

Ensuring Compliance and Control in Banks

SIRC of ICAI

Nov 22, 2025

CA Nagappan K

nagappankn8@gmail.com

What is Compliance?

It is process of adhering to laws, regulations, and internal policies.

In Banking terms, compliance means adherence to RBI Master Directions, Banking Regulation Act, 1949, Indian Banking Association, Payment & Settlement System,2007, FEMA, Income tax act, 1961, and other critical laws, standards & frameworks.

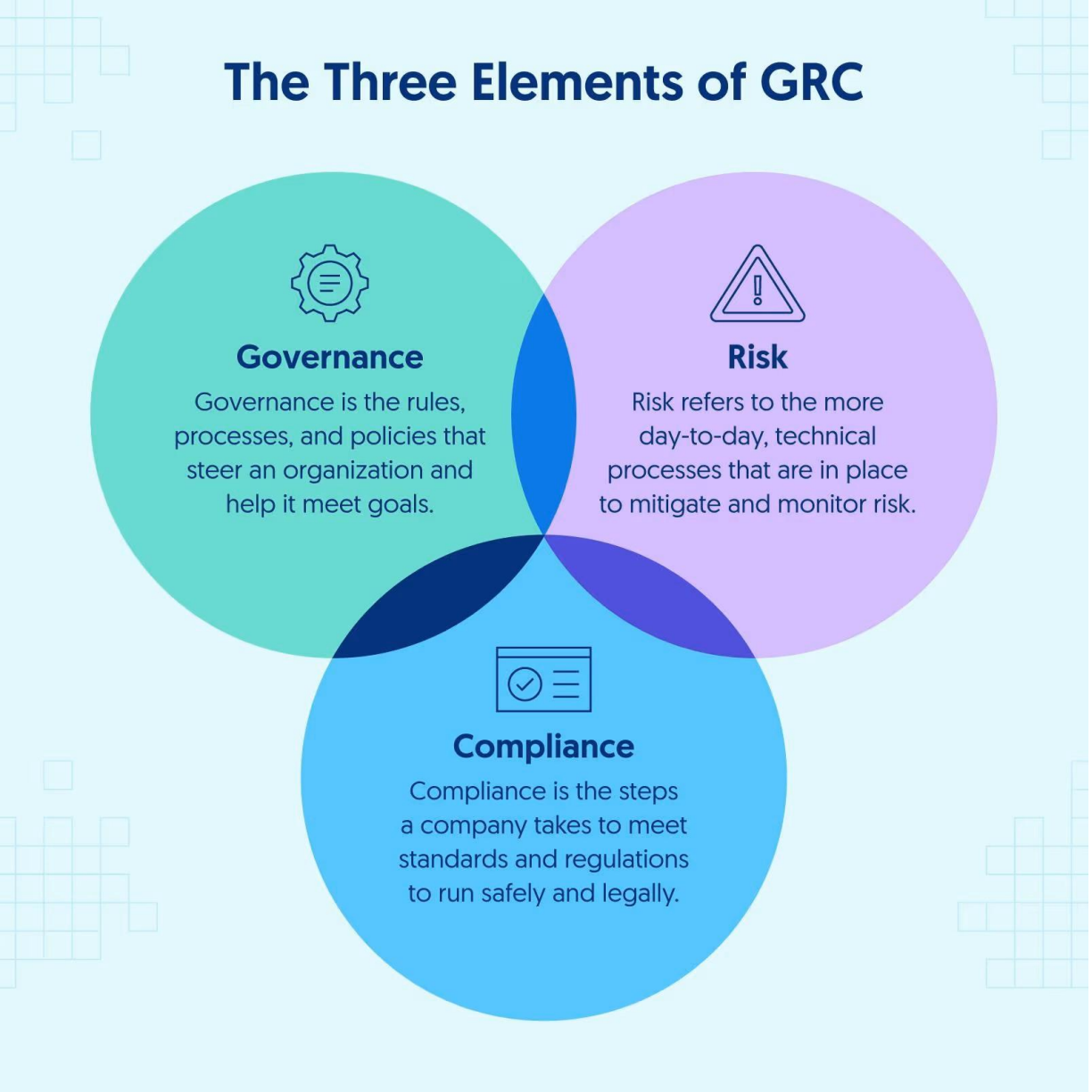
How can you ensure compliance?

