# Rationalized Input Template (RIT)
# An Internship Report Under ICT Division Bank Asia LTD

by

Swad Bin Ehtesham
Student ID: 15301135

An internship submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

Department of Computer Science and Engineering
Brac University
August 2015

# Declaration

It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

**Student's Full Name & Signature:**

Swad Bin Ehtesham

Student ID: 15301135

# Approval

The thesis/project titled "Rationalized Input Template (RIT) An Internship Report Under ICT Division Bank Asia LTD" submitted by

1. Swad Bin Ehtesham (15301135)

Of Fall, 2024 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on December 03, 2024.

**Examining Committee:**

Supervisor:
(Member)

A.F.M Mazharul Hoque

Assistant Vice President and Head of MIS
ICT Division
Bank Asia LTD

Co-Supervisor:
(Member)

Md. Golam Rabiul Alam, Ph.D.

Professor
Department of Computer Science and Engineering
BRAC University

Program Coordinator:
(Member)

Md. Golam Rabiul Alam, Ph.D.

Professor
Department of Computer Science and Engineering
BRAC University

Head of Department:
(Chair)

Dr. Sadia Hamid Kazi

Associate Professor and Chairperson
Department of Computer Science and Engineering
Brac University

# Ethics Statement (Optional)

This is optional, if you don't have an ethics statement then omit this page

# Abstract

The following report provides a broad understanding of the network infrastructure used in Bank Asia Ltd, particularly focusing on the well-proven applications and systems most essential to the bank's functioning. The infrastructure comprises physical networks such as branches and sub-branches, ATM, internet banking portals, mobile banking application, core banking solutions, and payment systems. All these components perform a significant function of enhancing the delivery of banking services to the customers through effectiveness, security and reliability. This report starts with the explanation of such important points of the network infrastructure, in which key physical and digital elements are described and explained as to how it is possible to build a network system. It stresses the importance of these components and how they are linked to ensure that there is proper Banking Industry Architecture. The bulk of the page is devoted to a list of issues that may exist on the network and their potential solutions. Specific problems, like low-performance servers, server failures, issues with content delivery as well as problems with the software, are discussed. Some of the solutions suggested to address these issues include direct routing in identity management to enhance network congestion, utilizing VNCs for technical support and training for employees as well as load balancing mechanisms to maximize availability and capacity of the servers. Security issues are among the document's strong features as the author does not leave the reader without critical information on different security aspects and measures. However, there are safety methods such as encryption methods, multi-factor authentication, fraud detection system, and network access control (NAC). The relevance of such measures in safeguarding customer information and providing simplicity to the payment process is highlighted. They also discuss disaster recovery procedures in more detail, emphasizing that data backups and restore solutions, infrastructure duplication, geographical dispersion, and business continuity plans are all essential. On the testing and training aspects, it is asserted that these are key factors in implementing a sound disaster recovery plan. This report also explores other evolutions of monitoring which are crucial when it comes to the management, maintenance and security of the network. Some of these areas include VPN tunneling, Traffic analysis, Firewall and intrusion prevention systems, Server and device monitoring and auditing. The focus is made to explain how these monitoring activities can help in management of regulatory issues and improvement of security at the bank. Besides presenting the current state of the network structure in the banking industry, this document presents trends and technological developments that might be relevant to banking networks. The following technological advancements are highlighted; blockchain, artificial intelligence, and quantum computing; with the positives and negatives that can accompany them. In sum, this report is a broad evaluation of the network infrastructure of Bank Asia Ltd. where we discussed its parts and pieces, issues and opportunities, and vision for the future. It is used as a reference to outline the challenges of banking systems as well as the procedures necessitated to ensure that the efficiency, security and reliability of these networks are maintained. In this way, dynamically developing and updating the network infrastructure, the financial institutions can guarantee the consumers safe, effective and innovative banking services considering the internal needs of the consumers and the requirements set by the legislation.

**Keywords:** Data Mining; Machine Learning; Cricket; T20; Prediction; Decision tree; Linear Regression Analysis

# Dedication (Optional)

A dedication is the expression of friendly connection or thanks by the author towards another person. It can occupy one or multiple lines depending on its importance. You can remove this page if you want.

# Acknowledgement

Firstly, all praise to the Great Allah for whom our thesis have been completed without any major interruption.
Secondly, to our co-advisor Teacher Name sir for his kind support and advice in our work. He helped us whenever we needed help.
Thirdly, Name and the whole judging panel of Conference Name. Though our paper not accepted there, all the reviews they gave helped us a lot in our later works.
And finally to our parents without their throughout sup-port it may not be possible. With their kind support and prayer we are now on the verge of our graduation.

# Table of Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction

## 1.1 Overview

Due to the continuous changes in finances/banking and the advances in technology, the architecture of the banking network is the main structure that arranges services in banking. This intricate structure includes many tangible and intangible components that function in cooperation to provide the proper function of banking processes. Some of the infrastructure components central to the firm encompass physical substructures, which despite the advent and growth of online banking are still pertinent in the development of customer relations and confidence. These branches are characteristic facilities, in which clients can perform transactions, work with accounts, and obtain different banking services.
These are backed by other physical sub-branches, the efforts put in the Automated Teller Machines (ATMs) that are also situated at convenient places to enable the client to carry out the key banking activities at any time they feel like such as withdrawals, deposit and checking of account balances. This is supported by the fact that digital platforms have today become crucial in the banking networks that exist in today's world. Internet banking systems and the applications on the customer's mobile devices provide clients with the opportunities to control their money in any place, make transactions and pay utility bills. Such digital solutions help not only to build the client-oriented services list but also improve the banks' internal performance by decreasing the branch influence on their work.
Also, fundamental to the traditional and the emerging players in the industry are core banking systems. These centralized software solutions handle the base aspects of the banking industry such as accounts, transactions, loans, and deposits. Core banking systems guarantee reliable service provision which keeps firms of the banking industry flexible and capable of delivering enhanced solutions in a competitive environment. Another segment of the banking network's downstream infrastructure is the payment networks. These networks help in safe and smooth transfer of money from one bank and financial institutions to another, which include ACH, wire transfer, card payment transfer, etc. These payment networks play an obvious and crucial role in the fluent running of the overlying financial system.

Security measures are paramount in ensuring the customer information and transactions are secure. To mitigate cyber risks and external break-ins various tools like encryption, multi-factor authentication, fraud detection systems, among others are

used. With the new complex threats on the horizon, this is why it is essential for continual development of those security measures, on consumer confidence and adherence to regulatory requirements.

Despite the fact that banking network infrastructure has become well-developed, there can be various problems and question concerning it: low-performance servers, possible errors in content delivery, failures of the servers, problematic actions of the software, etc. Solving these problems implies the usage of proper technical measures and structural practices. For example, in direct routing, it is possible to enhance the capability of the network through achieving faster data transmission among different networking points; VNC can deliver technical support and express training across remote channels. Load balancing deals with the fact that the load to the server is distributed to multiple servers to avoid saturation or congestion and increase the capability and availability of the servers. Business continuity management is critical to the success of banking institutions, especially in the management of disasters that are likely to hinder the efficient running of the business. Data backup and recovery systems and redundant infrastructure and geographical dispersion are the critical elements to address in the disaster recovery plan. Also confirmed, it is tested and trained to avoid compromising the safety of the people and other assets in an emergency. Supervising the functionality and protection of the banking network is a continuous process that implies controlling numerous aspects and elements. Analysis of traffic, firewalls, IPS and antivirus programs will assist in identifying threats in real-time. Compliance audits and performance metrics tracking also confirm and guarantee the network's high availability and compliance with the legislation.

## 1.2 The Reason for having a Conducive Banking Network Infrastructure

Reliability and security of banking network infrastructure regarding infrastructure's construction is crucial in effective and efficient running of financial organizations in the current financial climate. Today having approached the service-oriented strategy and enticed by digitalization, banks face the problem of having increased the importance Anduray of their network infrastructure. The fundamentals of the banking structure are very important, and the following are some of them; customer confidence, internal procedure, growth capacity, protection and adaptability for change.

To begin with, a good and secure banking structure is important to foster the level of confidence amongst the customers. Customers in this business require assurance that their monetary dealings and data are safe and retrievable. This trust is critical for the establishment of a long-term relationship between the company and the customers. Another important factor is operational efficiency, as it limits the number of physical branches and simplifies and economizes the organization's processes. This efficiency enables banks to satisfy their customers' expectations promptly and at the same time money resources better be managed.

One of the key areas in the thirties for success in the modern business environment is scalability and agility. An example of core banking systems includes the digital

platforms, these are essentials for the scaling of the respective banks and in turn enabling the ability of the banks to shift into different operational patterns following changes in the business environment. It thus assists banks to sustain the right positions by delivering diverse services and promptly considering clients' demands. There are also issues of security and compliance to follow, especially while performing the mentioned activities. Effective methods of security shield against the growth in cybersecurity risks and guarantee the confidentiality of the client's information. These security protocols are critical for keeping abreast of the regulations, avoiding legal fines and for sustaining customers' trust. Moreover, there is a potential to incorporate new technologies like block chain, AI's and Quantum computing to modify the banking network infrastructure. These innovations can go a long way in improving operational capacity, enhancing the customer experiences, and consequently enabling banks to remain relevant on the competitions' aggressive frontier. Financial institutions integrate these technologies well due to the strong infrastructure they put in place so as to be ahead in the industry.

Other important requirements are Disaster Recovery and Continuity. Viable and plausible approaches for approaching disaster and its impacts help the banking sector vow continuity in executing their duties. The policy of data backup and recovery, as well as redundant structures and geographical dispersion, are vital for the bank's operations' stability and clients' trust in emergency situations. On a general note, therefore, for the contingent and efficient delivery of banking services, a commendable banking network infrastructure is indeed mandatory. In this way, using physical and digital components, solving typical network problems, enhancing security measures, and forecasting the further development of technology, financial institutions can provide the stability, safety, and effectiveness of their work. This, in turn, enhances the trust and satisfaction of the customers hence making the long-run success and sustainability of the financial institutions.

## 1.3 Objective

### 1.3.1 Understand the Infrastructure

1. **Physical Branches:** These are the physical locations where customers can conduct transactions, open accounts, and access various banking services.

2. **ATMs (Automated Teller Machines):** These machines allow customers to perform basic banking transactions, such as withdrawing cash, depositing funds, and checking balances, without visiting a branch.

3. **Online Banking Platforms:** Digital platforms and websites that enable customers to access their accounts, transfer funds, pay bills, and other banking activities remotely.

4. **Mobile Banking Apps:** Smartphone applications provided by banks that offer similar functionalities to online banking platforms but are optimized for mobile devices.

5. **Core Banking Systems:** These are the centralized software systems that manage the basic banking operations, including customer accounts, transactions, loans, and deposits.

6. **Payment Networks:** Infrastructure that facilitates the transfer of funds between different banks and financial institutions, including Automated Clearing House (ACH) systems, wire transfer networks, and card payment networks like Visa and Mastercard.

7. **Security Protocols:** Measures such as encryption, multi-factor authentication, and fraud detection systems are essential components of banking infrastructure to ensure the security and privacy of customer data and transactions.

Understanding the infrastructure of a banking network involves comprehending how these various components work together to provide banking services to customers efficiently and securely. The Internet is a global network of computers that allows for the exchange of information and communication between users worldwide. It enables access to a vast array of resources, service and entertainment and plays a crucial role in modern society. An Intranet is a sub-computer network controlling infrastructure devices, for example, low –bandwidth sensors /actuator networks. Bangladesh bank monitors all private bank.

## 1.4 Problem identification

1. **Low-Performance Servers:** Low-performance servers receive many requests, while high-performance servers are underutilized.

2. **Content Problem:** Servers and applications are working properly but are responding to requests with "404 Object Not Found".

3. **Server Failure:** A server becomes unavailable due to a hardware failure or an Operating System failure.

4. **Software Failure:** Individual applications stop responding, even though other applications are healthy.

