful EFRM framework.

6.4.1 Security Measures in EFRM

These are intended to safeguard electronic fund transfer systems against security risks.

- ○ Firewalls and Intrusion Detection/Prevention Systems: These technologies shield networks and systems from unauthorized access and malicious behavior.
- ○ Firewalls serve as a shield, regulating network traffic according to predetermined rules, blocking unauthorized attempts, and preventing potentially malicious traffic from entering or exiting the bank's network.
- ○ Intrusion Detection Systems (IDS) observe network or system activity to detect malicious action or policy breaches.
- ○ Intrusion Prevention Systems (IPS) take things a step further by actively intercepting or forbidding detected intrusion.
- ○ Anti-Malware Solutions: Products that detect and prevent malware infestation.
- ○ Anti-malware products, such as antivirus software, are essential for safeguarding electronic fund transfer systems against diverse forms of malicious software, including viruses, worms, Trojans, and ransomware that can threaten system integrity and data confidentiality.
- ○ Vulnerability Management: Procedures for discovering, evaluating, and remediating system and application security vulnerabilities.
- ○ Vulnerability management entails frequent scanning of systems and applications for known vulnerabilities, prioritizing vulnerabilities on the basis of their risk, and applying patches or other remedies to correct them before they can be used by attackers.
- ○ Security Awareness Training: Training employees regarding security threats and best practices.
- ○ Security awareness training is critical to inform employees of the possible security threats, including phishing, social engineering, and insider threats, and to encourage security best practices, including good password management, secure browsing, and detection of suspicious activity.

- **Multi-Factor Authentication:** Forcing users to present several verification methods in order to access systems.Multi-factor authentication (MFA) introduces an additional level of security by compelling users to present two or more verification methods, for example, something they know (password), something they possess (single-use code from a mobile application), or something they are (biometric verification), which greatly minimizes the possibility of unauthorized access even in the event one factor is compromised.

- Data Encryption: Encrypting data to keep it out of unauthorized hands.
- Encryption is an essential security control where data is encoded so that only with a decryption key can it be made readable, safeguarding sensitive data while it is being transmitted and stored.
- Keeping an eye on things all the time is important to catch and react to potential threats.
- Security Information and Event Management (SIEM) Systems: SIEM systems gather and parse security logs and events to identify suspicious behavior.
- SIEM systems consolidate security logs and events from many sources throughout the IT infrastructure, offering a single platform for real-time monitoring, analysis, and alerting on possible security threats and anomalies.
- Log Analysis: Monitoring system and application logs to detect anomalies or security incidents.
- Log analysis entails the methodical examination of system and application logs to detect patterns, anomalies, or suspicious activity that can signify security incidents, system failures, or performance issues.
- Performance Monitoring: Tracking the performance of electronic fund transfer systems to identify any degradation or disruption.
- Performance monitoring entails monitoring the key performance indicators (KPIs) of electronic fund transfer systems, including transaction processing time, system availability, and error rates, to identify any performance degradation or potential disruption that might affect service delivery.
- Fraud Monitoring Systems: Systems that process transactions to identify and prevent fraudulent transactions.

Fraud monitoring systems implement different methods, including rule-based systems, machine learning models, and behavioral analysis, to screen electronic fund transfer transactions in real-time and flag potentially fraudulent behavior, like unauthorized transactions, takeover of accounts, and money laundering.

- Regular Security Audits: Third-party examinations of the EFRM model to guarantee that it is performing effectively.
- Periodic security audits, either by internal or external auditors, offer an impartial evaluation of the EFRM structure's design and functioning, detecting any vulnerabilities, loopholes, or shortcomings in security controls and procedures.
- Transaction Monitoring
- Transaction monitoring is an important part of tracking electronic fund transfers.
- For instance, in UPI transactions, transaction monitoring tools and special queries are employed to verify anomalies like hung transactions or errors.

- This is monitored at regular time intervals, and possible abnormalities are specified to raise alerts or further examination.

Connect24 Monitoring

Connect24, being a part involved in processing transactions, also needs monitoring.

- Certain logs and error codes are monitored to detect problems such as invalid account numbers, delays in processing, or system failures.