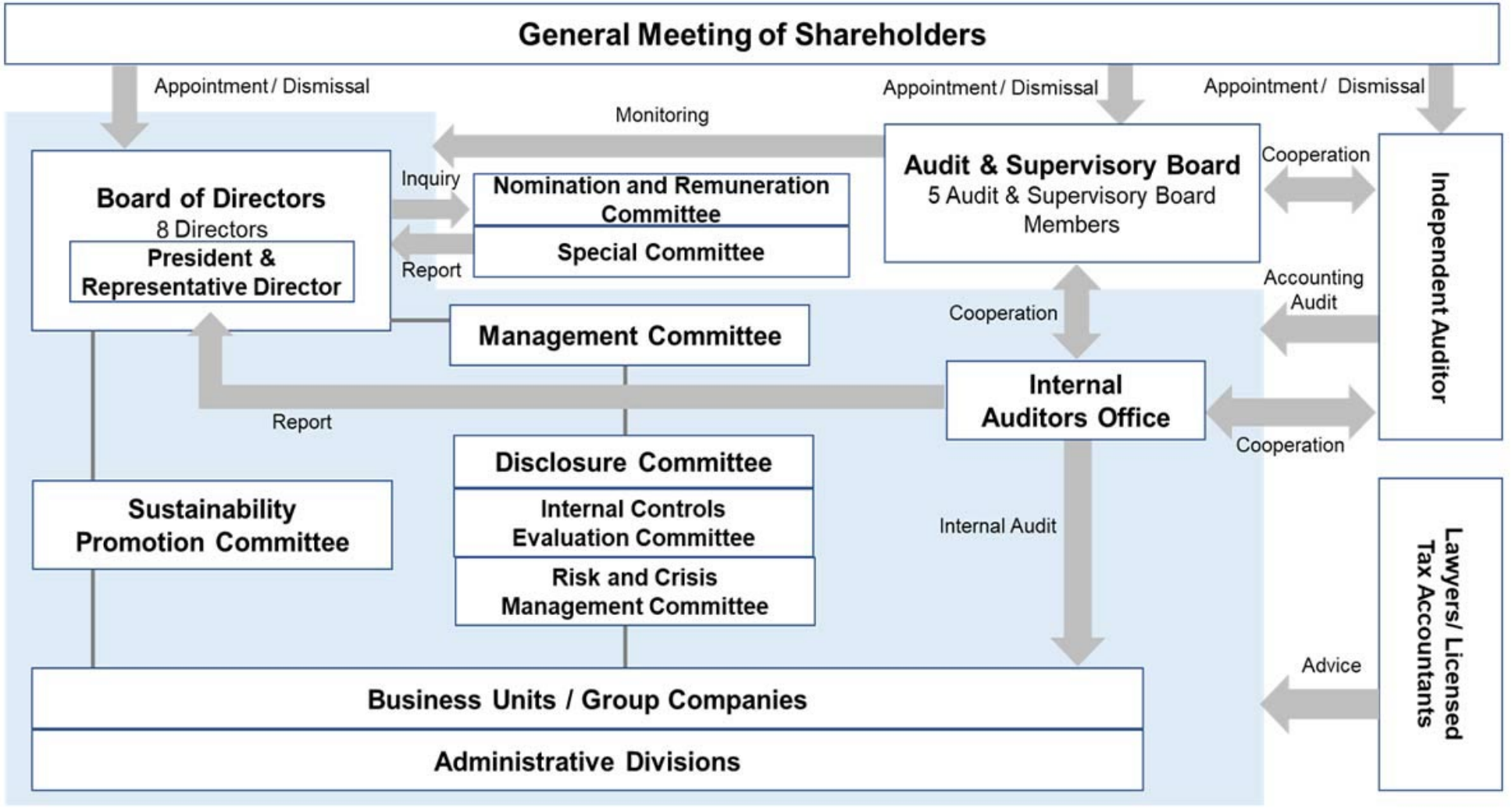
a. Governance

b. Risk

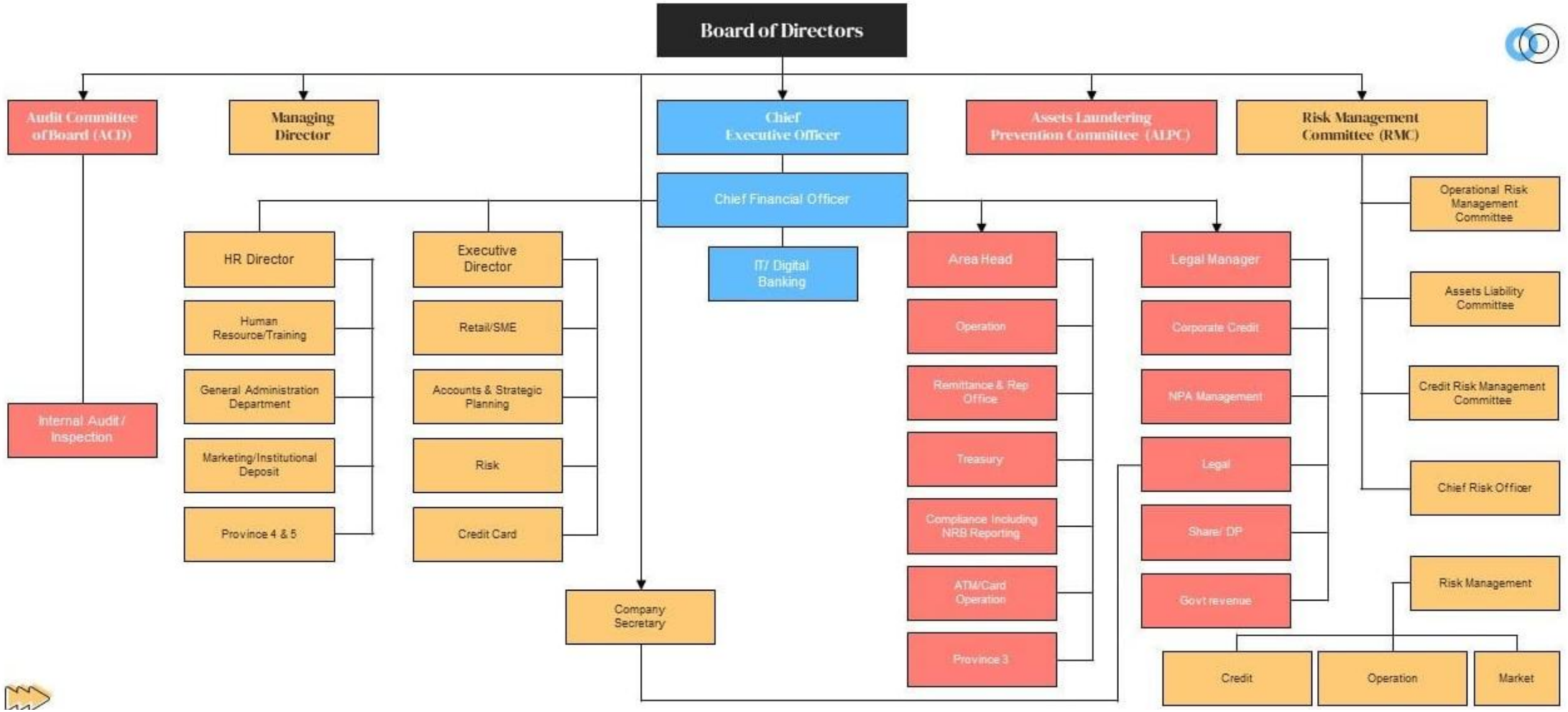
c. Compliance

This Photo by Unknown Author is licensed under CC BY-SA-NC


The Three Elements of GRC
Governance
Governance is the rules, processes, and policies that steer an organization and help it meet goals.
Risk
Risk refers to the more day-to-day, technical processes that are in place to mitigate and monitor risk.
Compliance
Compliance is the steps a company takes to meet standards and regulations to run safely and legally.



Corporate Governance

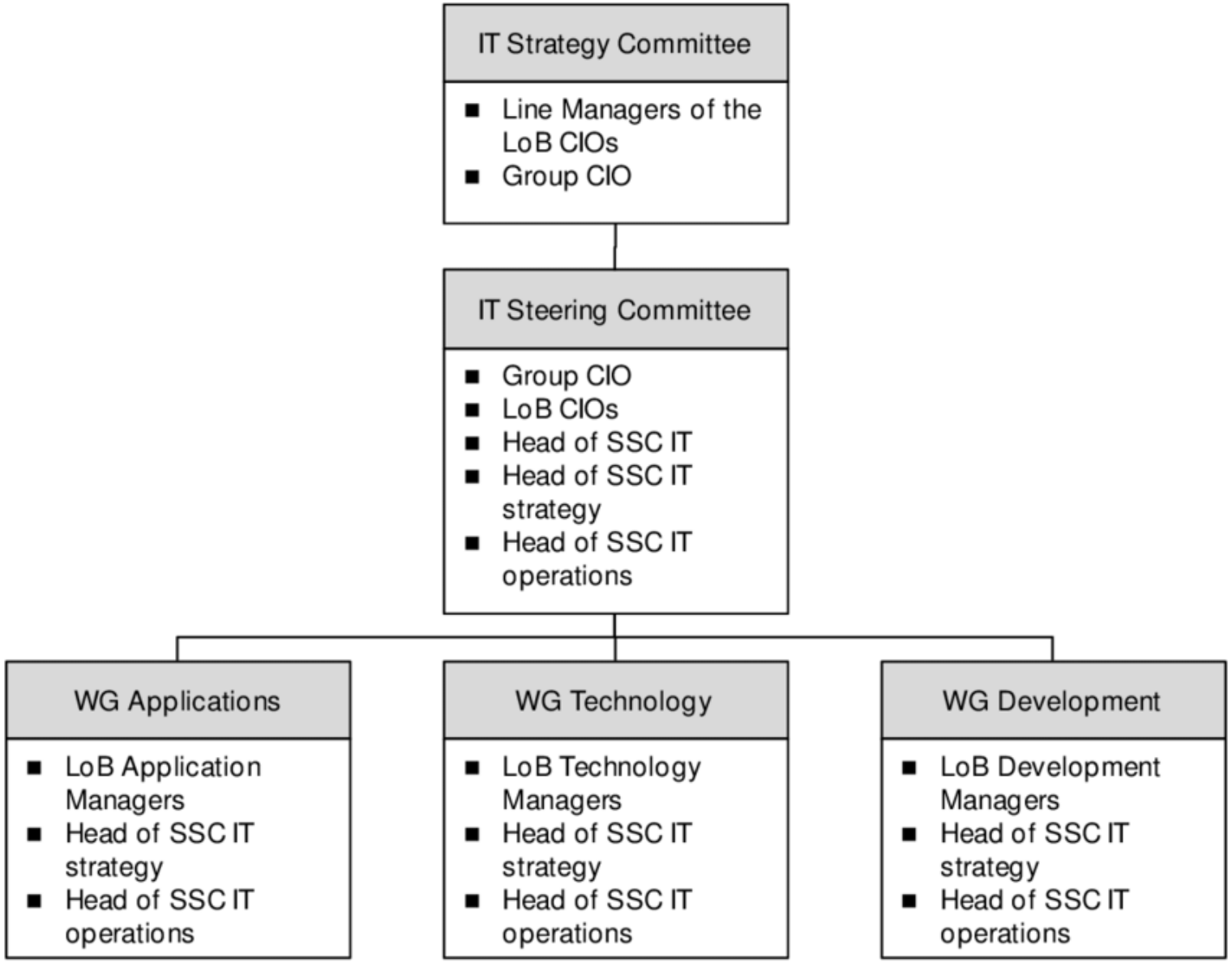


Governance structure in Banks

Set	set the bank's strategy and objectives
Select and oversee	select and oversee personnel
Operate	operate the bank's business on a day-to-day basis
Protect	protect the interests of depositors, and consider the interests of other recognized stakeholders
Align	align corporate culture with the bank's strategy to achieve the objective with integrity and in compliance with applicable laws and regulations; and
Establish	establish control functions

Basel – Corporate Governance

A Banks board and its senior management is responsible for carrying out the banks business and affairs, they include



Key: LoB - Line of Business; CIO - Chief Information Officer; SSC - Shared Services Center; WG - Working Group.

IT Governance in Banks

Colored Cells are the Risk Categories	Low Risk	Medium Risk	High Risk

Frequency of Scenario	Severity of Consequences		
	Low Severity	Medium Severity	High Severity
High Frequency	Medium	High	High
Medium Frequency	Low	Medium	High
Low Frequency	Low	Low	Medium

What is Risk?

As per ISO/IEC 73, Risk is the combination of the probability of an event and its consequence.