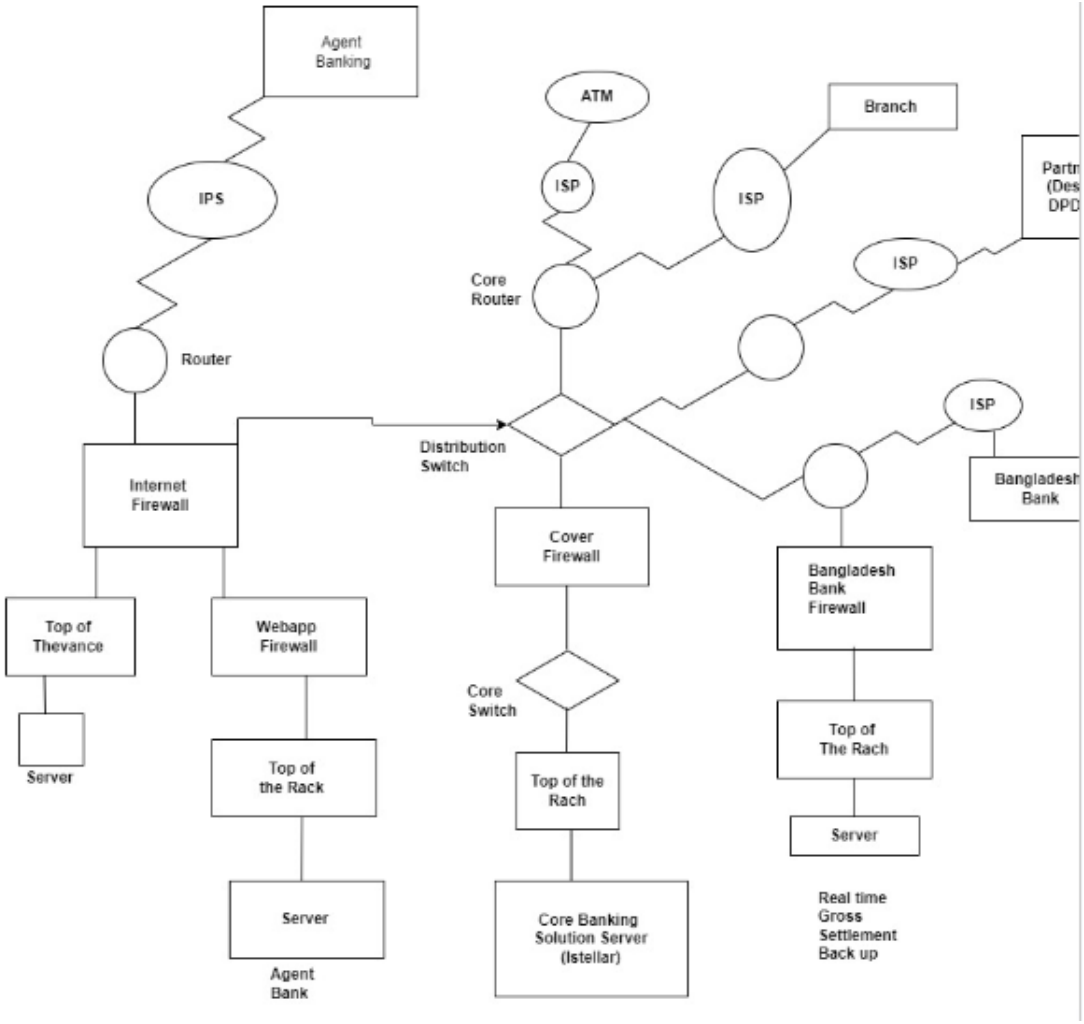


Figure 1.1: Core banking flow diagram 1

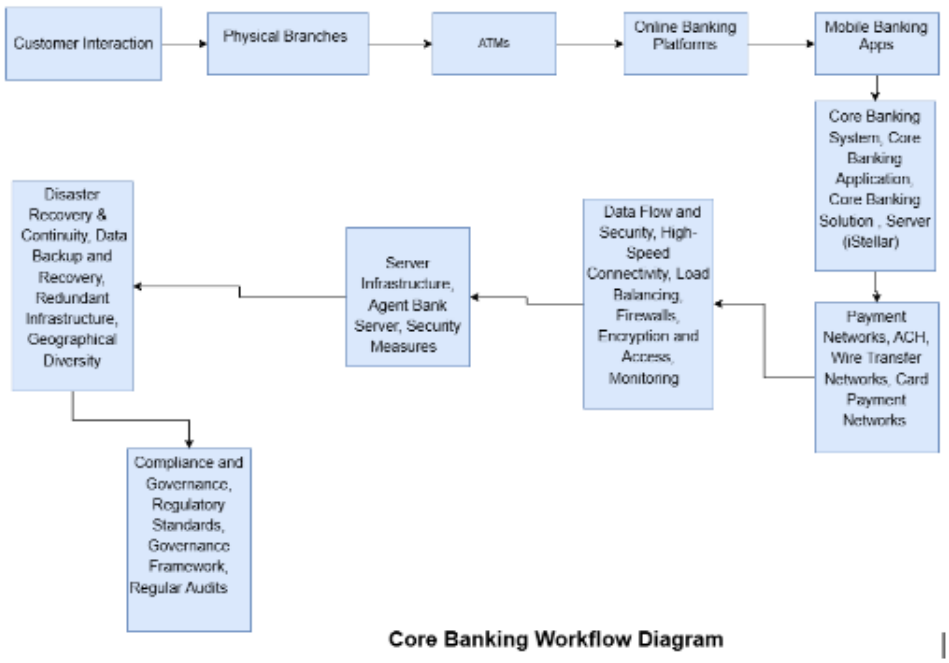


Figure 1.2: Core banking flow diagram 2

# Chapter 2

# Related Work

RIT is a module of MISDB (Management Information System Data Base) of Bank Asia. MISDB is a database management system for Bank Asia with a graphical user interface. The front end of MISDB has is developed using Oracle Apex 4.2.6, back end is developed using oracle database 12 c and it runs on Oracle Linux Server OS. Oracle APEX is a low-code development platform enabling you to build scalable, secure enterprise apps with world-class features that can be deployed anywhere. Using APEX, developers can quickly develop and deploy compelling apps that solve real problems and provide immediate value. You won't need to be an expert in a vast array of technologies to deliver sophisticated solutions. Oracle Autonomous Database and Oracle APEX deliver an unparalleled combination of superior data management and proven low-code application development. Oracle APEX uses a simple architecture that provides zero latency data access, top performance, and scalability, out of the box. Learn more about this architecture, how Oracle APEX uses Oracle REST Data Services, and how the Oracle APEX engine renders pages and has zero-latency access to data.

**Security** Oracle APEX is designed to build web apps that are highly secure out of the box. In a world of constantly changing web standards and increasingly resourceful attackers finding new ways to hack sites, our focus on security means that your applications stay protected.

**Authentication and Authorization** Authentication is the process of identifying who is accessing the application, while Authorization defines whether the user has permission to use an application, or parts of it.

**Authentication Schemes** Oracle APEX comes with a comprehensive set of built-in authentication schemes that make it simple to integrate with Cloud-based authentication providers, your company's LDAP repository or using the local Oracle APEX workspace repository.

**Authorization Schemes** Define access to your application, pages and page components with authorization schemes. Use the built-in Application Access Control to manage users and roles.

**Extensibility** Developers can easily extend Oracle APEX by writing custom authentication and authorization schemes in SQL and PL/SQL.

# Chapter 3

# Work Plan

## 3.1 Quality of Analysis

As any Software Development Life Cycle, the first and the most important step is Analysis. After interviews and online meeting sessions with employess from stake holding departments of RIT, the following primary requirements were identified: 1.Employees will see only the fields and input data into them which are only for their respective departments. 2.After the data has been input, it will be stored into data base for later purposes. The following usecase diagram illustrates thusly:
The Activity Diagram represents how and employee will get into MISDB and then RIT module to input the required data. As security is prime concern of Banks, users will have to login using ID and password. After all the departments are done giving their data ICT division then runs a process of cross checking to verify the data and then generate the .CSV file which is then submitted.

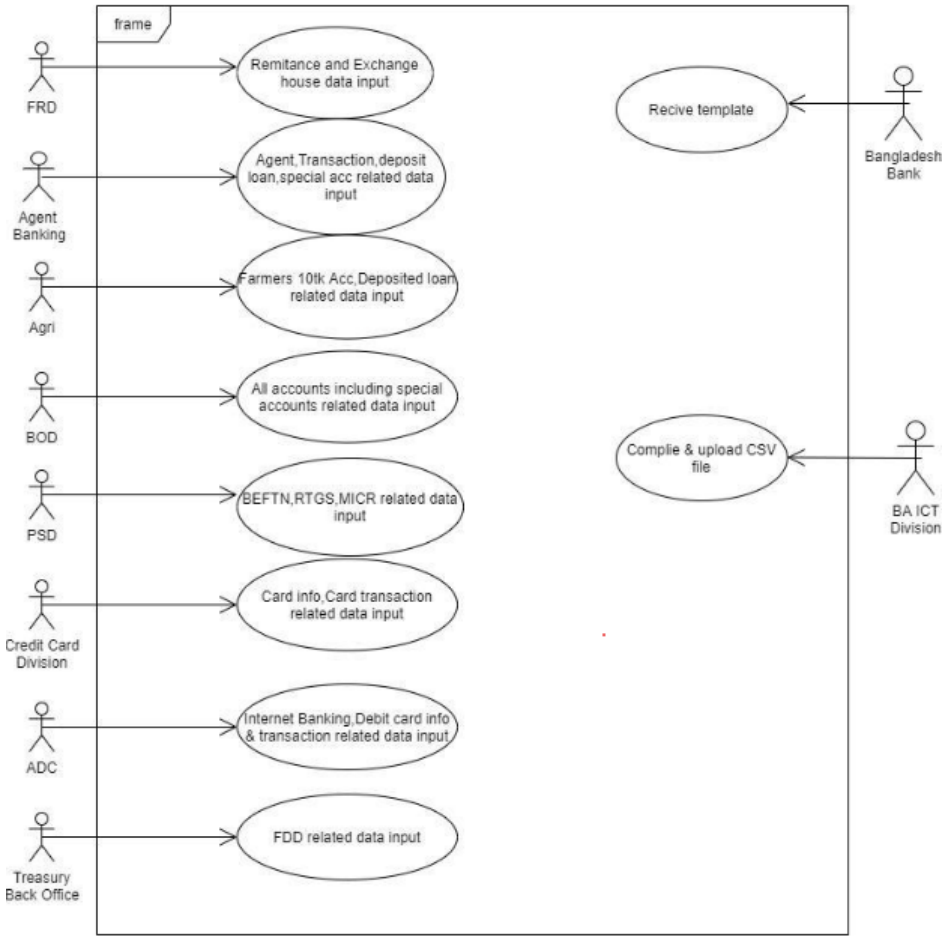


Figure 3.1: Use case Diagram for RIT

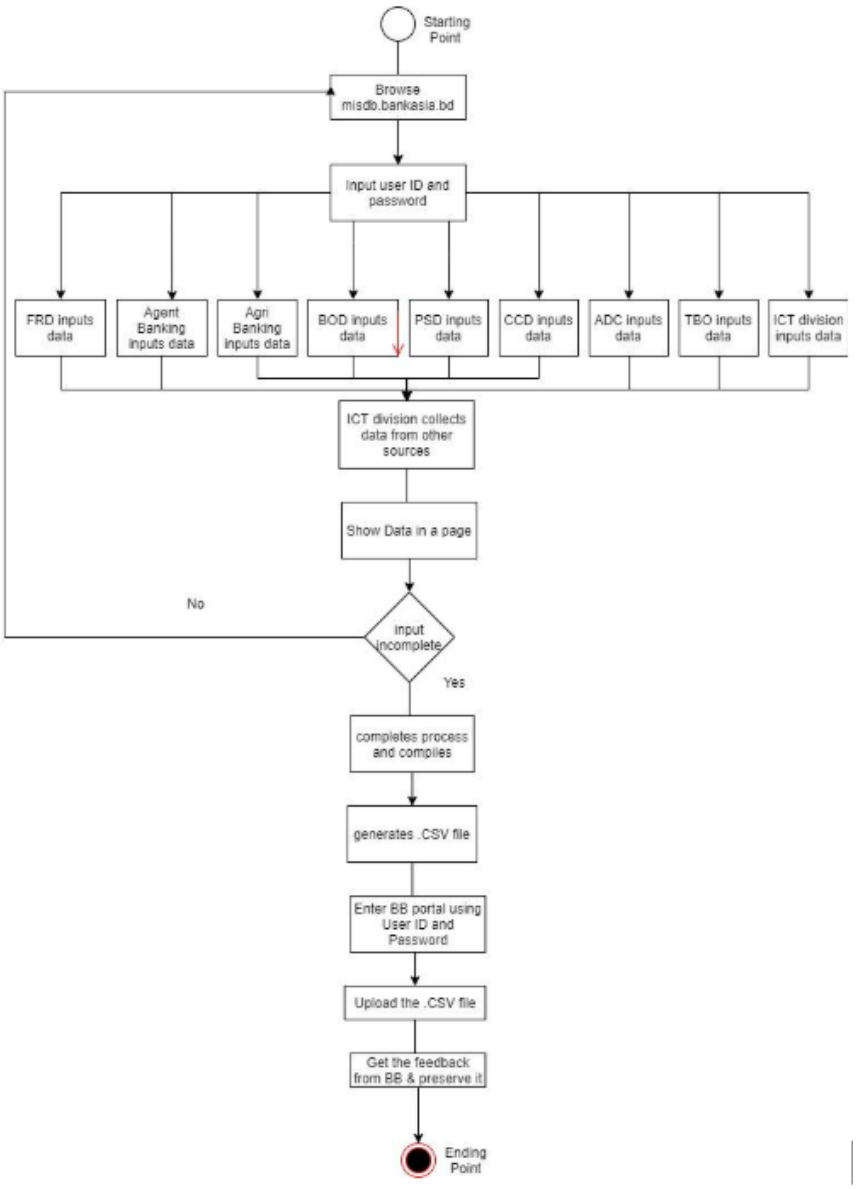


Figure 3.2: Activity Diagram for RIT module in MISDB

# Chapter 4

# Early stages of development

RIT and MISDB both has been developed using iterative model for the SDLC satisfies the work plan and aims to produce the best result in this case. Bank Asia plans to use this module long term as per the requirement of Bangladesh Bank, while having the option to upgrade it and with new features over time. Instead of beginning with well known specifications, as the possibilities are numerous, we enforce a series of software requirements, validate and analyze the result, rinse and repeat. One benefit over the SDLC methodologies: this model gives and early working version in development and makes it less costly to introduce changes.

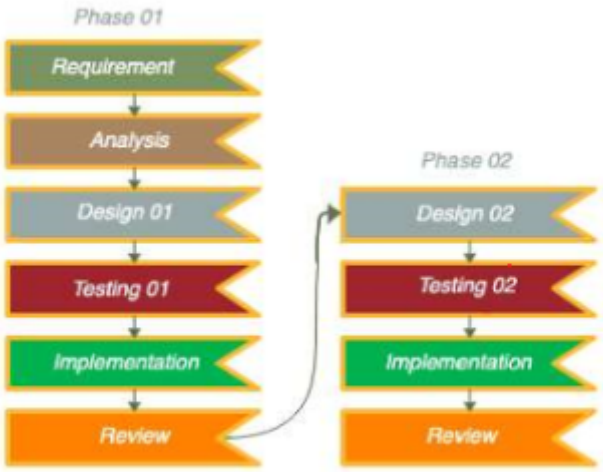


Figure 4.1: Workflow

## 4.1 Phase 1: Adding the RIT module in MISDB

As a part of MISDB RIT module was developed using apex and oracle sql,all the departments can input their data into the fields developed by us ( ICT division ),an employee needs to login into MISDB using user ID and password and employees are designated to their respective departments by HR

## 4.2 Phase 2: Fix identified Issues

We took the employee information from HR table, each employee ID is designated to it's respective department. There are some subdivisions of certain departments and Financial Inclusion Division (FID) is one of them included in Agent Banking. The segregation had to be done Manually from the data base by ICT division to as checker to see who is exactly the maker of the data.