- Fraud Management: This process aims at preventing, detecting and responding to fraud against electronic fund transfers.
- Security Incident Management: It encompasses steps to manage security incidents, for example, data breaches or cyber attacks, such as containment, eradication and recovery.
- Change Management: This process ensures that any change to electronic fund transfer systems or processes is made under controlled and secure conditions.
- Vendor Risk Management: This involves assessing and managing the risks associated with third-party vendors involved in electronic fund transfer services.

6.2.2 Data Security in EFRM

- Protecting data is fundamental to EFRM.
- Encryption: This involves encoding data to prevent unauthorized access during transmission and storage.
- These risks threaten the confidentiality, integrity, and availability of EFRM systems and data.
- Cyberattacks: These cover a range of malicious activities, including hacking, malware infection, and denial-of-service attacks.
- Data Breaches: Illicit access to and revelation of confidential information, including customer account details.
- Insider Threats: Dangers created by employees or other insiders who might misuse their access rights.
- Fraud: This covers a range of fraudulent activities, including unauthorized transactions, account takeovers, and payment fraud.

- Mobile and Online Banking Risks: Risks related to electronic fund transfers made through online and mobile banking platforms, including account takeovers and phishing.

- API Security Risks: Attackers could exploit weaknesses in APIs utilized for electronic fund transfers.

6.3.2 Operational Risks in EFRM

- These are risks that result from breakdowns in the company's internal processes, system failure, or human mistake.
- System Disruptions: Disruptions to the performance or availability of electronic fund transfer systems.
- Processing Errors: Errors or mistakes in the processing of electronic fund transfers resulting in improper transactions.
- Capacity Problems: Inability of systems to process the volume of electronic fund transfers.
- Model Risk: Risks that are due to the application of erroneous or inappropriate models for decision-making or risk measurement.
- Third-Party Risk: Risks in dependence upon third-party vendors to provide electronic fund transfer services.

6.3.3 EFRM Compliance Risks

These risks are related to non-adherence to laws, regulations, or internal policies.

- Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) Regulations: Failure to comply with regulations to prevent money laundering and terrorist financing.
- Data Privacy Regulations: Non-compliance with regulations relating to collecting, using, and disclosing customer information.
- Payment Card Industry Data Security Standard (PCI DSS): Failure to meet security standards for processing cardholder data.
- Consumer Protection Regulations: Breaches of regulations aimed at safeguarding consumers in electronic fund transfers.

6.4 EFRM Risk Mitigation and Monitoring

Mitigation and monitoring of risks are critical to an effective EFRM framework.

6.4.1 Security Measures in EFRM

- These measures aim to safeguard electronic fund transfer systems against security threats.
- Firewalls and Intrusion Detection/Prevention Systems: These technologies secure networks and systems against unauthorized access and malicious activity.
- Firewalls serve as a barrier, regulating network traffic in accordance with established rules, preventing unauthorized attempts to access, and blocking potentially malicious traffic from entering or exiting the bank's network.
- Intrusion Detection Systems (IDS) observe network traffic or system activity for malicious behavior or policy breach.
- Intrusion Prevention Systems (IPS) take it one step ahead by actively blocking or preventing identified intrusions.
- Anti-Malware Solutions: Software that detects and prevents malware infections.
- Anti-malware solutions, such as antivirus software, are important to safeguard electronic fund transfer systems against different forms of malicious software, including viruses, worms, Trojans, and ransomware, that can threaten system integrity and data confidentiality.
- Vulnerability Management: Processes for identifying, assessing, and remediating security vulnerabilities in systems and applications.
- Regular scanning of systems and applications for known weaknesses, prioritization of vulnerabilities based on their risk, and implementation of patches or other remediation actions to fix them prior to their exploitation by the attacker are all part of vulnerability management.
- Security Awareness Training: Training employees on security threats and best practices.
- Security awareness training is critical to inform employees about possible security risks, including phishing, social engineering, and insider threats, and to encourage security best practices, including secure password management, secure browsing practices, and identifying suspicious behavior.