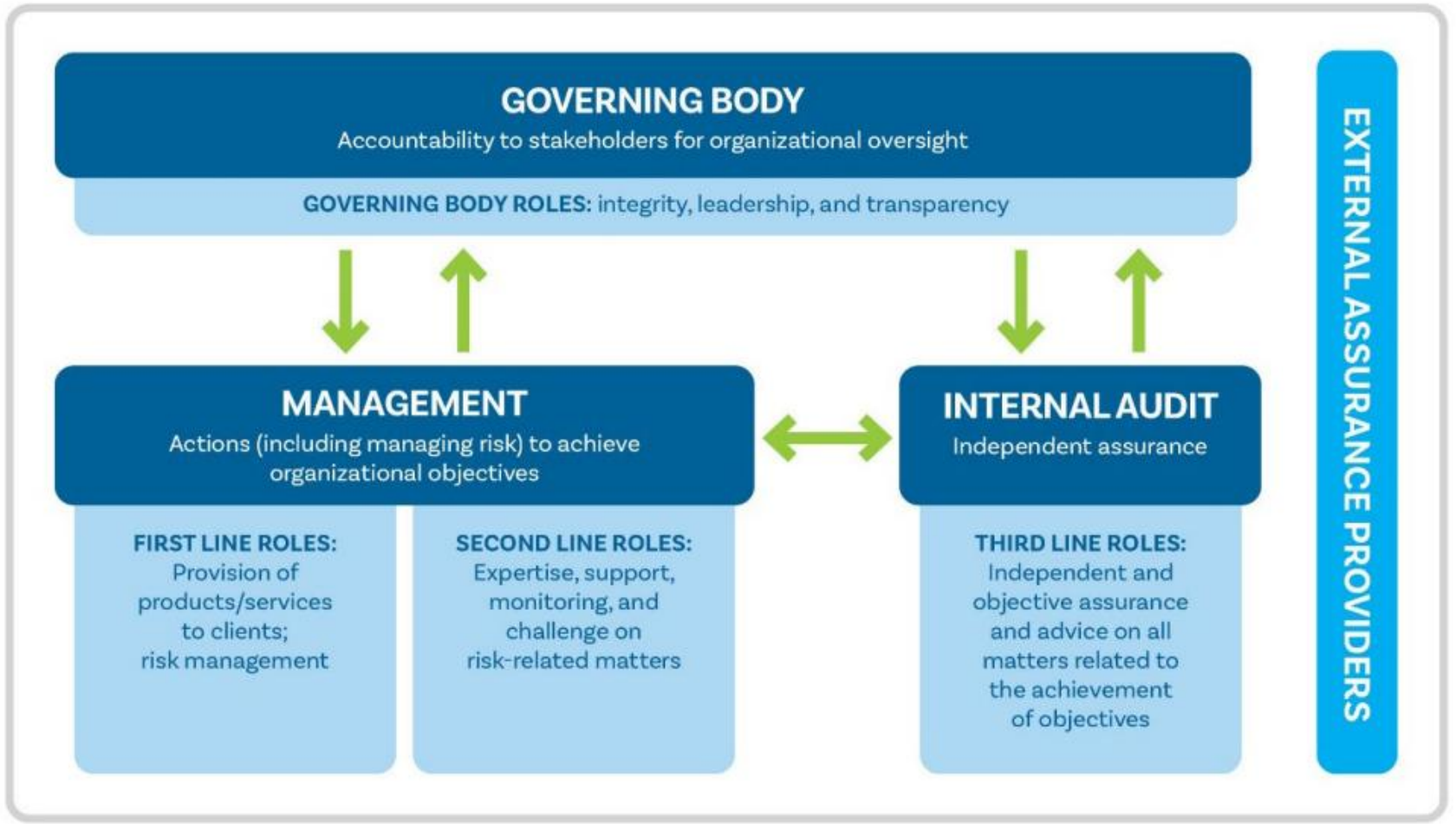
What is Risk management?

Risk management encompasses the overall process of identifying, assessing, prioritizing, and mitigating risks.

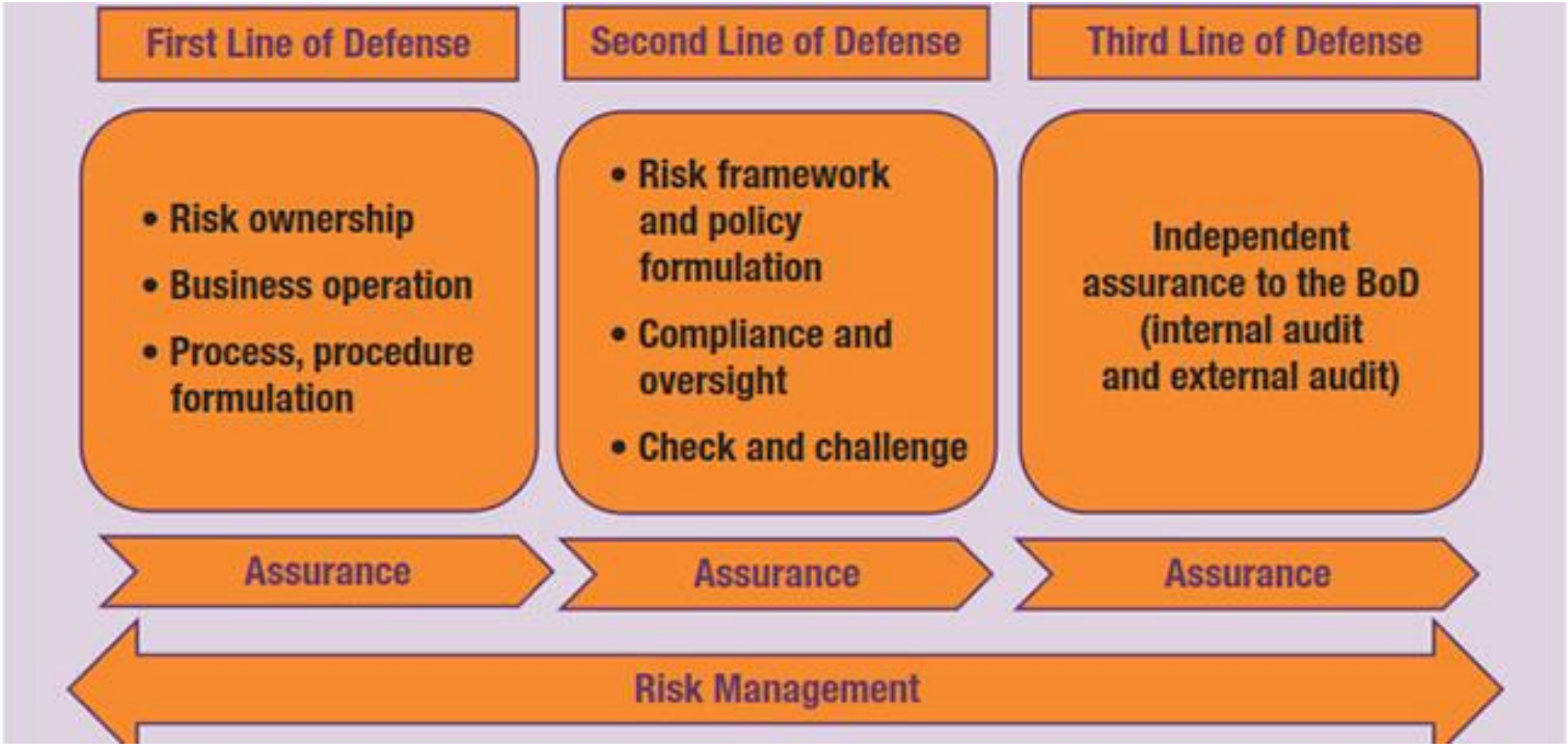
Types of Risk in Banking

Credit Risk	• Risk that a borrower or counterparty may fail or refuse to meet their financial obligations on loans, trades, or other transactions.
Liquidity Risk	• Risk that a bank may be unable to meet its financial obligations on time without impacting its financial stability or condition.
Operational Risk	• Risk of loss arising from failures in internal processes, people, systems, or due to external events, as per by RBI's Operational Risk Management framework.
Market Risk	• Risk of loss caused by fluctuations in market prices, interest rates, exchange rates, or other market variables affecting the value of positions.
Interest Risk	• Risk that fluctuations in market interest rates can affect a bank's earnings or the value of its assets and liabilities.
Compliance Risk	• Risk of legal penalties, financial loss, or reputational damage arising from failure to follow laws, regulations, internal policies, or best practices.