# Chapter 5

# Design

The following ER Diagram has been drafted to aid the modification of database early on in the design stage.
After login, getting into RIT module looks like this. Employess can input and check the data of a certain date. It will only show the data provided in the last month. All the stake holding departments needs to submit their data within the 7th of the month so that we can run the process of checking the data and generate the .CSV file and submit it in the web portal of Bangladesh Bank within 9th of the month.

## 5.1 Solve

### 5.1.1 Know about Direct Routing (DR)

Direct Routing is defined as the routing of the traffic directly from one node to another node without the basic need of any other nodes in between. In the organization of banking networks, the use of a direct route will produce a positive result in the optimization of communication between various members of the banking sector which include branches, ATMs, and other systems. In this manner, while direct routing allows for moving data as quickly as possible from one point to another, through eliminating the extra connections set, the risk of possible failure points is reduced as well.

**Key Benefits of Direct Routing**

- **Improved Network Performance:** Considering that direct routing forecast cuts out intermediary nodes, this means that data must travel a shorter distance and thus communication is fast and with less latency.
- **Enhanced Reliability:** The fewer devices, the fewer networks there are that could fail, thus making it easier to have a stable network.
- **Cost Efficiency:** Direct routing can also minimize the need for extra networking equipment and infrastructure, hence cutting down the expenses.
- **Simplified Troubleshooting:** Since there are relatively fewer components in its structure, it is easier and faster to diagnose and solve the problems within the network.

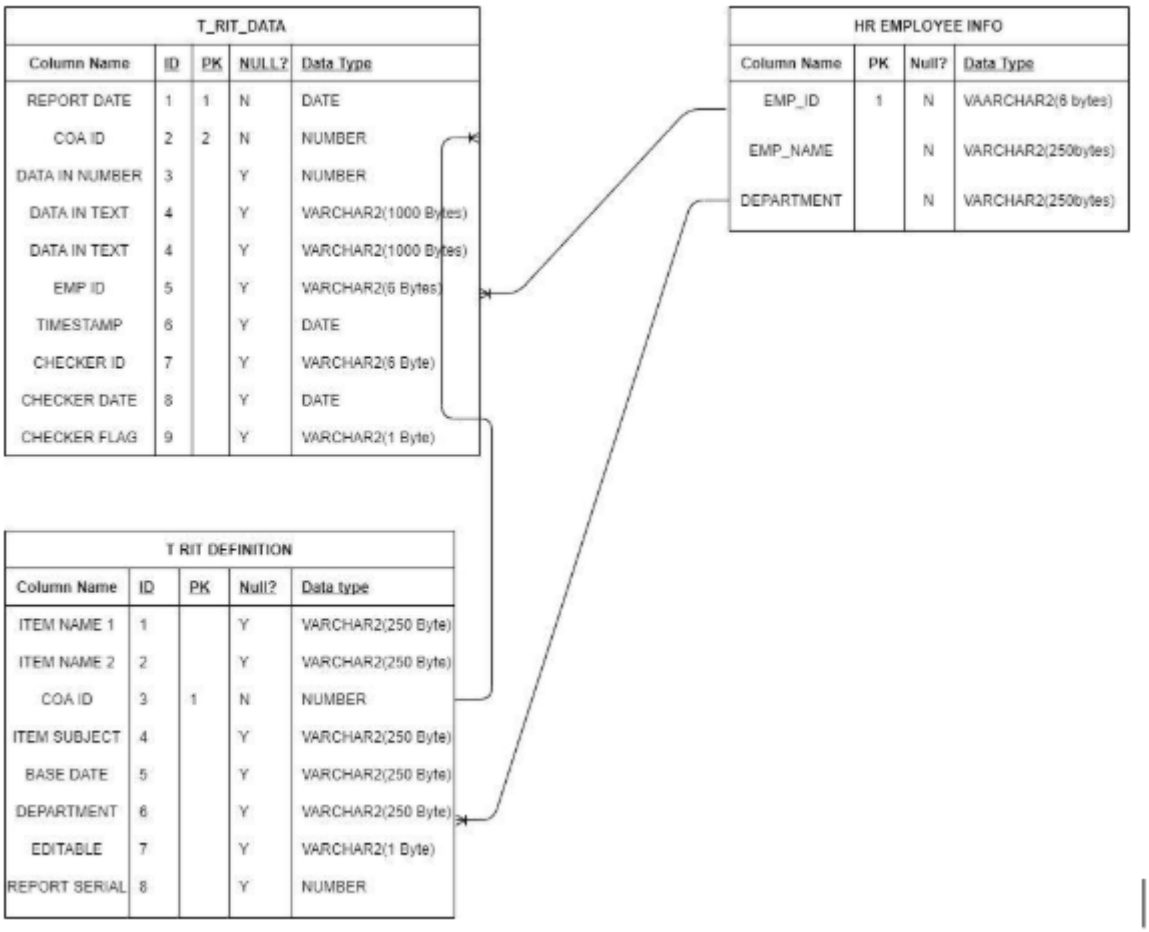


Figure 5.1: ER Diagram

**Implementation in Banking Networks**

- **Branch Connectivity:** The benefits of direct routing in the implementation of connecting the required services would include fast data transfer, low latency, and efficient link between the various branches of the bank.
- **ATM Networks:** Direct routing is another advantage of ATMs as it ensures that the machines maintain the best possible and secure lines of communication with the central banking systems so that the simple transactions can be processed with ease, in the shortest time possible, and with access to real-time updates.
- **Inter-bank Communication:** The direct routing plan enables banks to have a direct and secure communication channel with other financial institutions, thereby improving the interactions and transactions between the institutions.

### 5.1.2 Virtual Network Computing (VNC)

VNC is a method and an acronym for Virtual Network Computing that enables the operation of a computer from a distance with the help of a network connection. Despite the prospects of dangers within the use of VNC in the banking industry due to the insecurity associated with monetary data and structures, it is possible to identify certain cases within which the use of a VNC is valid, given the practice of extremely high levels of security.

**Potential Use Cases for VNC in Banking Networks**

- **Remote Technical Support:** Some of the ways in which banking can apply the VNC include IT assistance where the IT departments can use the application to offer distant technical support in tracking down technical problems with the banking systems, ATMs, other network-located devices among others. The remote access feature allows the IT department to solve problems without physically attending to them, hence saving time.
- **Training and Demonstration:** VNCs can be used in training the bank staff remotely or for easier demonstration of the new software and procedures. This can be especially effective when working in a multinational team or when delivering a training session to remote subordinates.
- **Internet Access:** In a bank environment, VNC can be employed in an intranet IT network to allow privileged users to access other secure parts of the network. This could range from connecting to internal servers, workstations, or virtual desktop infrastructure (VDI) systems.
- **Backup and Recovery:** In disaster recovery situations, VNC may be utilized to gain access to recovery systems or data backup facilities for activating the recovery process. This enables the IT teams to easily repair the equipment and have operations back online without having to be physically present.

**Security Measures**

- **Access Control:** Prohibit unauthorized people from accessing VNC.
- **Monitoring:** Log and monitor all VNC sessions to identify who is accessing the system and prevent unauthorized access.
- **Encryption:** Use secure methods of encoding information when it is being transferred during VNC sessions.
- **Secure Authentication:** Employ identity verification methods to enhance session security.
- **Session Recording:** Record training sessions for proof of implementation and future reference.

### 5.1.3 Server Load Balancing

Implementation of server load balancing is crucial in banking networks due to the demanding need to meet high availability, scalability, and optimal performance. A load balancer divides the incoming traffic across many servers so that one server does not overload and become congested while maintaining operations for many servers.

**Key Considerations for Server Load Balancing in Banking Networks**

- **Redundancy:** Use multiple servers in different data centers to ensure availability even during failures.
- **Geographical Distribution:** Manage traffic across data centers in various locations to improve disaster recovery and availability.
- **SSL Offloading:** Shift encryption/decryption responsibilities from application servers to load balancers for better efficiency.
- **Health Monitoring:** Regularly check server performance and reroute traffic if a server is unhealthy.
- **Session Persistence:** Maintain user session continuity during server switches.
- **Security:** Include firewalls, IDS/IPS, and DDoS protection to counter cyber threats.
- **Scalability:** Use auto-scaling to handle traffic changes dynamically.
- **Traffic Management:** Implement content-aware and URL-aware routing to manage traffic effectively.
- **Compliance:** Ensure the solution meets organizational standards like PCI DSS.
- **Monitoring and Logging:** Centralize log data collection and enable alarms for traffic changes or performance issues.

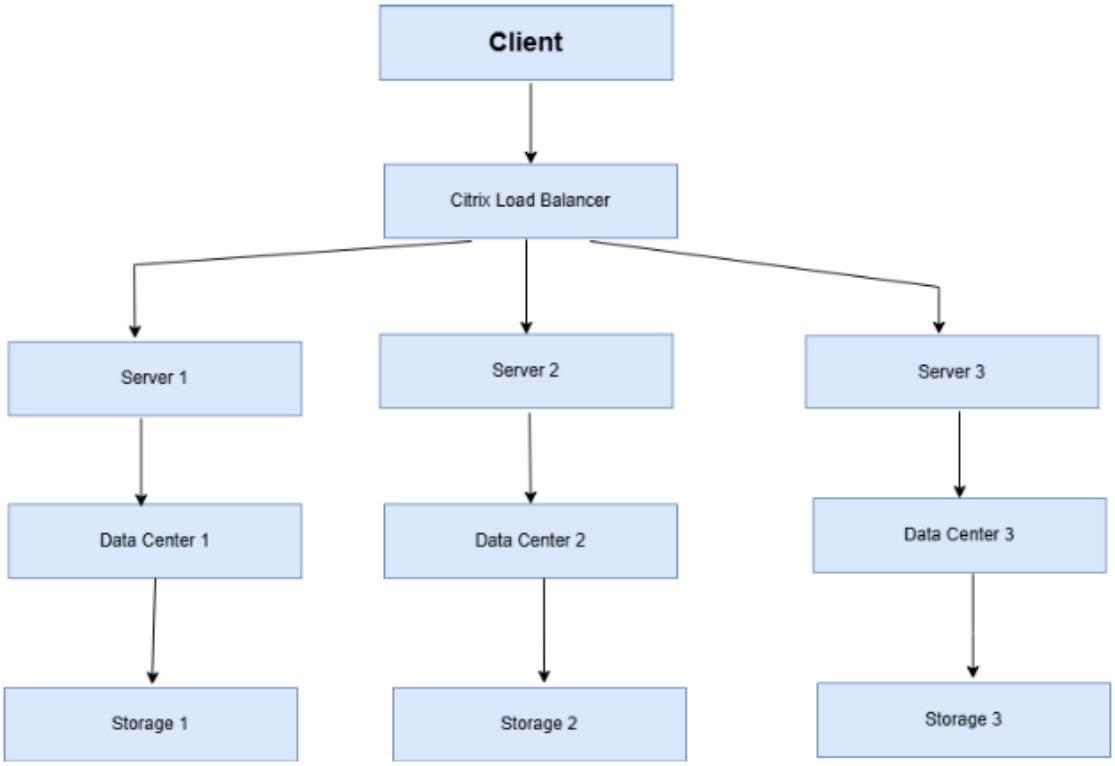


Figure 5.2: Server Load Balancing Architecture

### 5.1.4 VPN Tunneling

VPN tunneling is one of the most popular methods of creating a connection over the internet that is very safe through the establishment of an encrypted channel. This comprises the process of embedding one protocol's data packets in another protocol to guarantee security and integrity while transferring data. VPN tunneling is notably useful in establishing a secure connection within an insecure system, for instance, the internet, to access a secure network.

#### Key Features and Benefits of VPN Tunneling

- **Encryption:** VPN tunnels encapsulate the payload into this tunnel by encrypting the data packets so that only allowed parties can understand them. This encryption ensures that intercepted data cannot be read.
- **Data Integrity:** VPN tunneling involves the enveloping of the actual data packets to ensure their contents remain unchanged during transit.
- **Secure Access:** Allows employees, contractors, or partners to securely access the organization's resources from any geographical location.
- **Privacy:** VPN tunneling conceals the user's identity by hiding their IP address and limits monitoring.

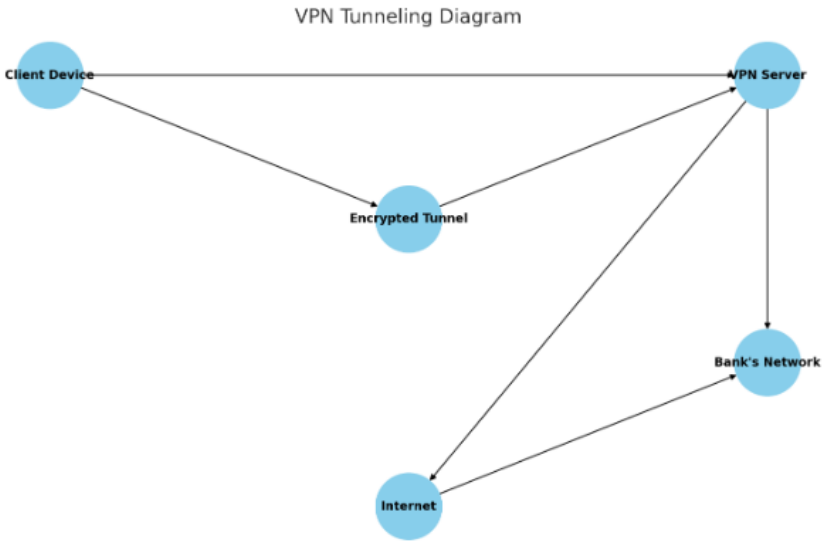


Figure 5.3: VPN Tunelling Diagram

**Applications in Banking Networks**

- **Remote Access:** Establishes a secure connection for remote employees, reducing risks of unauthorized access.
- **Inter-branch Communication:** Creates a secure channel for exchanging messages and information between branches.
- **Customer Transactions:** Protects sensitive information during online banking transactions, ensuring secure data exchange.