REFERENCES

[1] Official SOPs
[2] https://www.wikipedia.org/
[3] Official Training Material
[4] https://www.effor.tech/

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

PLAGIARISM VERIFICATION REPORT

Date: ....

Type of Document (Tick): □ PhD Thesis □ M.Tech/M.Sc. Dissertation □ B.Tech./B.Sc./BBA/Other

Name:______________________________ **Department:**__________________ **Enrolment No** __________

Contact No.________________________________ **E-mail.**_____________________________________

Name of the Supervisor: ____

Title of the Thesis/Dissertation/Project Report/Paper (In Capital letters): ___________________

____

____

UNDERTAKING

I undertake that I am aware of the plagiarism related norms/ regulations, if I found guilty of any plagiarism and copyright violations in the above thesis/report even after award of degree, the University reserves the rights to withdraw/revoke my degree/report. Kindly allow me to avail Plagiarism verification report for the document mentioned above.

- Total No. of Pages =
- Total No. of Preliminary pages =
- Total No. of pages accommodate bibliography/references =

(Signature of Student)

FOR DEPARTMENT USE

We have checked the thesis/report as per norms and found **Similarity Index** at .... (%). Therefore, we are forwarding the complete thesis/report for final plagiarism check. The plagiarism verification report may be handed over to the candidate.

(Signature of Guide/Supervisor) **Signature of HOD**

FOR LRC USE

The above document was scanned for plagiarism check. The outcome of the same is reported below:

Copy Received on	**Excluded**	**Similarity Index (%)**	**Abstract & Chapters Details**	
	• All Preliminary Pages • Bibliography/Images/Quotes • 14 Words String		Word Counts	
			Character Counts	
Report Generated on		**Submission ID**	Page counts	
			File Size	

Checked by
Name & Signature **Librarian**

....

Please send your complete Thesis/Report in (PDF) & DOC (Word File) through your Supervisor/Guide at plagcheck.juit@gmail.com

E-Skin

ORIGINALITY REPORT

11%	6%	9%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Chandrashekhar S. Patil, Sourabh B. Ghode, Jungmin Kim, Girish Kamble et al. "Neuromorphic devices for electronic skin applications", Materials Horizons, 2025 Publication	2%
2	www.ncbi.nlm.nih.gov Internet Source	2%
3	Vineet Kumar, Nargish Parvin, Sang Woo Joo, Tapas Kumar Mandal, Sang Shin Park. "Great Carbon Nano Materials based Composites for Electronic Skin: Intelligent Sensing, and Self-Powered Nano Generators", Nano Energy, 2025 Publication	1%
4	Narjes Pourjafarian, Anusha Withana, Joseph A. Paradiso, Jürgen Steimle. "Multi-Touch Kit", Proceedings of the 32nd Annual ACM Symposium on User Interface Software and Technology - UIST '19, 2019 Publication	1%
5	www2.mdpi.com Internet Source	1%
6	narges-pourjafarian.github.io Internet Source	<1%
7	publikationen.sulb.uni-saarland.de Internet Source	<1%
8	www.slideshare.net Internet Source	<1%
9	Submitted to Canada College Student Paper	<1%

10	www.mdpi.com Internet Source	<1 %
11	Submitted to Nightingale College - School of Nursing Student Paper	<1 %
12	Submitted to City University of Hong Kong Student Paper	<1 %
13	Submitted to University of East London Student Paper	<1 %
14	iopscience.iop.org Internet Source	<1 %
15	Xinyi Ke, Yifan Duan, Yifei Duan, Zhe Zhao et al. "Deep-learning-enhanced metal-organic framework e-skin for health monitoring", Device, 2025 Publication	<1 %
16	cvr.ac.in Internet Source	<1 %
17	mediatum.ub.tum.de Internet Source	<1 %
18	theses.gla.ac.uk Internet Source	<1 %
19	www.researchgate.net Internet Source	<1 %
20	findresearcher.sdu.dk Internet Source	<1 %
21	hdl.handle.net Internet Source	<1 %
22	iris.sissa.it Internet Source	<1 %
23	www.eurekaselect.com Internet Source	<1 %
24	www.hindawi.com Internet Source	

<1%

25	www.pnas.org Internet Source	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		