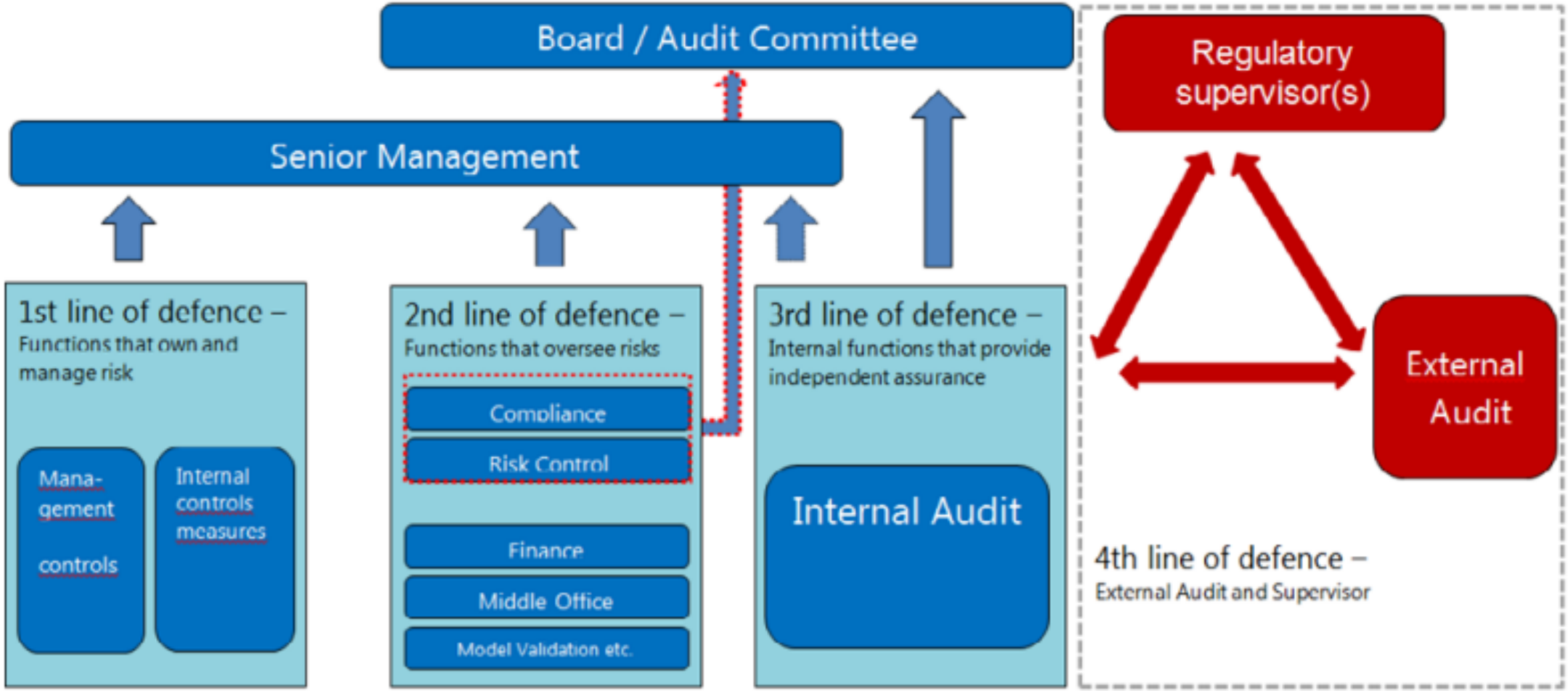
The IIA's Three Lines Model



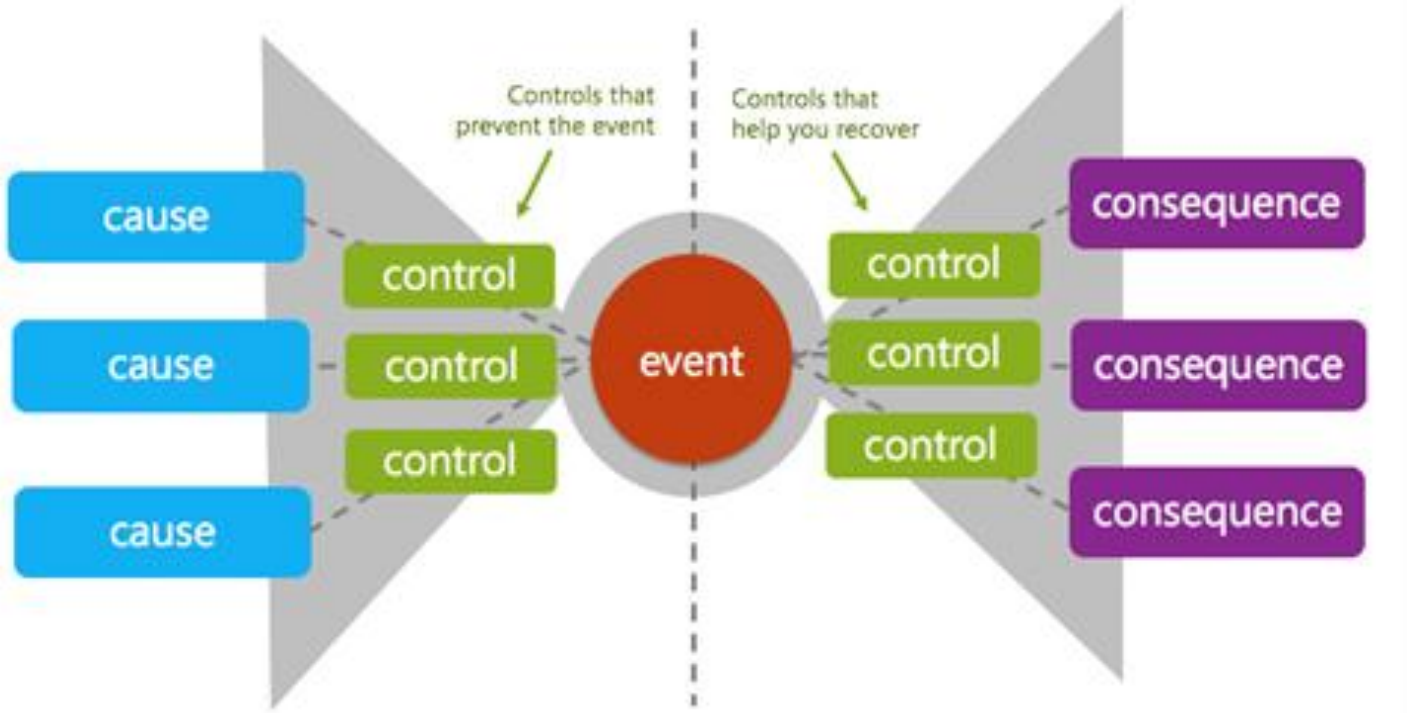
Copyright © 2020 by The Institute of Internal Auditors, Inc. All rights reserved.



ISACAs' Collaborative Defense



BIS – Four-lines-of-defence for FI



What is control?

Controls in risk management refer to measures put in place to minimize or eliminate potential risks and ensure the safety and security of an organization. The different types of control used are

a. *Preventive,*

b. *Detective,*

c. *Corrective.*

Control Objectives – Financial & IT

Financial

- Completeness
- Accuracy
- Validity
- Authorization

IT & Infosec

- Confidentiality
- Integrity
- Availability
- Effectiveness & Efficiency

Measures of Conformance testing?

Regulation

It is a mandatory exercise which should be conducted to comply with the laws.

Best Practices

These are the measures taken by the prominent players in the Industry.

Base line

The essential level of performance, security, and compliance that a process or systems should meet.