### 5.1.5 Web Application Firewall (WAF)

Web Application Firewalls (WAFs) are crucial in protecting web applications from threats such as injection attacks, cross-site scripting (XSS), and SQL injection. By monitoring and filtering HTTP/HTTPS traffic between a web application and the internet, WAFs detect and block malicious traffic while allowing legitimate traffic through.

**Key Features and Benefits of WAF**

- **Advanced Threat Detection:** Blocks sophisticated attacks using threat patterns and intelligence.
- **Granular Access Controls:** Implements detailed security policies, limiting access to authorized users only.
- **Real-time Monitoring and Logging:** Scans logs and traffic in real-time, allowing for immediate response to threats.

- **Compliance with Industry Regulations:** Helps meet standards like PCI DSS by securing monetary operations and identity information.
- **Integration with Other Security Solutions:** Works with SIEM systems for end-to-end protection.
- **Scalability and High Availability:** Handles high bandwidth and grows with traffic demands.
- **Regular Updates and Patches:** Adapts to emerging threats with frequent updates.

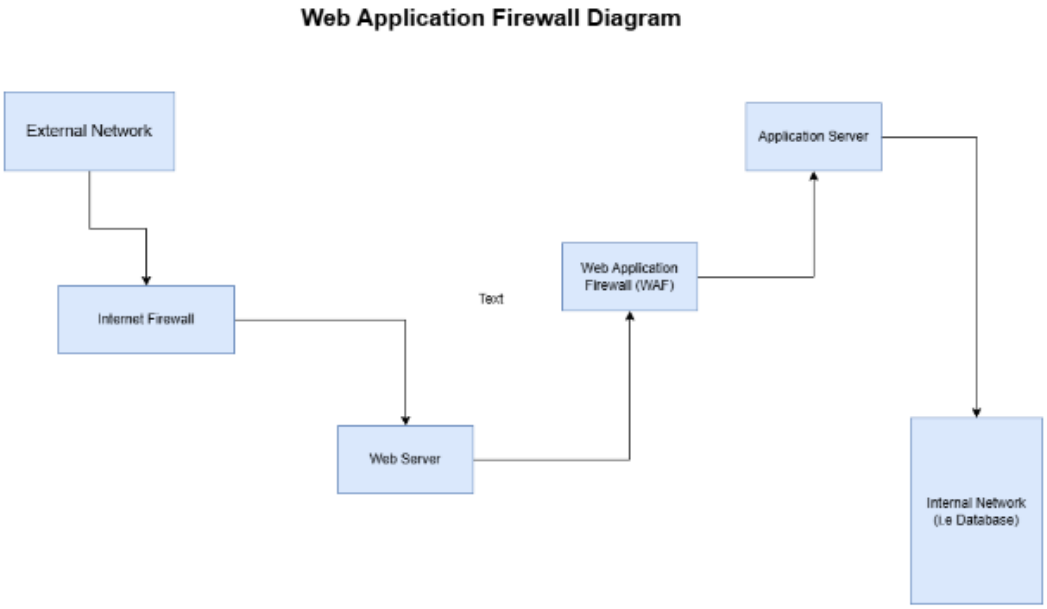


Figure 5.4: Web Application Firewall Features and Functions

### 5.1.6 Network Access Control (NAC)

Network Access Control (NAC) solutions enforce policies to regulate access to the banking network based on users' and devices' compliance with security protocols.

#### Key Features of NAC

- **Endpoint Security Checks:** Ensures devices are compliant with security policies, such as having up-to-date antivirus software.
- **Authentication:** Uses multi-factor authentication (MFA) and other methods to validate user identities.
- **Role-Based Access Control (RBAC):** Grants access to network resources based on users' roles.
- **Monitoring and Logging:** Tracks and records all network access attempts for security reviews and audits.

**Applications in Banking Networks**

- Prevents unauthorized access by filtering users and devices.
- Enhances endpoint security by ensuring connected devices meet compliance standards.
- Maintains regulatory compliance with industry standards.
- Provides critical data for incident response and analysis.

### 5.1.7 Information Security Controls (ISC)

Information Security Controls (ISC) encompass policies, technologies, and measures to protect banking networks from risks such as cyber threats and data breaches.

**Key Components of ISC**

- **Firewalls:** Filter incoming and outgoing traffic based on security rules.
- **Intrusion Detection and Prevention Systems (IDS/IPS):** Monitor network activity to detect and respond to threats.
- **Encryption:** Protects data in transit and at rest from unauthorized access.
- **Access Controls:** Restrict access to sensitive information using role-based policies.
- **Authentication Mechanisms:** Use biometric verification, smart IDs, and tokens for secure access.
- **Incident Response Procedures:** Define actions for detecting, handling, and mitigating security incidents.

**Benefits of ISC**

- Reduces risks and enhances overall network security.
- Builds customer trust by safeguarding sensitive data.
- Ensures compliance with industry regulations.
- Supports business continuity during security breaches.

### 5.1.8 Advanced Persistent Threats (APT)

Advanced Persistent Threats (APTs) are long-term cyber-attacks aimed at gaining unauthorized access to a network without detection.

**Characteristics of APTs**

- **Stealth and Persistence:** Designed to remain undetected while infiltrating deeper into the network.
- **Targeted Attacks:** Focus on specific entities with high-value data.
- **Multiple Attack Vectors:** Use various methods such as phishing and zero-day exploits.

**Countermeasures for APTs**

- Deploy advanced detection tools like IDS and EDR.
- Conduct regular security audits and penetration testing.
- Educate users about APT risks and mitigation strategies.

### 5.1.9 DNS Security

DNS security is critical in protecting banking networks against cyber threats, ensuring the confidentiality, integrity, and availability of services and data.

**Effective DNS Security Measures**

- **DNSSEC (DNS Security Extensions):** Prevents DNS spoofing and cache poisoning by signing DNS records and ensuring data authenticity.
- **DNS Filtering:** Blocks access to malicious or phishing domains using DNS filtering services.
- **DNS Firewall:** Monitors and filters DNS traffic, blocking suspicious patterns and blacklisted domains.
- **DDoS Protection:** Shields DNS servers from Distributed Denial of Service (DDoS) attacks, ensuring uptime and functionality.
- **DNS Monitoring and Logging:** Tracks DNS traffic to identify intrusions or malicious activity.
- **Regular Updates and Patching:** Keeps DNS servers updated with the latest security patches.
- **Two-Factor Authentication (2FA):** Secures DNS management interfaces by requiring an additional authentication step.
- **Segregation of Duties:** Restricts access to critical DNS components using role-based access control.
- **Incident Response Plan:** Establishes a detailed response strategy for DNS-related incidents.
- **Employee Training and Awareness:** Educates staff on DNS vulnerabilities and best practices to mitigate risks.

### 5.1.10 Web Proxy

Web proxies act as intermediaries between users and the internet, enhancing privacy and access control. In banking, proxies must be used cautiously for secure operations like money transfers.

**Key Considerations for Web Proxies**

- **Reputation and Security:** Choose proxies with a strong history of secure performance.
- **Data Protection:** Avoid entering sensitive information, such as passwords or financial details, when using proxies.
- **Access Restrictions:** Be aware of potential threats like activity logging or advertisement injection by proxy providers.
- **Secure Transactions:** Always use HTTPS for secure connections when performing financial operations.

### 5.1.11 SIEM (Security Information and Event Management)

SIEM systems collect, analyze, and correlate log data from various sources to identify threats and assist in incident management.

**Key Features and Benefits of SIEM**

- **Real-Time Threat Detection:** Monitors events and identifies potential security issues in real-time.
- **Centralized Log Management:** Aggregates logs from multiple sources for a unified view.
- **Correlation and Analysis:** Identifies patterns and anomalies by correlating data from different sources.
- **Automated Response:** Triggers actions like isolating threats or alerting security personnel.
- **Compliance and Reporting:** Ensures adherence to regulatory requirements and facilitates audits.
- **Incident Investigation:** Provides tools for analyzing past events and preventing recurrence.
- **Scalability:** Handles increasing log volumes and integrates additional systems as needed.

### 5.1.12 Antivirus Solutions

Selecting robust antivirus solutions is critical for protecting banking networks from malware and other cyber threats.

**Key Considerations for Antivirus Solutions**

- **Robust Malware Detection:** Detects and removes various threats like viruses, ransomware, and spyware.
- **Intrusion Prevention:** Proactively blocks unauthorized access and identifies vulnerabilities.
- **Real-Time Monitoring:** Continuously scans for threats and provides alerts.
- **Regular Updates:** Incorporates the latest virus definitions and security patches.
- **Compliance with Industry Regulations:** Adheres to standards like PCI DSS for data security.
- **Expert Consultation:** Engages cybersecurity experts to select optimal solutions.

### 5.1.13 Advanced Persistent Threats (APTs)

APTs are sophisticated, targeted attacks designed to infiltrate networks and remain undetected for extended periods.

**Countermeasures for APTs**

- Deploy advanced detection tools like Endpoint Detection and Response (EDR).
- Use threat intelligence to stay informed about emerging threats.
- Implement network segmentation to limit attackers' lateral movement.
- Conduct regular security audits and penetration testing.
- Train staff to recognize phishing attempts and report suspicious activities.

# Chapter 6

# Head Office

The head office for a banking network can vary depending on the specific network. Some banking networks, like JPMorgan Chase or HSBC, have their head officers in major financial centers such as New York City or London. The head office for a banking network typically serves as the central administrative and decision-making hub for the entire network. It oversees various functions such as strategic planning, risk management, compliance, finance, human resources, and technology. The structure of the head office often includes executive leadership teams, departments, and specialized units responsible for different aspects of the network's operations. These structures may vary depending on the size, complexity, and geographical scope of the banking network.

# Chapter 7

# Server Disaster Recovery

The possibilities of disaster recovery for a banking network are an essential factor in the preservation of banking operations and activities in the context of various emergencies and accidents. This entails a complete and integrated course of action and preparations aimed at making certain that banking services are sustained in the event of a disaster and can promptly restore services in the aftermath of a disaster. The following elaborates on key components of an effective disaster recovery plan:

## 7.1 Data Backup and Recovery Systems

It is important to ensure that the most important data gets backed up regularly because it forms the basic foundations of any disaster recovery (DR) plan. Before running this application in banks, the defined set of requirements demands that data is backed up and stored securely. These consist of customer information, records of transactions, financial books, and accounts.
The data backup system should be fully automated to provide regular backups, which decreases the chance of data loss. Additionally, banks must have competent recovery mechanisms to use in case of data loss or corruption. These include:

- Incremental backups
- Snap-shot backups
- Cloud backups

These mechanisms enable the restoration of lost data within the shortest time possible to prevent business interruption.

## 7.2 Redundant Infrastructure

Banks are entitled to have backup systems to provide essential services despite possible failures of the primary systems. Examples of redundant infrastructure include:

- Backup servers and networks to replace failed primary systems.
- Data center redundancy, where data is duplicated in two or more data centers with operations kept in synchronization. If one data center is unavailable, another can take over.

- Power utilities with generators and UPS backup power to ensure uninterrupted service.

## 7.3 Geographical Diversity

Data centers and critical infrastructures should be established in various geographical locations. Centralizing all facilities in one area risks disruption in the event of a disaster. Geographical distribution ensures:

- Continued operation even when some areas face issues like earthquakes, floods, or hurricanes.
- Added security as operations are not prone to regional hitches.

## 7.4 Business Continuity Planning

During and after a disaster, business continuity is essential to maintain vital banking services and products. Strategic business continuity plans (BCP) include:

- Identification of essential business processes.
- Designation of key personnel and their roles.
- A comprehensive communication plan.
- Detailed response plans for various types of disasters.

The goal is to ensure that critical processes such as commercial operations, client relations, and accounting continue to function properly, even during primary system failures.

## 7.5 Testing and Training

Frequent testing and staff training are critical for disaster recovery plan performance. These activities:

- Familiarize employees with the plan through scenarios and drills.
- Identify loopholes and provide insights for improvement.
- Ensure employees understand disaster management techniques.
- Avoid poor handling of emergency events by continuously training employees.

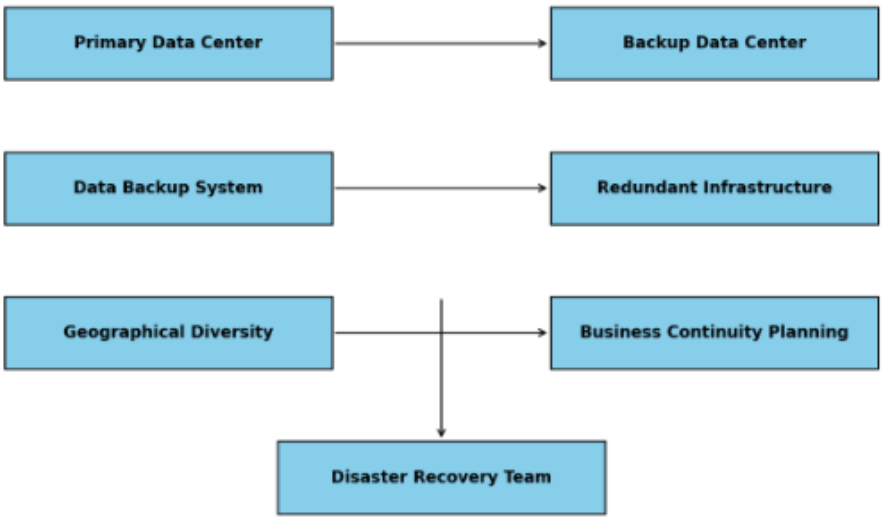


Figure 7.1: Server disaster Recovery Plan Diagram

## 7.6 Security Measures

Security measures are vital to prevent losses associated with banking systems and data during disasters. Effective security measures include:

- Superior firewalls, Intrusion Detection and Prevention Systems (IDPS), and encryption solutions to enhance physical, logical, digital, and information security.
- Multi-factor authentication and access controls to minimize unauthorized access to key systems.
- Recurring security reviews and updates to stay ahead of emerging threats.

# Chapter 8

# Monitoring

The management of a banking network is a constant and integrated activity that consists in observing and controlling all the network nodes and elements. This enhances venture efficiency, quick identification of problems, and the provision of effective solutions. Monitoring is crucial since it helps in maintaining the integrity, availability, and confidentiality of services, specifically in the case of banking services. The following aspects highlight key components and practices essential for robust network monitoring:

## 8.1 VPN Tunneling

One of the critical aspects in the management of modern companies is controlling VPN tunnels. It is vital to provide effective and secure communications between network nodes, such as remote branch offices and mobile employees. VPN tunnels ensure that users are provided a secure route to the banking network as all the information relayed from a user via a network connection is encrypted to ensure that it cannot be intercepted by anyone.
The monitoring must be performed constantly to catch evidence of any kind of malfunction, whether it was a connectivity problem or a decrease in the tunnel's performance, as well as any kind of security threats like attempts at unauthorized access. Visibility and control tools for VPN monitoring are typically in the form of real-time alerts as well as detailed log entries in case of issues.

## 8.2 Network Traffic

The consistent supervision of network traffic is essential for identifying any abnormal activities, which might be signs of a cyber threat or attack, such as a Distributed Denial of Service (DDoS) attack or data exfiltration. Network traffic analyzers and intrusion detection systems (IDS) are used to monitor network flow, identify potential threats, and notify security teams.
Through traffic analysis, banks can predict mishaps and proactively prevent them. This practice also increases the efficiency of a network by identifying congestion points and resolving them.

## 8.3 Firewall and Intrusion Prevention Systems (IPS)

Firewalls and Intrusion Prevention Systems are essential tools in fighting external threats to the network. Firewalls enforce rules that enable or deny traffic, while IPS proactively scans traffic to identify and mitigate potentially exploitable vulnerabilities.
Verifying these systems involves:

- Checking log files for unauthorized access attempts.
- Updating firewall rules to counter new vulnerabilities.
- Acting on detected threats to enhance security.

## 8.4 Server and Device Health

Regular monitoring of servers, routers, switches, and other network devices is critical to avoid network unavailability. Monitoring focuses on factors such as:

- CPU usage
- Memory usage
- Network latency

Alarms are configured to inform the network team of failures or decreases in device efficiency. This proactive monitoring ensures uninterrupted banking services.

## 8.5 Web Application Firewalls (WAF)

Due to the growing trend of application-level attacks, WAFs must be continuously monitored for threats like SQL injection, cross-site scripting (XSS), and other web-based attacks. A WAF sits between the internet and web applications, inspecting HTTP/HTTPS traffic to and from the applications.
Key aspects of WAF monitoring include:

- Identifying and rejecting malicious traffic while permitting legitimate traffic.
- Updating rules to address new vulnerabilities.
- Generating fine-grained logs to identify potential attacks and enable real-time alerting.

## 8.6 Compliance and Security Logs

The financial industry, and banks in particular, are subject to stringent regulatory compliance requirements. Security logs capture events such as:

- User login attempts
- Modifications to systems

- Security breaches

These logs should be checked periodically for compliance and can play a major role in post-incident investigations. Best practices include:

- Collecting and securely storing logs.
- Systematically analyzing log files to identify suspicious activities or attacks.

## 8.7 Antivirus and Malware Detection

Daily supervision of antivirus alerts helps identify infections by malicious software. This involves:

- Installing and updating virus definitions and scanning engines.
- Using anti-spyware tools to prevent programs containing viruses from running.
- Centralized management of antivirus deployments for consistent security across the network.

## 8.8 Data Backup and Recovery Systems

Scheduled backups ensure data integrity and recovery success. Key considerations include:

- Regularly checking backup definitions and job success.
- Verifying the health of storage media used for backups.
- Testing backup restoration processes to ensure data can be restored promptly in case of loss or corruption.

## 8.9 Real-time Gross Settlement (RTGS) Systems

Banks involved in high-value transactions must continuously monitor RTGS systems to ensure:

- Transactions occur without constraints or delays.
- Compliance with relevant regulations.
- Immediate optimization and resolution of problem areas to maintain client confidence in high-stakes financial transactions.

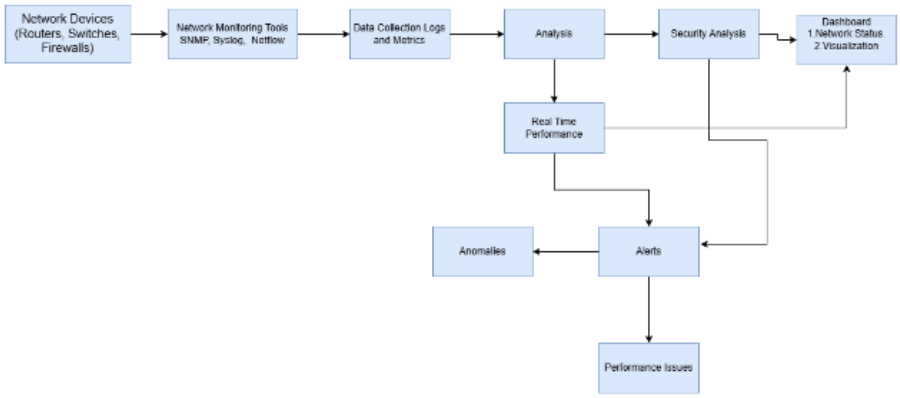


Figure 8.1: Network Monitoring Diagram

## 8.10 Load Balancing

Monitoring load balancers ensures balanced distribution of incoming network traffic across servers. This involves:

- Sustaining service delivery during peak times.
- Managing resources and boosting performance.
- Avoiding server congestion to provide a consistent user experience.

Constant supervision confirms proper operation, identifies performance issues, and ensures adaptive traffic distribution.

# Chapter 9

# Security Protocols and Encryption

## 9.1 TLS and SSL Monitoring

TLS and SSL are critical protocols that enable secure communication over the internet. Monitoring these protocols is essential to ensure the security of information exchanges between servers and clients. This involves a multifaceted approach to secure communications:

### 9.1.1 Certificate Configurations

Proper configuration of digital certificates is vital. This includes:

- **Installation and Validity:** Ensuring certificates are installed correctly and remain valid.
- **Trusted Issuers:** Certificates must be issued by a trustworthy Certificate Authority (CA).
- **Expiration Checks:** Frequent checks to prevent expired certificates.
- **Vulnerability Identification:** Addressing issues like self-signed certificates or weak algorithms.

### 9.1.2 Strong Cipher Suites

The security provided by cipher suites is dependent on the strength of encryption. Recommendations include:

- Enabling only strong and secure cipher suites.
- Removing outdated protocols such as SSLv3 and early TLS versions.
- Regularly reviewing and updating cipher suite configurations to address vulnerabilities.

### 9.1.3 Adherence to Security Standards

Compliance with current security standards ensures robust protection. This includes:

- Following IETF and NIST guidelines.
- Adhering to best practices for securing communication devices.
- Ensuring protection methods are capable of mitigating modern threats.

## 9.2 Patch Management

Patch management involves updating software components with the latest security patches to address vulnerabilities effectively. Key aspects include:

### 9.2.1 Identification of Vulnerabilities

Periodic scanning to detect security threats to TLS/SSL helps identify areas requiring updates or fixes.

### 9.2.2 Deployment of Patches

Patches must be deployed efficiently to address identified vulnerabilities in applications or systems.

### 9.2.3 Testing and Validation

Testing patches in controlled environments ensures that fixes do not create additional problems or disrupt existing services.

### 9.2.4 Documentation and Compliance

Maintaining records of applied patches, including dates and mitigated vulnerabilities, ensures:

- Clear visibility of security measures taken.
- Compliance with regulatory requirements.

### 9.2.5 VPN Auditing

Virtual Private Networks (VPNs) are integral for providing secure remote access to banking networks. Regular auditing ensures configurations meet current security standards. Key elements of VPN auditing include:

### 9.2.6 Encryption Algorithms

VPNs must use strong encryption methods such as AES-256 to protect data in transit. Outdated algorithms can compromise the security of VPN tunnels.

### 9.2.7 Authentication Mechanisms

Secure authentication methods ensure only authorized users can access the network. These include:

- Multi-factor authentication (MFA).
- Regular verification of authentication mechanisms for reliability and effectiveness.

### 9.2.8 Access Controls

Access controls limit VPN usage to authorized users. Measures include:

- Role-Based Access Control (RBAC) to restrict access based on job roles.
- Regular checks on authorization rights to prevent unauthorized access.

### 9.2.9 Logging and Monitoring

Logging and monitoring VPN activities help detect incidents. Key considerations include:

- Logging connection details such as user identity, time, and data exchanged.
- Using real-time monitoring tools to detect suspicious activities, such as multiple failed logins or connections from unusual locations.

### 9.2.10 Regular Audits and Penetration Testing

Periodic security audits and penetration testing help identify vulnerabilities in VPN setups. These tests simulate various attack scenarios to:

- Measure the strength of security precautions.
- Identify areas for improvement to enhance overall security.

# Chapter 10

# ATM and Branch Monitoring

## 10.1 ATM and Branch Monitoring

Physical security controls, especially at ATM and branch sites, play a critical role in ensuring the security and integrity of banking operations. Comprehensive monitoring strategies utilize a broad range of technologies and methodologies to identify criminals or suspects, detect security threats, and prevent malicious activities. The key components involved in ATM and branch monitoring are detailed below:

## 10.2 Video Surveillance

Closed-circuit video surveillance is a vital security measure for branch locations and ATMs. These systems involve placing high-technology cameras to capture all essential areas. Continuous video recording serves multiple purposes:

### 10.2.1 Deterrence of Criminal Activity

The presence of surveillance cameras acts as a warning to potential criminals by creating the impression that their actions are being monitored.

### 10.2.2 Detection of Incidents

Video surveillance can capture unusual activities at ATMs and branches, such as tampering, the installation of skimming devices, or physical attacks.

### 10.2.3 Evidence Collection

In the event of an incident, recorded footage serves as critical evidence for investigations and legal proceedings.

### 10.2.4 Remote Monitoring

Advanced security systems often allow security personnel to monitor multiple regions in real-time through a command-and-control structure. This feature enables rapid responses to incidents, minimizing the time to address security breaches.

## 10.3 Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDS) are essential tools for protecting ATM and branch networks from unauthorized access and cyber threats. IDS technology monitors network traffic and analyzes it for signs of suspicious activity:

### 10.3.1 Network Traffic Analysis

IDS scans and interprets the flow of network traffic and organizational activities to identify irregularities. Examples include:

- High traffic volume.
- Transfer of large data amounts.
- Communication with known malicious IP addresses.

### 10.3.2 Anomaly Detection

IDS can identify unusual activities, such as:

- Attempts to bypass security measures.
- Unauthorized access to restricted network areas.
- Tampering with hardware or software components.

### 10.3.3 Alert Generation

In the event of an anomaly, IDS generates alarms to notify security staff, enabling timely investigations to prevent or address breaches.

### 10.3.4 Integration with Other Security Systems

IDS often integrates with firewalls and Security Information and Event Management (SIEM) systems to provide layered protection against cyber threats.

## 10.4 Transaction Monitoring

Efficient transaction monitoring systems are vital for detecting fraudulent activities and safeguarding financial assets. These systems utilize anomaly detection algorithms and advanced analytics to scrutinize transaction data:

### 10.4.1 Anomaly Detection Algorithms

These algorithms analyze transactions and compare them with baseline patterns to identify deviations that may indicate fraud. Examples include:

- High-value transactions.
- Transactions originating from unusual geographical areas.
- Consecutive transactions that deviate from typical customer behavior.

### 10.4.2 Behavioral Analysis

Transaction monitoring systems examine account activity over time to identify trends and patterns indicative of future fraudulent behavior. Examples include:

- Spending bursts.
- Access from unknown devices.

### 10.4.3 Real-time Analysis

Modern transaction monitoring systems operate in real time, identifying risky behaviors and enabling instant reactions to mitigate fraud. This reduces the window of opportunity for fraudsters to exploit organizational weaknesses.

### 10.4.4 Flagging Suspicious Activities

When suspicious activities are detected, the system flags them for further investigation. Security personnel can take actions such as:

- Contacting customers to verify their activities.
- Temporarily suspending accounts.
- Conducting deeper investigations into potential fraud.

# Chapter 11

# Mobile and Online Banking Platforms

## 11.1 Performance Monitoring

Ongoing monitoring of mobile and online banking applications is imperative due to the likelihood of encountering issues that affect their performance and usability. This process includes monitoring different metrics, such as system availability, response time, and usability.

### 11.1.1 System Uptime

Monitoring system uptime ensures that the banking platform is available for use by customers whenever needed without breakdowns. The primary goal of high availability is to provide uninterrupted access, ensuring clients are not inconvenienced.

### 11.1.2 Response Times

Monitoring response times allows banks to identify periods of increased processing or loading times, which can adversely affect consumers. Tracking these response times enables swift resolution of latency issues.

### 11.1.3 User Experience Metrics

Gathering information on users' experiences with the platforms helps identify usability problems. Key metrics include:

- Time to full page load.
- Rate of completed transactions.
- User flow analysis.