Banking compliances

Finance laws

- RBI Act, 1934
- Income tax act, 1961
- GST & Customs
- PMLA, 2000
- FEMA, 1999

Data Privacy Laws

- IT Act, 2000
- DPDP Act, 2023
- GDPR, 2018

General laws

- Indian Contract Act, 1872
- Negotiable Instrument Act, 1881

Standards & Frameworks

- ISO 27001
- PCI - DSS
- NIST

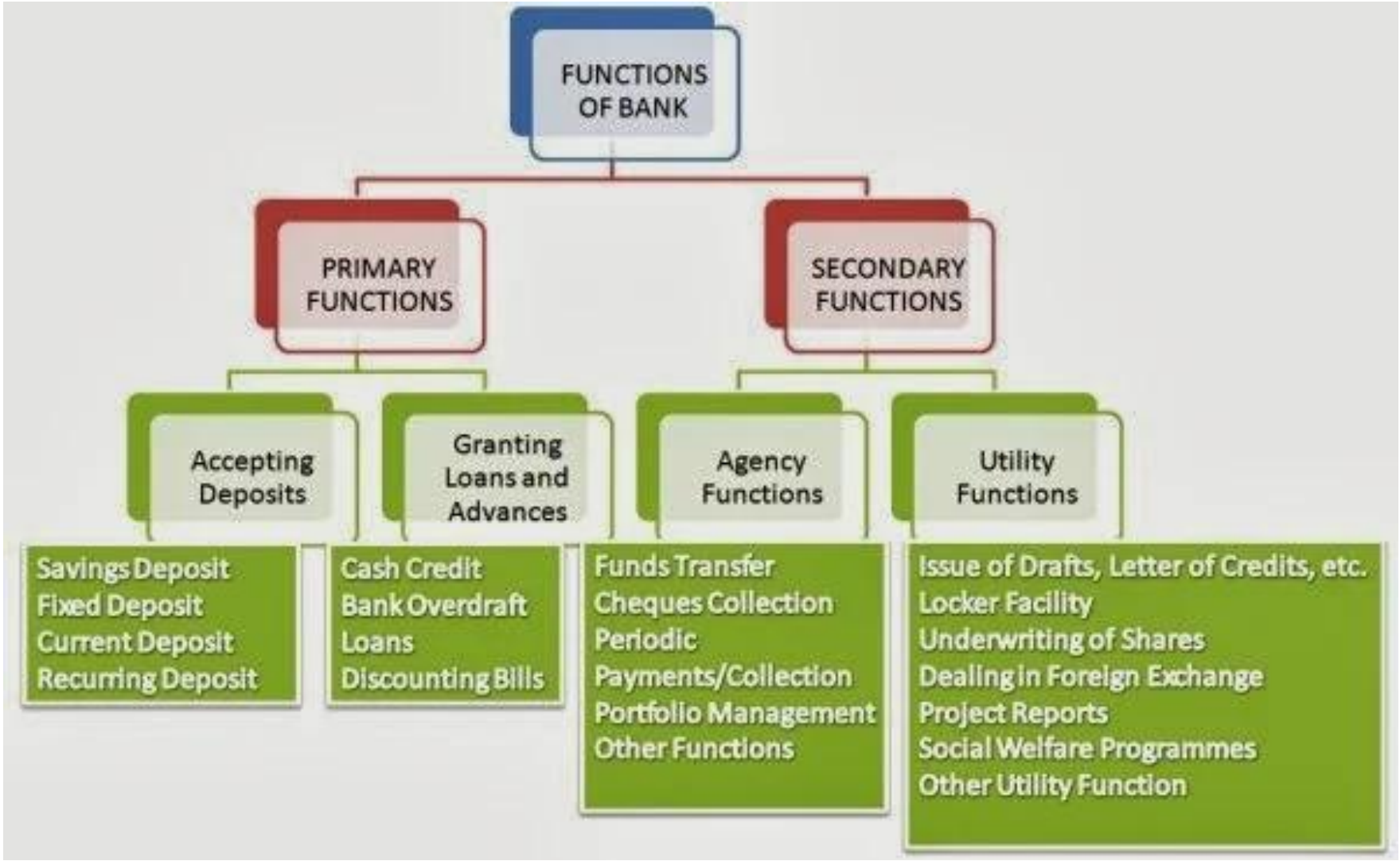
Basel III – Capital Regulations

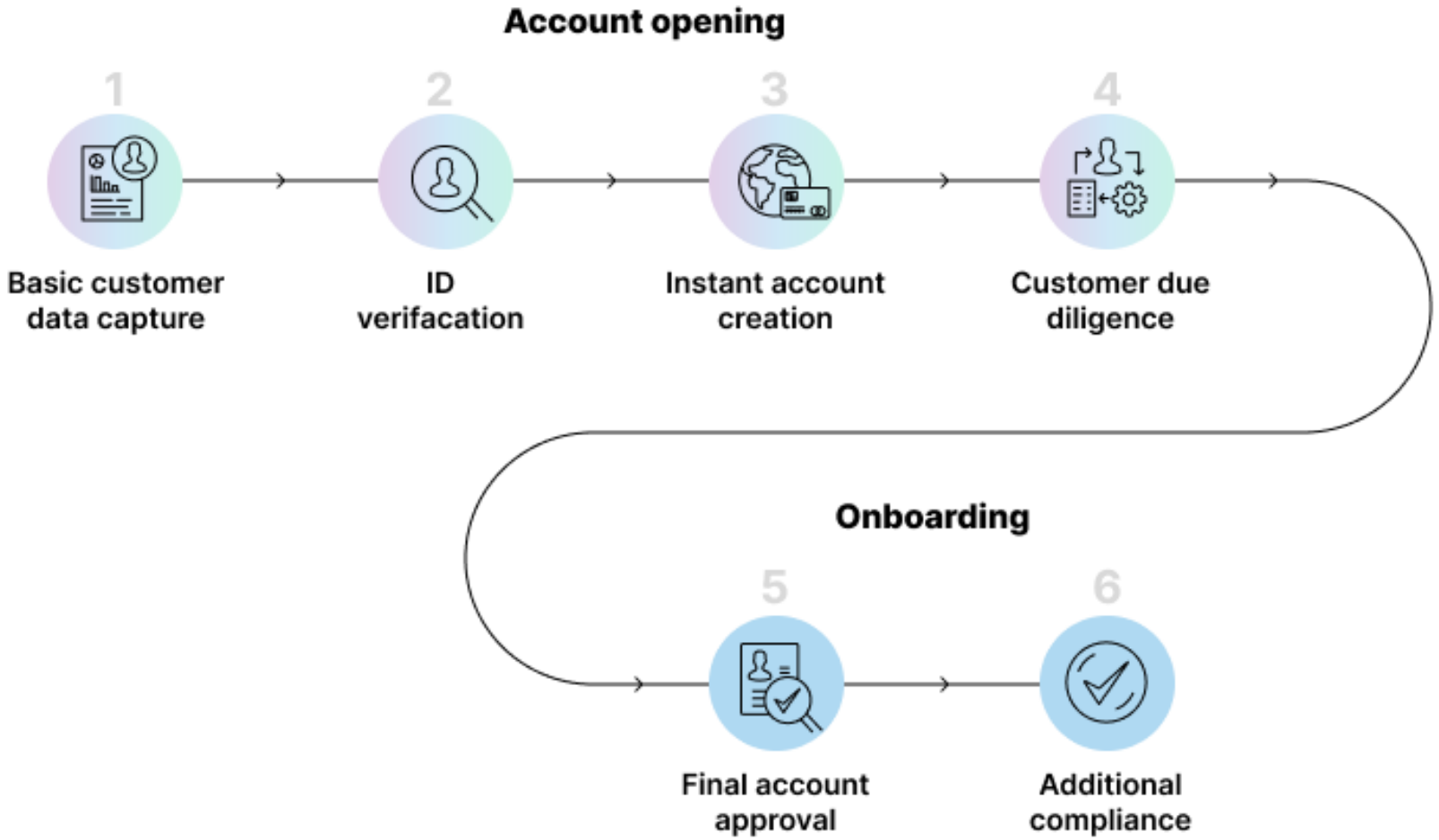
Pillar 1 – Minimum Capital Requirement

Pillar 2 – Supervisory Review and Evaluation Process

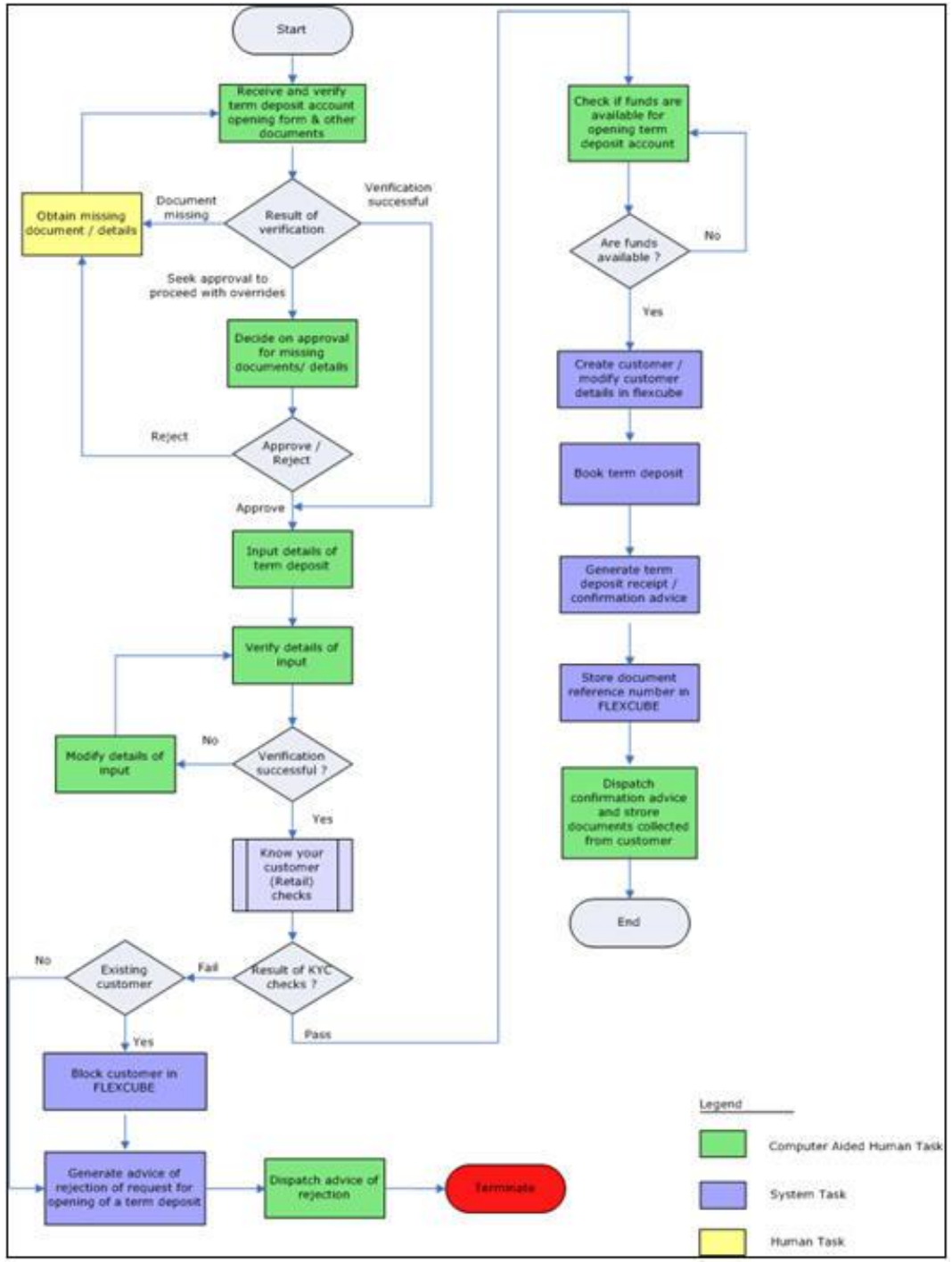
Pillar 3 – Market discipline (disclosure)