These metrics help banks understand customer behavior on the platforms and identify areas for improvement.
Through the constant evaluation of these performance aspects, banks can diagnose and resolve issues with their mobile and online banking solutions. This ensures efficient performance, preventing disruptions and maintaining consistent service availability for customers.

## 11.2 Security Measures

Security is a critical factor for mobile and online banking solutions as they handle individuals' financial information. The primary objectives of security are to detect and prevent unauthorized access and protect data from modification.

### 11.2.1 Strong Authentication Mechanisms

Multi-factor authentication (MFA) enhances security by requiring multiple forms of user identification:

- Something the user knows, such as a password.
- Something the user has, such as a smartphone.
- Something the user is, such as biometric data.

### 11.2.2 Encryption of Sensitive Data

Encryption protects sensitive data from being intercepted or accessed by unauthorized parties. Key practices include:

- Encrypting data exchanged between the user's device and the bank's servers using advanced encryption standards (AES).
- Encrypting stored data to prevent breaches.

### 11.2.3 Regular Security Assessments

Frequent security checks ensure banking platforms are resilient to attacks. These include:

- Penetration testing.
- Vulnerability scanning.
- Security audits.

Such assessments address potential vulnerabilities before they can be exploited, maintaining consistent security.

### 11.2.4 Patch Management

Failure to update software and systems can leave them vulnerable to exploitation. Timely updates minimize risks by:

- Closing security loopholes.
- Preventing hackers from exploiting vulnerabilities.

## 11.3 Update Management

Regular updates and patches are essential for mobile applications and web-based platforms to address threats and ensure stability. Effective update management involves structured implementation of updates to balance security and usability.

### 11.3.1 Addressing Security Vulnerabilities

Updates often include fixes for security vulnerabilities discovered in earlier versions. Failure to apply these updates promptly can expose platforms to cyberattacks.

### 11.3.2 Improving System Security

Updates also enhance system security by:

- Adding new security features.
- Improving encryption techniques.
- Strengthening authentication mechanisms.

Ongoing supervision ensures these improvements are seamlessly integrated into the system.

### 11.3.3 Enhancing User Experience

Updates provide opportunities to:

- Eliminate bugs.
- Improve performance.
- Add new features.

Tracking user feedback and performance indicators helps prioritize updates that align with user expectations.

### 11.3.4 Compliance with Regulations

Regular updates help maintain compliance with regulatory standards and laws, protecting customer data and avoiding penalties. Periodic updates ensure platforms remain aligned with industry requirements.

# Chapter 12

# Employee Access and Activity Monitoring

Because banking network security must be managed and protected, it is essential to monitor the employees' access and activities. It entails constant monitoring and tracking of all the communication that transpires within the banking network to minimize instances of insider Deceit, unauthorized access and any other violations of database's security. This is a rather holistic approach, which guarantees that only those personnel who have the right to do it can address the bank's systems and information and that can contribute to the protection of integrity and confidentiality of the corresponding work. 12.1. Login Monitoring: Login auditing is a critical procedure that requires the tracking and scrutinizing of employees' logins and interaction with the banking network. It involves tracking login activities, the time and place of logins, and most importantly, any contact with a privileged record. Thus, monitoring these activities the bank will be able to identify attempts at unauthorized or suspicious access on time. It also includes the monitoring of configuration modifications made to systems, as this act may signal a possible security attack or insider danger. For instance, when an employee tries to download data during the evening or from a geographical point that they do not regularly use, such procedures will raise alarms. The aim is to make sure all the entry points of the business are protected from any unauthorized access and to act immediately if there is any suspicious behavior.

## 12.1 Role-Based Access Control (RBAC)

RBAC is a security model that grants rights based on an employee's position in an organization. With RBAC implemented, employees are authorized to use only the systems and resources that are essential to the performance of their roles and functions, thus reducing the chances of having a system breach on employee's malicious actions. The principle of least privilege bars employees from accessing materials that are not related to their line of work; hence, they cannot compromise sensitive information. In RBAC, users define roles based on the responsibilities of the workers, and permissions affecting each role are defined as well; thereafter, workers are assigned to the various roles. For instance, a bank teller would be able to view the customer account and transaction processing system but could not access the organizational back-end system or customer's credit card detail. Through RBAC,

the access type has limitations; thus, it proves effective in increasing the security level of banks besides observing the regulatory laws.

## 12.2 User Behavior Analytics (UBA)

User Behavior Analytics (UBA) is a security approach that utilizes employees' behavior data for purposes of assessing deviations likely to point to misuse or the emergence of new threat sources. To illustrate, to prevent fraud, UBA uses machine learning and data analytics techniques to identify a baseline of normal behavior of each of the employees and, therefore, any changes from this baseline are flagged as suspicious. For instance, if an employee, who usually works with many Customers, starts to deal with so many customer accounts which are so valuable, this is a deviation from the normally expected standards and is likely to be investigated. UBA could pick up risks that are preliminary to security events, including when access is done at odd hours or when the amount of data downloaded is particularly high or there are attempts to penetrate certain parts of the network that are off bounds. Through these steps, it is possible for the banks to prevent insider threats and unauthorized access from escalating into bigger problems. This strategy also has the effect of increasing the security of the banking network in general, as any peculiar or, in the best case, suspicious activity on the network will be quickly detected.

# Chapter 13

# Compliance Audits

## 13.1 Regulatory Compliance

It is crucial to conduct routine compliance audit check-ups to ensure that the financial entities' banking networks do not violate any of the numerous laws and acts regulating the businesses. Some of these regulations are the General Data Protection Regulation (GDPR) which requires protection of personal data of a person within the participating Union, and the Payment Card Industry Data Security Standard (PCI-DSS) that outlines measures to be followed while processing credit card transactions. Moreover, it is essential to adhere to banking laws of the specific country to ensure operation legal tender statuses; and thus limit the possibility of the business facing legal consequences. These are then termed as compliance audits that entail routine assessment of the policies, procedures and systems of the bank regarding these strict regulations. The tools for monitoring are becoming the essential part of such processes as they are responsible for the collection and the logging of the data which is needed for the audits. These tools generate and record system activities, access logs, and transaction histories which the auditors can go through to confirm if the bank is meeting all the laid down regulations. There are often progress reviews and updates to ensure the compliance policies are modified as required by the changes in laws and regulations and to address any of the issues stated above.

## 13.2 Data Protection

Regulatory compliance is a key component of doing business, particularly handling and protecting clients' information. Data protection solutions are implemented to achieve security objectives that would shield information from unfavorable incidents such as unauthorized access, data leaks, and other similar vices. CCTV cameras are used to monitor the access and utilization of data within the banking network permanently. Measures that can be adopted to enhance the level of data protection include using advanced means of data encryption whereby the data cannot be understood by any unauthorized person, in addition, applying strict measures of access control whereby only persons who are allowed can access the data set. Such precautions as IDS, IPS, and new generations of firewalls are set up to counter possible cyber threats. Furthermore, activities like risk assessment and vulnerability scans that expose loopholes are also conducted to check. In data protection compliance audits, the latter confirms that these protective measures work and are correctly

applied in the protection of customer information. This includes the examination of such areas of banking networks security as encryption, access, and policy checks.

## 13.3 Documentation and Reporting

The final procedures of compliance audits are documentation and reporting. Tools used for monitoring produce excellent documentation and logs which account for all events, attempts, and changes that occur in a system. Such reports act as a record of the bank's compliance programs presence, offering a clear account of its safety procedures. Documentation refers to the organizational policies and processes that affect the protection of the information, incident management procedures, and records establishing employees' training and education. These documents are used during the compliance audits to check them for compliance with the set regulations and policies and conforming to industry standards. Reporting also includes preparing and submitting various compliance reports which update the regulatory bodies on the level of the bank's compliance with laws and regulations in its operations. Such documentation ought to be kept up to date and undergo revision every time there is a change in the laws or the company's policies. Through reporting there will be evidence of legal compliance but at the same time give insight to where reforms can be practiced and create quality assurance in the banking institution.

# Chapter 14

# Performance Metrics and Service Quality

## 14.1 Transaction Processing Times

Transaction processing times must be monitored so that efficiency problems that could affect the overall service delivery quality can be detected early. This entails monitoring the time that it takes for various transactions to be affected from the time they are entered in the system to the time they are processed to their completion. When transactions are processed slowly, it becomes a source of dissatisfaction to the customers hence the need for the optimization of the transactions for the banking sectors. More specifically, the time taken to process a transaction, such as in the case of banking transactions, can help banks identify possible bottlenecks in terms of transactions by pointing out possible reasons for delay, for example the time taken by the network to connect two nodes, the time it takes for a server to process a transaction or an efficient algorithm to be used in a piece of software, among others. When these are realized, then effective ways of operating could be looked at or new and better hardware put in place, or the software could be made to run more efficiently. Efficient and effective transaction processing helps increase the satisfaction level of the customers besides improving the overall capacity of the management of the bank in handling large numbers of transactions daily.

## 14.2 System Availability

The last measure of system availability is a parameter that guarantees customers' access to banking services at any time they need them. High availability of a system is designed by system redundancy, failover and regular system checks. Redundancy means having many identical copies of the basic parts like servers and network devices so that if some fail, they are replaced by others, and service is not affected. Failover is a process by which backup systems are activated to take over the operations in case the main systems fail to function, this helps in reducing the time for which the operations are stopped to allow for system maintenance. Monitoring on the other hand involves scrutinizing all the components in the system with an aim of identifying a situation that requires the intervention of a diagnostics tool before it turns out to be severe. This can range from the monitoring of the load and

traffic level on servers to the performance of the resident applications. Through the above strategies, guaranteed high system availability can be attained that will lead to customer confidence and satisfaction as the banking services will always be up.

## 14.3 Error Rates

Supervision of the error rates is an indispensable factor for evaluating and preventing problems that jeopardize the quality and stability of banking services. They can show the defects in the software, settings problems, or hardware problems that need to be fixed. This type of monitoring focuses on the number of occurrences and loss rate of the transactions that go through a particular system, and several other factors, including system crashes and data discrepancies. Because the errors themselves are significant, it is important for banks to also pay attention to the issues that they indicate. Fixing can then be performed regarding software glitches updating and modifying system configurations that may have caused the problem to appear in the first place or replacing a defective part. System updates and patches can also be of assistance in lowering errors because these contain identified risks and contribute to a more stable environment. This involves constant surveillance and quick problem identification and solution as they allow bank managers to solve small problems before they grow into a huge problem thus making the experience of banking efficient and effective for the customers.

# Chapter 15

# Third-Party and Partner Network Connections

## 15.1 Security Assessments

Security auditing of third-party connections with the banking network and the partners' connections should be done periodically. These assessments consist of the assessment of the security processes and controls in place in the third parties and their ability to meet or satisfy the banks' security standards on third-party management.

1. Encryption Protocols: Third party encryption protocols are one of the primary results of security assessment. The transmission of data and information requires protection particularly between the bank and its partners; thus, encryption is crucial in the protection of information exchanged. The assessment verifies the effectiveness of such mechanisms as SSL/TLS and confirms that they are optimally developed and correspond to modern trends.

2. Access Controls: Other important parts of security assessments also include matters to do with access controls. This entails ascertaining that the third party's suppliers have adequate measures of access control that would prevent unauthorized access to the required data and systems. It includes the responsibility of ensuring the right level of access is given to the users, and this can be done following the least privileged principle where the user is only given privileges necessary for a given task. It also looks at whether MFA and other modern access control mechanisms have been applied.

3. Data Protection Measures: Another aspect of security assessments that is also vital is the assessment of the third parties' data protection measures. This entails reflecting on how data is recorded, analyzed, and how it is protected from cyber criminals. The assessment questions are about the measures that the third parties have put in place during the data life cycle, including data encryption at rest, backup procedures, and adequate data breach response measures.

## 15.2 Performance Monitoring

It is significant to continuously monitor the performance of the third-party connections to improve communication between various systems. Performance monitoring involves the tracking of several factors that are related to the efficiency and condition of the connections discussed.

1. Network Latency: Measuring network latency is crucial in showing the delays that may occur in the transmission of data that the Bank has with third party vendors. Big delays can also prove highly problematic when it comes to application and service availability that would be slow to deliver, unresponsive, or offer poor customer experience. Monitoring the bank should be done regularly so that if it is revealed to have latency issues, remediation should be taken to enhance the network's performance.

2. Throughput: Throughput is the actual amount of data passed within a network in each time frame. Throughput checking helps in making sure that the required amount of data traffic can pass through the network with no issues. This is especially relevant for programs that send large amounts of data over the network, for instance, when performing monetary transactions or when two databases need to be in sync.

3. Availability: Much focus must be given to having the best availability of the third-party connections to have the best banking services with no interruption. Finally, an important factor that falls under the umbrella of performance monitoring is the availability of these connections, that is, the ability to track any interruption or unavailability. The ability to track availability constantly ensures timely identification of potential problems to the bank to solve them and reduce their effect on its functioning.

## 15.3 Vendor Management

Vendor management is a critical factor since most third parties connect companies to a network with a view to keeping it safe and efficient. This includes managing third parties and providers of related services to meet the requirements that the bank has put in place for security and performance.

1. Contractual Agreements: In other words, vendor management starts with making certain, legal and detailed contracts with third party vendors. These agreements describe how security and performance will be managed and maintained, and they set the expected standard. Some of the aspects could be specific provisions of data protection, measures and safeguards, rules and regulations of the data protection law, and sanctions for violating the law.

2. Service Level Agreements (SLAs): SLAs are important because they set the performance parameters and expectations of the third-party service providers. SLAs define availability in terms of guaranteeing up-time, response time to a ticket and time required to resolve a ticket. It is therefore helpful every now and then to check over and increase the SLAs to make sure the vendors are on their toes observing the laid down norms and standards.