Functions of a Bank





Case Study 1 – Accepting Deposits



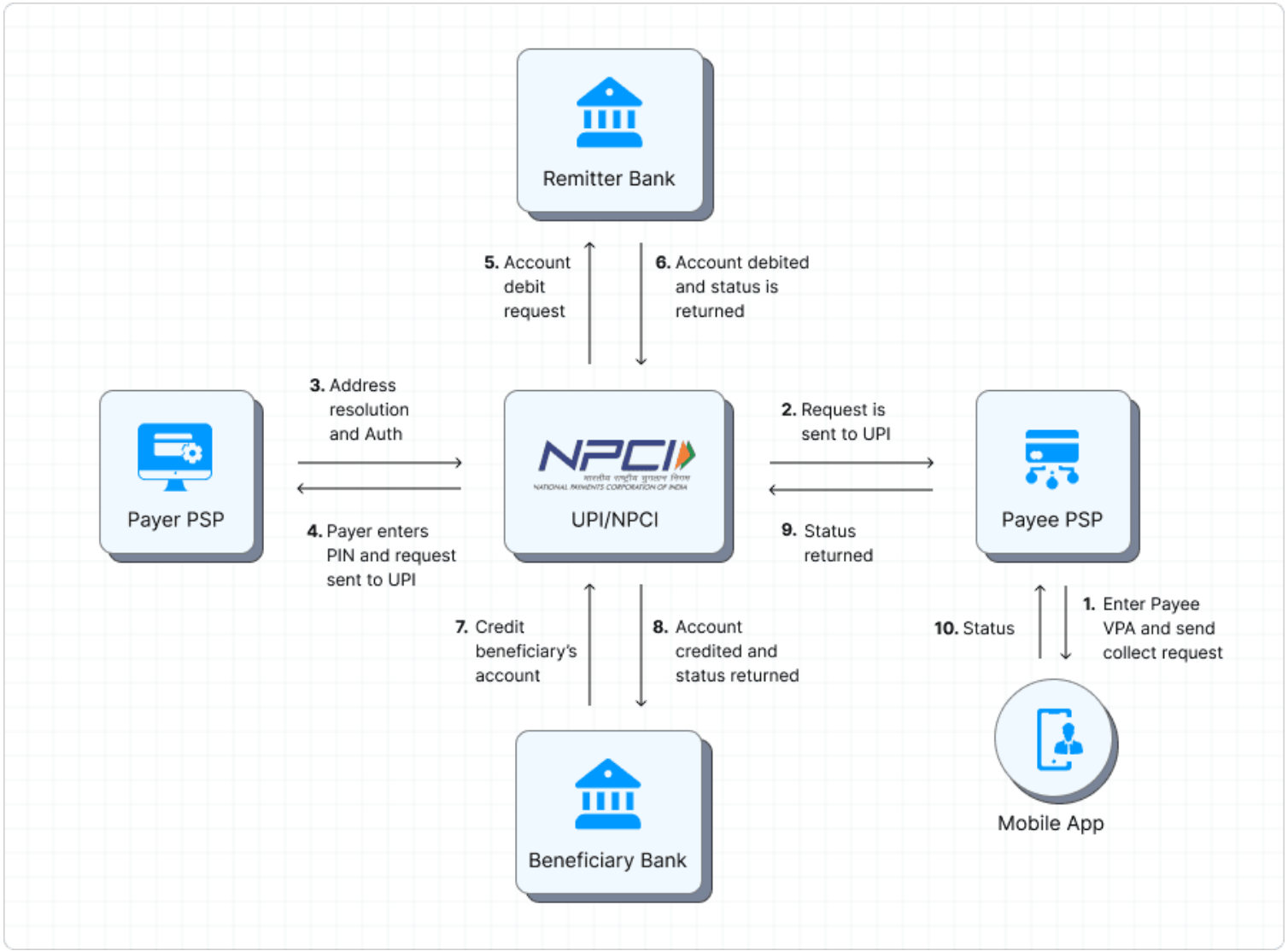
Case Study 1 – Accepting Deposits (contd.)

Validation sources and methods

- **Name** – CRM, Sanction list, OFAC, FIU-Ind, Global list & Internal list
- **Address** – Sanction list, OFAC, FIU-Ind, Global list & Internal list
- **Phone number** – FFRI, Global list & Internal list
- **Occupation type** – High cash, heavy losses, seasonal, casinos, online gaming, raincoat & umbrella, tourism, travels etc., - Internal list based on risk appetite of the top management
- **Officially Valid Documents (OVD) verification:**
  - ❑PAN – NSDL / Income tax portal (mandatory for non-individual)
  - ❑Aadhaar – UIDAI & Aadhar vault enabling
  - ❑CIN – MCA
  - ❑GSTIN – GST portal (cross verification with PAN)
  - ❑License no – Parivahan portal

Video KYC highlights

Hosted on-premise
VAPT & Security audit should be conducted by Cert-in empanelled auditors
Assisted V-CIP via Business Correspondent (BCs)
Geo-tagging (IP outside India should be blocked)
Anti-spoofing of IPs outside India
Liveness detection (to rule out pre-recorded videos or static images)
Encryption of entire interaction
Audit & storage



Payment request made via UPI

Key points to be noted while verifying NPCI payments

- Payer is authenticated and still active in the bank with sufficient funds
- Payees VPA is correct and valid
- Payee account is active while making payment
- Payments and receipts has to be reconciled on a daily basis
- Alerts to be generated for status of each transaction

Case Study 2 – Granting loan and advances

Lawful Basis and Specific Consent	Processing requires valid consent or legitimate use, preceded by a clear, independent notice detailing the purpose [14(1), 15(1), 18(1), 214(a)].
Data Quality and Correction	Ensure completeness, accuracy, and consistency of personal data used for making decisions that affect the Data Principal or for disclosure [32(3), 45(2)].
Accountability for Processing	The bank is responsible for compliance for all processing undertaken by it or by its Data Processor under a valid contract [31(1), 32(2)].
Data Retention and Erasure	Erase personal data when the specified purpose is no longer served, unless retention is necessary for compliance with any law (e.g., statutory record keeping) [34(7), 35(II)].
Log and Traffic Data Retention	Retain personal data, associated traffic data, and processing logs for a minimum period of one year from the date of processing.
Reasonable Security Safeguards	Implement appropriate technical and organisational measures, including encryption, access controls, monitoring, and data backups, to prevent data breaches [33(4), 33(5), 223(a), 223(b), 224(d)].

Digital Personal Data Protection

Scope of IS Audits

- ITGCs cover overall IT environment, focusing on infrastructure, security, and operational aspects.
- ITACs focus on individual applications. Input, Processing & Output
- Business Continuity Management (BCM)
- Network security
- Data migration focus on movement of data from source to destination
- IT Gap analysis and remediation

IS policy

It is a high-level business rule which defines the control that the organization must follow.