3. Regular Audits: Another critical factor that cannot be overlooked in the management of third parties is the periodic auditing of the vendor's compliance with the defined security and performance benchmarks. A typical audit entails the assessment of the vendor's security postures, rates of successful operations, and compliance with contractual obligations. These audits assist in finding out areas that need to be changed or need specific emphasis to ensure that the vendors have not relapsed in the set standard by the bank.

# Chapter 16

# Incident Response and Management

Managing and responding to incidents are critical sub-processes of the banking network infrastructure. Such processes help ensure that when an organization's security is compromised, the incidents are managed in the shortest time possible so that the business is back to normal. The next sections of this work describe the key factors related to the incident response process and its management.

## 16.1 Incident Response Plan

An incident response plan management (IRP) is a detailed policy outlining what action should be taken in case of occurrence of a security incident. This plan is vital in that it helps in formulating a coherent and systematic approach to handling an incident, hence reducing the effect of the same. Key components of an IRP include

1. Roles and Responsibilities: Implementation of the proper strategy and allocation of duties for each participant in the incident response procedures. It can be arranged in such a manner that everyone understands his role and position and can respond appropriately.

2. Escalation Procedures: Some of the common practices of how far the incident goes up the management and how it is handled depending on its seriousness and area of impact. This makes sure that the appropriate solutions to the problem are availed by the right expertise at the right time.

3. Communication Protocols: Standardization of internal and external communication means. This involves informing such stakeholders as the shareholders, regulatory agencies, and if the public has been affected, the public. The management of the incident may also be very effective with communication to those affected and the public.

## 16.2 Real-time Alerts

Real-time alert creation is an essential step in incidents' identification and handling. Specific monitoring tools and systems that are in place make use of duct tape in

the following way: when there is evidence of increased security threats or other useful data provided by other tools and systems, alerts can be raised. These alerts are rather preventive evaluations, which means that the security team can react in time. Key aspects include:

1. Configuration: Having measures in place that enable the system to signal when something is wrong, like suspicious logins, high traffic or traces of a virus. The tools should be refined in a way that eliminates most of these notifications, but at the same time, actual threats aren't missing.

2. Triage and Investigation: Once the alert is created, it is routed for classification to figure out its particularity. Concerning high-risk alerts, investigation properly takes place, and the situation's nature and risk levels are established. This happens by looking at log files, system behavior and anything else that can be used to build out what is happening.

3. Incident Categorization: In the classification process, depending on the type of incident, it is essential to know if it is phishing, ransomware, or a data breach, so that the correct response measure can be taken.

## 16.3 Containment and Mitigation

The process of operating in case of a security threat requires containment and mitigation. The goal here is to try and confine the extent of the infection within the network and prevent it from getting worse. Key actions include:

1. Immediate Containment: When there is a threat of the threat spreading, get hold of the situation by disconnecting all the affected systems from the network. It may include removal of affected devices, suspension of identified compromised users or blacklisting of bad IPs.

2. Blocking Malicious Activity: Measures for halting on-going malicious activities. For example, if there is malware present, it might involve isolating the files that are affected and prevention of the virus from spreading further.

3. Temporary Fixes: Temporary measures to bring back fundamental operations and safeguard the place until a more thorough rehabilitation is made. This may encompass plugging the identified weaknesses, improving settings on a firewall, or adding other tools to the already existing security measures.

## 16.4 Post-Incident Analysis

When the normal business functioning is resumed, and the threat is removed, the post-incident analysis is conducted. This phase is important in finding out the causes of the circumstances that led to the incident and prevent such in the future. Key steps include:

1. Root Cause Analysis: To solve the problem, that is, to look for the causes that underlie the given circumstances, one is to conduct an inquiry into the

details of the case described. This may include the analysis of system logs, comparing the organizational security policies implementing and questioning the staff involved in the response process.

2. Lessons Learned: Sharing the results and determining the key and less successful factors concerning the implementation of the process during the incident response. This contributes to enhancing the general flow of the company's response to the incident and the improvement of subsequent responses.

3. Procedure Updates: Increasing the effectiveness of the incident response procedures based on that. This may include increasing detection ability, developing nice ways to counter the threats or increasing the response's capacity.

4. Security Controls Improvement: Increasing the level of security and ensuring that the organization minimizes instances of vulnerabilities or weakness. This could involve purchasing new security equipment, running further awareness sessions among employees, or adjusting the principles of security.

# Chapter 17

# Implementation of the Network System

To implement the network, the following components and devices are required:

## 17.1 Network Devices and Implementation Procedures

### 17.1.1 Network Devices

**Routers**

- **Core Router:** Manages data traffic between different network segments and directs traffic to the distribution switch and other connected devices.

**Switches**

- **Distribution Switch:** Connects branches, ATMs, and agent banks to the core network.
- **Core Switch:** Provides a central connection point for various servers and internal network segments.
- **Top of the Rack (ToR) Switches:** Positioned at the top of server racks to efficiently manage data traffic within the data center.

**Firewalls**

1. **Internet Firewall:** Protects the network from external threats by filtering incoming and outgoing internet traffic.
2. **Web Application Firewall (WAF):** Adds an extra layer of security specifically for web applications to protect against various online threats.
3. **Core Firewall:** Ensures the security of the core network components, protecting against unauthorized access and attacks.
4. **Bangladesh Bank Firewall:** Protects the connection between Bank Asia Ltd. and Bangladesh Bank, ensuring secure data transmission.

**Servers**

1. **Agent Bank Server:** Manages operations related to agent banking.
2. **Core Banking Solution Server (iStellar):** Hosts core banking applications and provides necessary infrastructure for banking operations.
3. **Real-Time Errors, Settlement, Backup Server:** Manages real-time transactions, error handling, settlement processes, and data backups.
4. **General Purpose Servers:** Used for various operational needs and hosting other applications as required.

**Network Security and Monitoring**

1. **IPS (Intrusion Prevention System):** Monitors network traffic for suspicious activity and blocks identified threats.
2. **Antivirus Software:** Deployed across the network to protect against malware and other malicious software.
3. **Oracle Solaris:** Used on some servers for its robust, scalable, and secure operating system capabilities, particularly for managing enterprise-level applications and databases.

**Connectivity**

1. **ISP (Internet Service Provider) Connections:** Provide internet connectivity to different branches, ATMs, and agent banks.
2. **IPsec VPN:** Ensures encrypted and secure communication over the internet.

**Other Components**

1. **Network Cables:** Various types of Ethernet cables (Cat5e, Cat6, etc.) to connect different devices within the network.
2. **Power Supply Units:** Uninterruptible Power Supply (UPS) systems to ensure continuous power supply to critical network components.
3. **Rack Enclosures:** To house the servers, switches, and other network devices in an organized manner.
4. **Cooling Systems:** Essential for maintaining optimal operating temperatures for servers and other network equipment.

### 17.1.2 Implementation and Maintenance: Network Architecture for Bank Asia Ltd. and Connectivity with Bangladesh Bank

**Overview**

The network architecture for Bank Asia Ltd. is designed to facilitate secure, efficient, and reliable communication between various banking entities, including branches,

ATMs, agent banks, and the central banking system of Bangladesh Bank. This comprehensive setup includes a combination of routers, switches, firewalls, servers, and advanced security systems to ensure robust network operations. Below is an elaborated description of the network components and their implementation procedures within the context of Bank Asia Ltd. and its secure communication with Bangladesh Bank.

**Router Implementation**

**i) Core Router:** The core router is pivotal in managing data traffic between different network segments within Bank Asia Ltd. It directs traffic to the distribution switch and other connected devices, ensuring optimal data flow. The core router maintains network efficiency and stability by managing high-volume traffic and implementing routing policies that prioritize critical banking applications.

- **Configuration:** Configure the core router with routing protocols (such as OSPF or BGP) to handle inter-network data flow efficiently.
- **Security:** Implement access control lists (ACLs) to restrict unauthorized access and ensure secure data transmission.
- **Monitoring:** Use network monitoring tools to oversee traffic patterns and optimize performance.

**Switch Implementation**

**i) Distribution Switch:** Connects branches, ATMs, and agent banks to the core network.

- **Installation:** Deploy distribution switches at strategic locations to connect different branches and remote banking units.
- **Configuration:** Set up VLANs to segment network traffic and improve security and performance.
- **Redundancy:** Ensure redundancy with multiple uplinks to the core router to prevent single points of failure.

**ii) Core Switch:** Provides a central connection point for various servers and internal network segments.

- **High-Speed Connectivity:** Utilize high-speed interfaces (such as 10Gbps or 40Gbps ports) to connect critical servers and devices.
- **Load Balancing:** Implement load balancing to distribute network traffic evenly and prevent bottlenecks.
- **Security:** Use port security and ACLs to protect internal data flows.

**iii) Top of the Rack (ToR) Switches:** Positioned at the top of server racks to efficiently manage data traffic within the data center.

- **Rack Placement:** Install ToR switches at the top of each server rack to minimize cabling and enhance management.

- **Interconnectivity:** Connect ToR switches to the core switch using high-speed uplinks.
- **Segmentation:** Use VLANs to segment traffic for different applications and services.

**Firewall Implementation**

**i) Internet Firewall:** The internet firewall protects Bank Asia Ltd.'s network from external threats by filtering incoming and outgoing internet traffic.

- **Rule Setting:** Define firewall rules to block suspicious traffic and allow legitimate communications.
- **Monitoring:** Continuously monitor firewall logs to detect and respond to threats in real-time.
- **Updates:** Regularly update firewall firmware to protect against new vulnerabilities.

The chapter continues with similar detailed sections for all network devices and implementation procedures. If you'd like the complete content including servers, monitoring, connectivity, and additional firewall setups in full LaTeX, let me know and I'll provide it!

# Chapter 18

# Regulatory Compliance and Governance in Banking Networks

## 18.1 Compliance and Governance in Banking

### 18.1.1 Importance of Compliance

Regulatory standards must be followed to ensure the reliability of banking networks. For Bank Asia and the Central Bank of Bangladesh (Bangladesh Bank), adherence to legal and regulatory requirements is essential for safeguarding customer information, maintaining financial system stability, and fostering trust among customers, investors, and banking authorities. Compliance helps prevent financial wrongdoings such as money laundering and fraud by enforcing strict policies and monitoring mechanisms.
Moreover, compliance promotes ethical reporting of financial activities, improving the public image of the banking sector. Conversely, non-compliance carries severe ramifications, including:

- Severe penalties.
- Legal repercussions.
- Loss of public trust and financial resources.

This makes compliance a central component of the institution's operations.

### 18.1.2 Key Regulations

Bank Asia and Bangladesh Bank must adhere to numerous national and international legal and regulatory requirements to enhance their capabilities and protect the financial rights and data of citizens. Some of the key regulations include:

#### GDPR (General Data Protection Regulation)

The GDPR enhances the protection of personal data for European Union (EU) citizens. Although primarily for EU countries, its extraterritorial nature applies to any bank dealing with EU citizens' data, including Bank Asia.

- **Data Privacy:** Personal information must be protected from unauthorized access and misuse.
- **Data Subject Rights:** Individuals have rights concerning their data, including access, erasure, and rectification.
- **Data Breach Notification:** Banks must inform regulatory authorities and affected individuals of data breaches affecting personal data.

#### PCI DSS (Payment Card Industry Data Security Standard)

PCI DSS establishes requirements to protect customers' credit card information. Bank Asia must ensure adherence to PCI DSS policies to safeguard cardholder data.

- **Data Encryption:** Cardholder data must be encrypted during transmission and at rest.
- **Access Controls:** Strict access controls must limit access to cardholder data.
- **Regular Audits:** Routine security assessments and risk analyses ensure ongoing PCI DSS compliance.

#### SOX (Sarbanes-Oxley Act)

The Sarbanes-Oxley Act prescribes standards for financial reporting and corporate governance, particularly for institutions operating in US markets or with securities listed there.

- **Financial Reporting:** Ensures accuracy in financial statements and prevents fraudulent reporting.
- **Internal Controls:** Enhances internal control over financial reporting to protect resources and data.
- **Audit Committees:** Establishes independent audit committees to address financial reporting issues and ensure SOX compliance.

### 18.1.3 Governance Framework

To comply with current legislation, Bank Asia and Bangladesh Bank must establish a comprehensive governance framework. This framework encompasses policy development, risk management, and continuous monitoring to prevent non-compliance risks.

#### Policy Development

Developing sound policies is a cornerstone of good governance. These policies should:

- Respond to regulatory requirements and standards.
- Benchmark against best practices in banking operations.

Key policies include:

- **Data Protection Policies:** Incorporate guidelines that align with GDPR and other data protection laws.
- **Security Policies:** Develop policies for safeguarding financial information, including permissions, encryption, and breach response.
- **Financial Reporting Policies:** Establish clear procedures for financial reporting in compliance with SOX requirements.

### Risk Management

Understanding and mitigating compliance risks is vital for regulatory adherence. Effective risk management includes:

- **Risk Assessment:** Frequently assess compliance risks in data protection, financial reporting, and security.
- **Mitigation Strategies:** Strengthen internal auditing, review standards, align practices with best practices, and provide employee training.
- **Continuous Monitoring:** Use automated tools and regular reviews to detect and address compliance breaches.

### Continuous Monitoring and Improvement

Ongoing compliance requires continuous monitoring and updating of policies and procedures. Key practices include:

- **Compliance Audits:** Conduct regular audits to evaluate adherence to regulations and identify areas for improvement.
- **Training and Awareness:** Provide employees with training programs to foster a culture of compliance.
- **Regulatory Updates:** Stay informed about changes in regulatory landscapes through industry forums, regulatory bodies, and publications.

# Chapter 19

# Cybersecurity Threats and Mitigation Strategies

In protecting its assets, the importance of security, particularly in the contemporary world where personal computers are common among financial institutions is of paramount importance. Organizations in the financial sector including Bank Asia and the Central Bank Bangladesh Bank, their critical position in the financial system and exposure to significant amount of immensely sensitive information make them favorite targets of cyber attackers. It is crucial for these institutions to be acquainted with various typical threats to cybersecurity, as well as to have adequate protection measures in place aimed to prevent their potential threats from damaging such key aspects as integrity, confidentiality, and availability.

## 19.1 Common Cyber Threats

1. **Phishing Attacks:** Phishing refers to the fraudulent tricks used to obtain authorized access to a computer or network through the digital interface of an organization by imitating a trustworthy source. Most hackers employ tactics where they send emails, instant messages, or even fake websites meant to trick people into revealing sensitive information. For example, the following email may appear to be a legitimate message from a trusted source like the internal IT department of the bank or a recognized vendor. The email could contain a link to a spoofed site where users are deceived into providing their username, password, or other sensitive information.

2. **Ransomware:** Ransomware is a form of computer virus that holds its victim's data hostage and restricts access until a ransom is paid. This type of attack can paralyze banking operations by encrypting critical data and processes. For instance, a ransomware attack on Bank Asia could involve attackers encrypting customers' account information, transaction data, and other essential resources. The bank would then become partially or fully nonfunctional until the attackers provide the decryption key or the organization restores data from backups.

3. **Distributed Denial of Service (DDoS) Attacks:** DDoS stands for Distributed Denial of Service. It works by flooding a network's accessibility and

resources with illegitimate Internet traffic, thereby denying services to legitimate users. For example, an attacker may launch a DDoS attack on the online banking services of Bangladesh Bank, causing the website to become inaccessible and preventing customers from transacting online.

## 19.2 Mitigation Strategies

1. **Employee Training:** Awareness is a critical component of any security program. A proposed weekly training schedule ensures that bank employees stay informed about existing threats and how to prevent them. Another benefit of cybersecurity training is that personnel can serve as the first layer of protection against cyber threats.

2. **Phishing Awareness:** Users should be educated on phishing emails and their detrimental consequences. Practical activities, role plays, case scenarios, and simulations can enhance this learning effectively.

3. **Password Management:** Training on forming strong passwords and using password generators helps prevent unauthorized access. Employees should be encouraged to use strong, unique passwords and update them regularly.

4. **Reporting Procedures:** Incident response procedures define how the IT department should react to occurrences such as phishing attacks or security breaches, providing a clear course of action.

5. **Advanced Threat Protection:** Employing highly technical solutions counters existing threats and prevents severe impacts in the future. Key technologies include firewalls, intrusion detection systems (IDS), and antispyware applications.

6. **Firewalls:** Firewalls in a computer network security infrastructure prevent unwanted external traffic from entering the internal network and control traffic flow from the internal network to the outside world. They block unauthorized traffic and ban malicious IP addresses.

7. **Intrusion Detection Systems (IDS):** IDS monitor network traffic patterns to recognize various forms of threats. They generate alerts to help the security team investigate and act on identified threats.

8. **Antivirus Software:** Antivirus programs detect and remove malicious software on devices, preventing attacks. Regular updates ensure the antivirus remains effective against the latest threats.

9. **Incident Response Plans:** Incident handling and response plans are crucial for addressing security breaches effectively. A detailed plan reduces confusion and ensures proper handling of incidents to minimize their impact.

10. **Preparation:** Designate roles and responsibilities for staff involved in incident handling. Ensure team members are well-trained and fully aware of standard response policies.

11. **Detection and Analysis:** Implement means to identify security breaches. Conduct analyses to determine the appropriate course of action and understand the nature of the situation.

12. **Containment:** Quickly cordon off the breach to prevent further spread. Actions may include disconnecting contaminated systems, locking out commandeered accounts, or blacklisting attackers' IP addresses.

13. **Eradication:** Identify and eliminate the root cause of the problem. This may involve installing security patches, updating antivirus definitions, or realigning firewall settings.

14. **Recovery:** Restore affected systems and data to their normal state. Ensure availability and the option to restore backups within the shortest possible time if required.

15. **Post-Incident Analysis:** Conduct a detailed analysis of the incident to incorporate lessons learned into training and improve future responses. Update incident response plans and related documents as needed.

# Chapter 20

# Discussion

The Importance of Robust Network Infrastructure in Banking: Modern banking sector is a very competitive environment that has appeared and develops in a constantly changing technological context. Thus, while organizations like the Bank Asia, Bangladesh Bank among others continue to invest in new age technologies to improve on their services, the reliability of the underlying network becomes even more vital. This section examines the factors of improving the banking network's reliability key issues regarding infrastructure sections and their interactions, compliance with laws and regulations, protective features against cyber threats, and possible technology development trends.
Infrastructure Components and Their Integration: Network structure of the Bank Asia can be defined as physical and logical implemented system components that jointly provide the support to perform banking activities. Thus, physical counters, automated teller machines, internet and mobile banking, banking software application, and payment system form the critical channel of the banking services. The effective coordination of these elements is vital so that customers get standard, secure and reliable services. The infrastructure of handling and processing of basic banking activities like the transactions, accounts, loans, and deposits are performed with the help of core banking systems. The links between physical branches and the online world must be seamlessly managed to enable exchange of information and/or transactions. Hardware and software networking: routers, switches and firewall facilitate the free and proper circulation of data in the banking environment.
Regulatory Compliance and Governance: The banking networks simply cannot operate without adhering to one regulatory standard or the other. Local laws like GDPR, DSS PCI, and SOX are among the regulations that exert a lot of pressure on organizations in terms of data protection, financial reporting and internal controls. Therefore, Bank Asia and Bangladesh bank must also develop the corporate governance structures that are in commensurate with such regulations. Some of the policy areas that should be considered include the formulation of policies as well as the management of the risks involved in the corporation's operations alongside the monitoring of the policies that have been developed. Measures such as data protection policies, security measures, and proper financial reporting are crucial to avoid the possible consequences of failure to comply with those rules. Policies are reviewed and updated from time-to-time, training is also provided to the employees and audits are conducted frequently to make certain the banks meet all the required standards and to familiarize themselves with the changes in law.

Cybersecurity Measures and Threat Mitigation: This is due to the idea that the various and complex types of threats that exist in the modern world of computing are dangerous for banking networks. Thus, banks like Bank Asia and Bangladesh Bank remain vulnerable and hot targets for hackers because they deal with highly sensitive information that is financially based. The prevention and mitigation of security threats and risks to the banking services are important and must be integrated into the institutions effectively. Today, various forms of cyber threats such as phishing attacks, ransomware, and DDoS attacks are very rampant and dangerous and, therefore, need to be addressed. A proactive and effective way of boosting the first line of defense is to provide the employees with training on phishing awareness, passwords protection, and the process of reporting a cyber-attack. A firewall, intrusion detection system (IDS), and antivirus software are some of the most significant tools when it comes to countering threat. Formulation and evaluation of the holistic incident response management capabilities guarantees the bank's ability to contain and reduce the effects of security threats. These plans should include measures on how the preparations for the crisis are made, its identification, control, elimination, restoration, and follow-up assessment.

Future Technological Advancements: This paper aims to identify the roles of new generation emerging technologies like blockchain, AI and quantum computing in re-modelling the banking network infrastructure. Blockchain increases trust and security in transactions as AI increases anti-fraud measures, customer satisfaction, and productivity. Quantum computing, though still under development, holds the key to solving enormous problems at a much faster rate that could revolutionize data protection and security measures on data.

Special attention should be paid to the technological trends mentioned, and their impact on the network should be evaluated by banks. Implementation of new technologies becomes a process that must be properly managed, trialed, and funded to integrate with the rest of the infrastructures.

# Chapter 21

# Conclusion

The study of the network structure of Bank Asia Ltd. has given a significant overview of the complex factors on which the efficient functioning of the bank both in terms of security and the services offered depend. The major characteristic components that have emerged in this study are the physical branches, ATMs, online and mobile banking platforms, core banking system as well as the payment networks that together make up the network architecture of the firms. It is noteworthy that all these components encompass fundamental and therefore crucial aspects of the banking environment that must be guaranteed for banking processes to be efficient and fail-safe. One of the major discoveries that was made in the research is the dynamic interdependence between the physical and the digital layers. Thus, while physical branches and ATMs are still very important for customer attraction and availability of services the use of digital channels changed the nature of customer relations and allows extended hours of service provision. It also benefits the customer whilst at the same time increasing the bank's efficiency with regard to operational flow, as the service load is spread across the various channels. The definitions of the core banking systems have been established as follows; The CB has been defined as the central banking platform that holds important account data and manages main banking operations including Customer Accounts, Transactions, Credit Facilities and Deposits. These systems make it possible for the bank to be able to adapt to the increasing market demands in relation to the scale the bank is expanding at. Moreover, ACH, wire transfer systems, and card payment networks contribute to the secure procedures of making payments which in turn are helpful for supporting the entire financial environment. Network security is a priority issue starting from the overall network architecture. Thus, this report has highlighted the need to implement proper security features where current encryption methods, multi-factor authentication, fraud detection systems, and network access control should be implemented. These measures are very important in ensuring the integrity of the transaction of the customers' data. The elaboration of the disaster recovery approaches underlines the necessity of the advance planning of potential mishaps. Data backup and storage solutions, duplicate or disparate IT assets, the regional setting of IT facilities, and the implementation of business continuity measures are the major elements necessary for organizations' preparation for various challenges. Monitoring approaches like VPN tunneling, network traffic analysis as well as the use of firewalls and intrusion aware systems are very important in enhancing the effectiveness and safety of the network. Such measures as a compliance

audit on a regular basis and full compliance with generally accepted best practices also contribute to the security level and compliance with the banking legislation's requirements.

It can be concluded that Bank Asia Ltd.'s infrastructure network has an organized and secured establishment for the bank's strong foundation to provide and embrace efficient, safe and revolutionary banking services. Implementing and evolving the network topology of a financial institute such as Bank Asia Ltd. can ensure the institute addresses its client's needs and regulatory bodies' demands adequately. It will be useful to comprehend all the challenges and processes that must be done to provide an effective, safe, and reliable banking network in the world of constantly growing and developing finance. The constant improvement of these systems will play a significant role in sustaining a competitive edge and ensuring the stakeholders' confidence and trust.

# Chapter 22

# Reference

## References


1. *Network Infrastructure and Architecture: Designing High-Availability Networks* by Krzysztof Iniewski, Daniel Minoli, Carl McCrosky.

2. *What Is Disaster Recovery (DR)?* by IBM. Available at: https://www.ibm.com/topics/disaster-recovery.

3. *How to Protect Your IT Infrastructure: A Guide to Server Disaster Recovery.* Available at: https://medium.com/@zomev/how-to-protect-your-it-infrastructure-a-guide-to-s

4. *Systems and Network Infrastructure Integration: Design, Implementation, Safety and Supervision* by Saida Helali.

5. *What is Load Balancing? — How Load Balancers Work.* Available at: https://www.cloudflare.com/learning/performance/what-is-load-balancing/.

6. *Cybersecurity Threats and Mitigation Strategies in the Digital Age: A Comprehensive Overview.* Available at: https://www.researchgate.net/publication/368591426_Cybersecurity_Threats_and_Mitigation_Strategies.

7. *Governance, Risk, and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices* by Anthony Tarantino.

8. *Scaling Networks Companion Guide* by Cisco Networking Academy.

9. *Incident Response: Best Practices for Managing and Mitigating Cyber Attacks.* Available at: https://hsctf.com/incident-response/.

10. *Dealing With Third-Party Vendor Connections in Your Network.* Available at: https://securityintelligence.com/dealing-with-third-party-vendor-connections-in-your-network

11. *Key Benchmarks for Measuring Transaction Processing Performance.* Available at: https://www.techtarget.com/searchdatamanagement/feature/Key-benchmarks-for-me

12. *Compliance Audit: Definition, Types, and What to Expect.* Available at: https://www.auditboard.com/blog/compliance-audit/.

13. *Exploring the Impact of Digital Transformation on The Banking Sector: Opportunities and Challenges.* Available at: https://www.researchgate.net/publication/369858116_Exploring_the_Impact_of_Digital_Transformation_on_The_Banking_Sector_Opportunities_and_Challenges.

14. *The Importance of ATM Monitoring and Management Systems.* Available at: https://www.ir.com/guides/atm-monitoring.

15. *Chapter 5: Planning and Implementing TLS.* Available at: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/securing_networks/planning-and-implementing-tls_securing-networks.

16. *What is Patch Management?* Available at: https://www.ibm.com/topics/patch-management.

17. *VPN Audits — A Primer and a Security Audit Checklist.* Available at: https://openvpn.net/blog/vpn-audit/.

18. *What Is Network Access Control?* Available at: https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html.

19. *What Is a Web Proxy?* Available at: https://www.lifewire.com/what-is-web-proxy-3481607.

20. *An Overview of VNC (Virtual Network Computing).* Available at: https://www.linode.com/docs/guides/what-is-virtual-network-computing/.

21. *What is a WAF? — Web Application Firewall Explained.* Available at: https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf.

22. *What is an Advanced Persistent Threat?* Available at: https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt.

23. *What is DNS Security?* Available at: https://www.cloudflare.com/learning/dns/dns-security.

24. *What is a VPN Tunnel?* Available at: https://www.expressvpn.com/what-is-vpn/vpn-tunnel.

25. *What is AAA Security? Authentication, Authorization, and Accounting.* Available at: https://www.strongdm.com/blog/aaa-security.

26. *The Management of Projects* by D. Muench et al. (1994). London: Thomas Telford.

27. *Internship Report for Information Systems Studies* (2004), Fabiann Kannemann.

28. *APEX 20 For Beginners* by Riaz Ahmed.

29. *Oracle Application Express: A Clear and Concise Reference* by Gerardus Blokdyk.

30. *The Software Development Lifecycle: A Complete Guide* by Richard Murch.

31. *Database Design and Rational Theory* by C.J. Date. Available at: https://apex.oracle.com/en/.