IS policy contents

It should contain the following basic points



E-mail policy template

Purpose

Scope

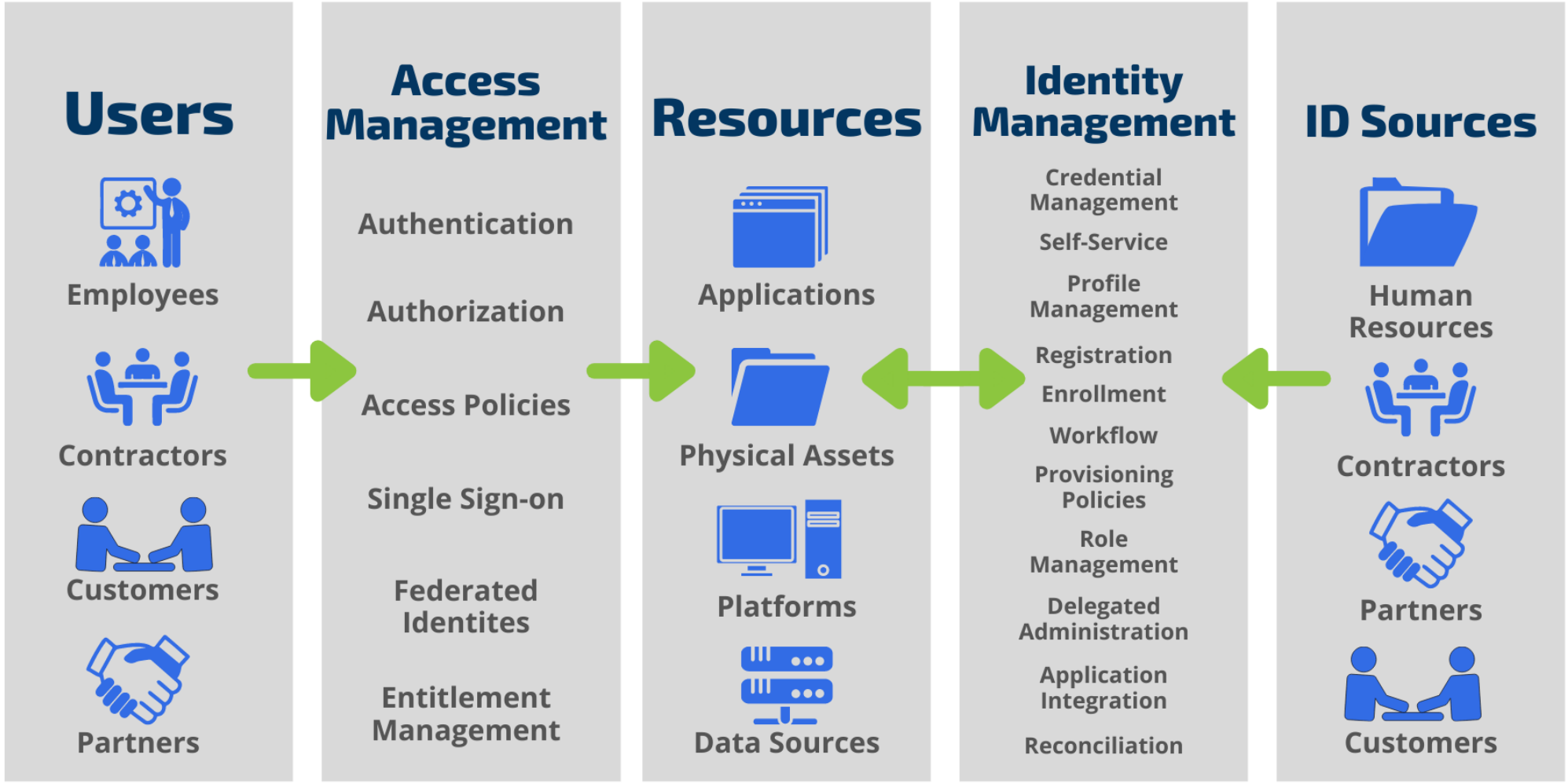
Consequence of non-compliance

Refer to standards & Procedures

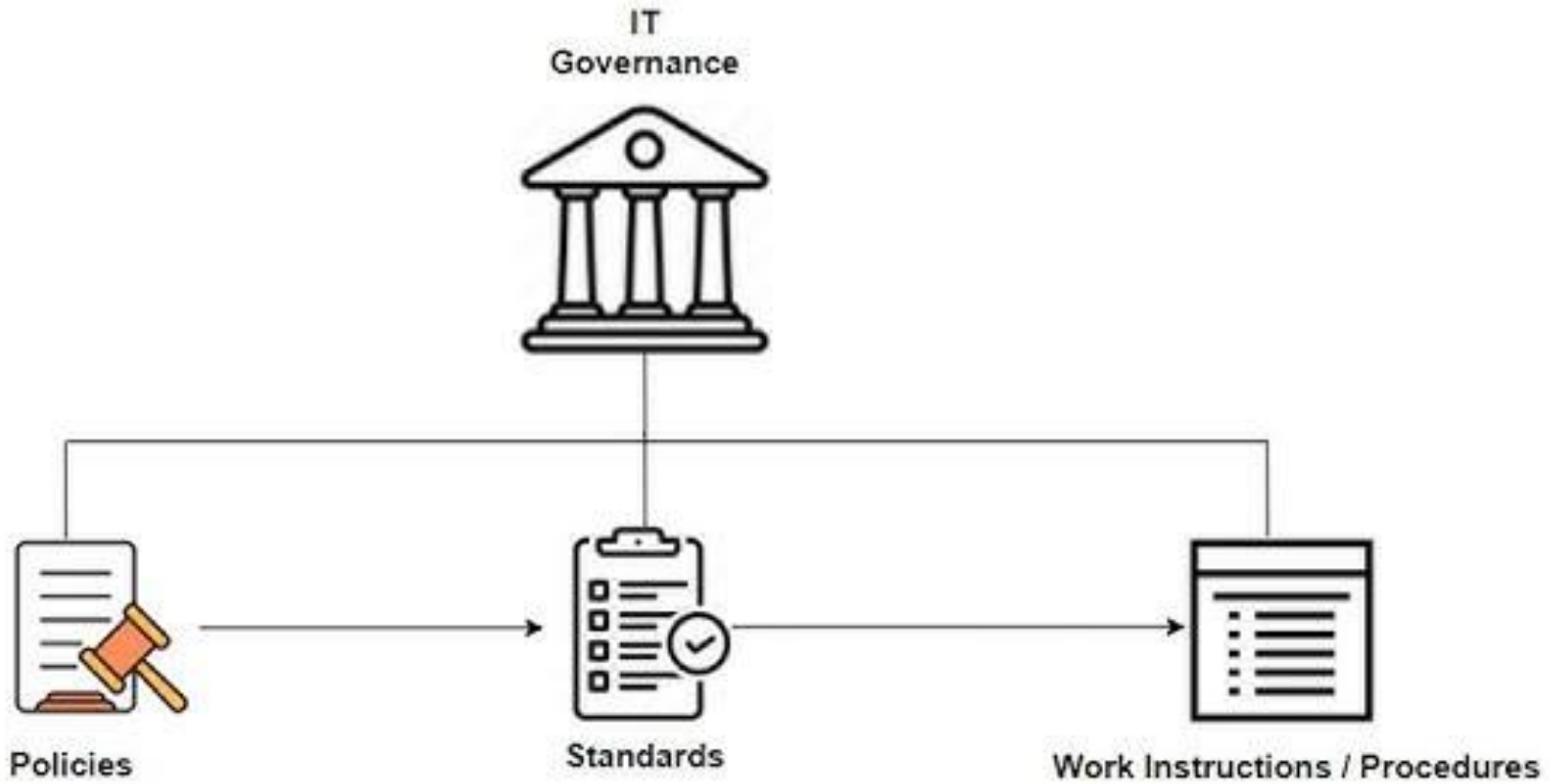
Approval

Revision history

Identity & Access Management



IT Governance Framework



Example

Let's break down the user password requirement example into a password policy, a corresponding standard, and a procedure document for implementation:

1. Password Policy:

Here's an example of what a password policy might include:-

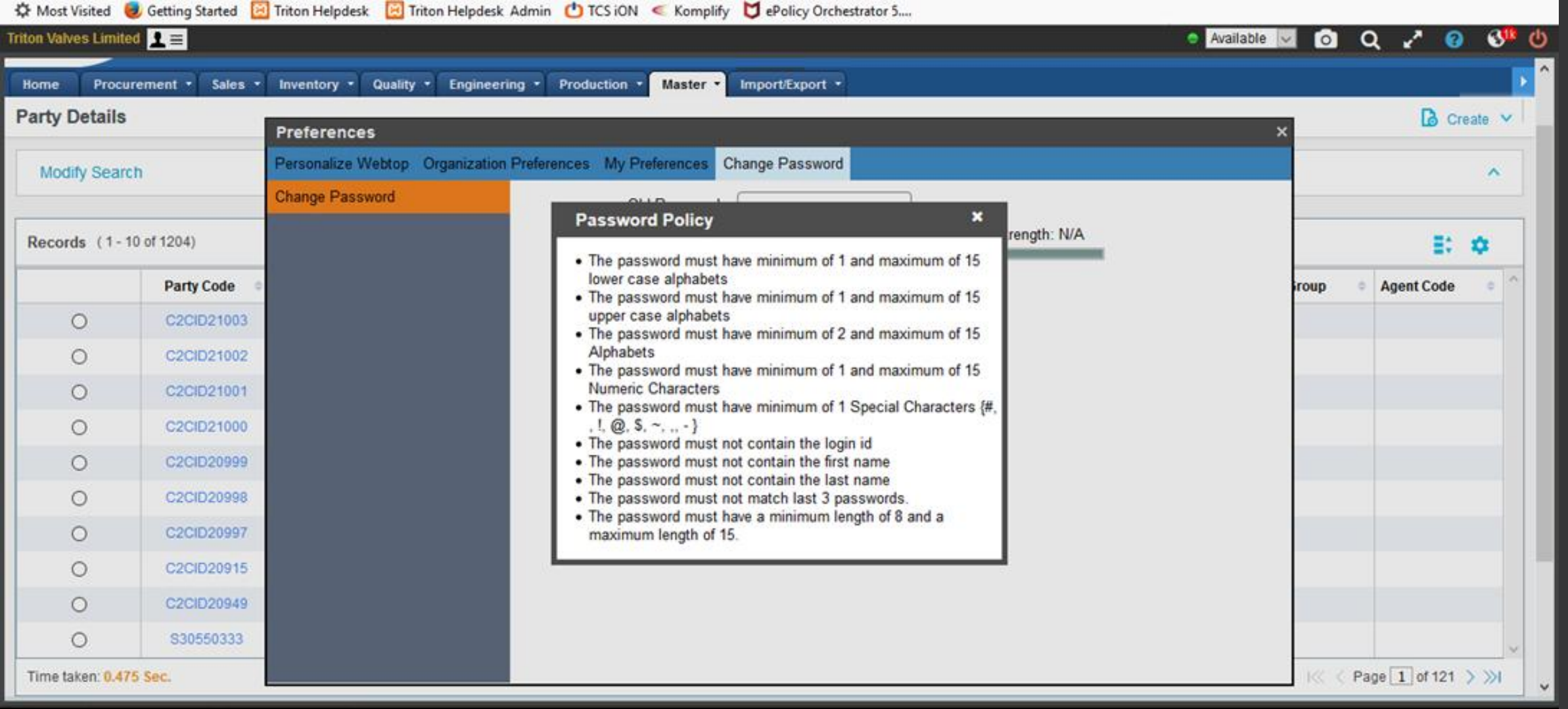
- Password Complexity: Passwords must meet certain complexity criteria, such as a minimum length, a combination of uppercase and lowercase letters, numbers, and special characters.
- Password Expiration: Passwords should have a predefined expiration period, after which users are prompted to change their passwords.-
- Password History: Users should not reuse their previous passwords within a specified number of password changes.
- Account Lockout: After a certain number of failed login attempts, user accounts should be locked temporarily to prevent brute-force attacks.
- Password Sharing: Users should not share their passwords with others or use the same password for multiple accounts.
- Password Storage: Passwords should be stored securely using encryption or hashing techniques.

2. Password Standard:

- Minimum Password Length: Passwords must be at least eight characters long.
- Complexity Requirements: Passwords must contain a combination of uppercase and lowercase letters, numbers, and special characters.
- Password Expiration: Passwords should expire every 90 days.
- Password History: Users should not reuse their previous five passwords.
- Account Lockout: After six consecutive failed login attempts, the user account should be locked for 15 minutes.
- Password Storage: Passwords should be stored using a one-way cryptographic hash function.

3. Password Procedure Document:

- Password Creation: Step-by-step instructions on creating a strong and secure password, including examples of acceptable password formats.
- Password Change: Guidelines on how to prompt users to change their passwords regularly, including instructions on providing password change reminders and notifications.
- Account Lockout Handling: Instructions on how to handle and unlock temporarily locked user accounts, including the duration of the lockout period and the steps to verify user identity.
- Password Reset: Guidelines on the password reset process, including user authentication methods and validation procedures.
- User Education: Recommendations on user training and awareness programs to promote password security practices and discourage password sharing.

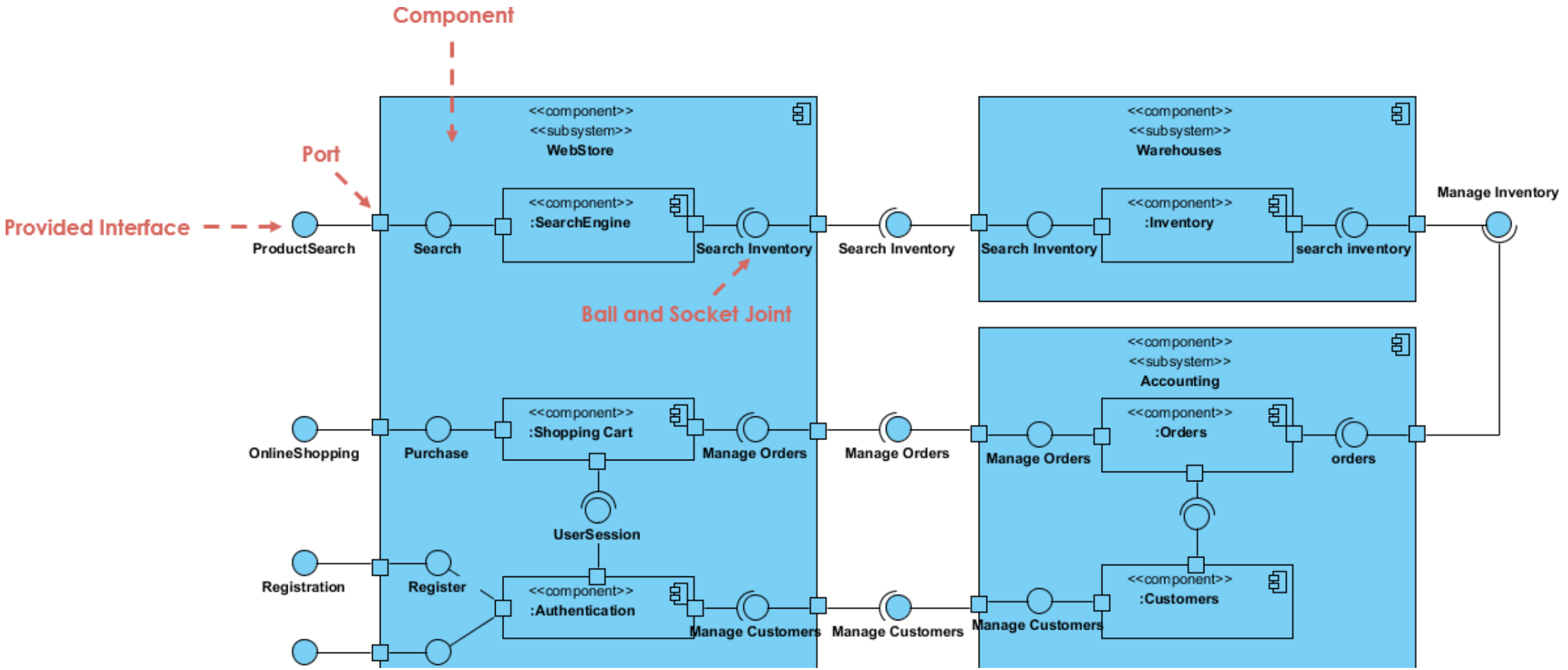


Logical access control – Password configuration

sph_id	sph_log_id	sph_service_id	sph_username	sph_curr_password	sph_new_password	sph_status
2986	30	17164	onx6rebiYG6QTQ9lAr0ZJw==	F3n9TWEUv/nNtJOAqhF1...	hTrAajKXQ7lb+z4VG26Cf4J751H...	True
2987	31	17165	3ofg+4mk7huxb/pw8AmH4...	F3n9TWEUv/nNtJOAqhF1...	kIo8ynuzNAUIzR5NRxKzESAZxf...	True
2988	32	17166	onx6rebiYG6QTQ9lAr0ZJw==	F3n9TWEUv/nNtJOAqhF1...	rX1+5UFJnxg/YrLyFpyxxg==	True
2989	33	17167	3ofg+4mk7huxb/pw8AmH4...	F3n9TWEUv/nNtJOAqhF1...	WO0KC9+qFRkVLTPX8mLCyWaK...	True
2990	34	17167	3ofg+4mk7huxb/pw8AmH4...	F3n9TWEUv/nNtJOAqhF1...	o4QR8HasgIgfERutlDmjZ6WL3vJ...	True
2991	35	17168	9NdUZWI3j+jSFZe+TQCRLg...	F3n9TWEUv/nNtJOAqhF1...	o4QR8HasgIgfERutlDmjZ6WL3vJ...	True
2992	36	17169	3ofg+4mk7huxb/pw8AmH4...	F3n9TWEUv/nNtJOAqhF1...	VrUVwk+QyuNPGozHQ8JLEhb32...	True
2993	37	17169	3ofg+4mk7huxb/pw8AmH4...	F3n9TWEUv/nNtJOAqhF1...	lOQqI0iLoczZdL86iVV505FXwHo1...	True
2994	38	17170	3ofg+4mk7huxb/pw8AmH4...	F3n9TWEUv/nNtJOAqhF1...	jzSJJWcmn8sq23KWhLS7CxSVE...	True
2995	39	17171	3ofg+4mk7huxb/pw8AmH4...	F3n9TWEUv/nNtJOAqhF1...	o4QR8HasgIgfERutlDmjZ6WL3vJ...	True

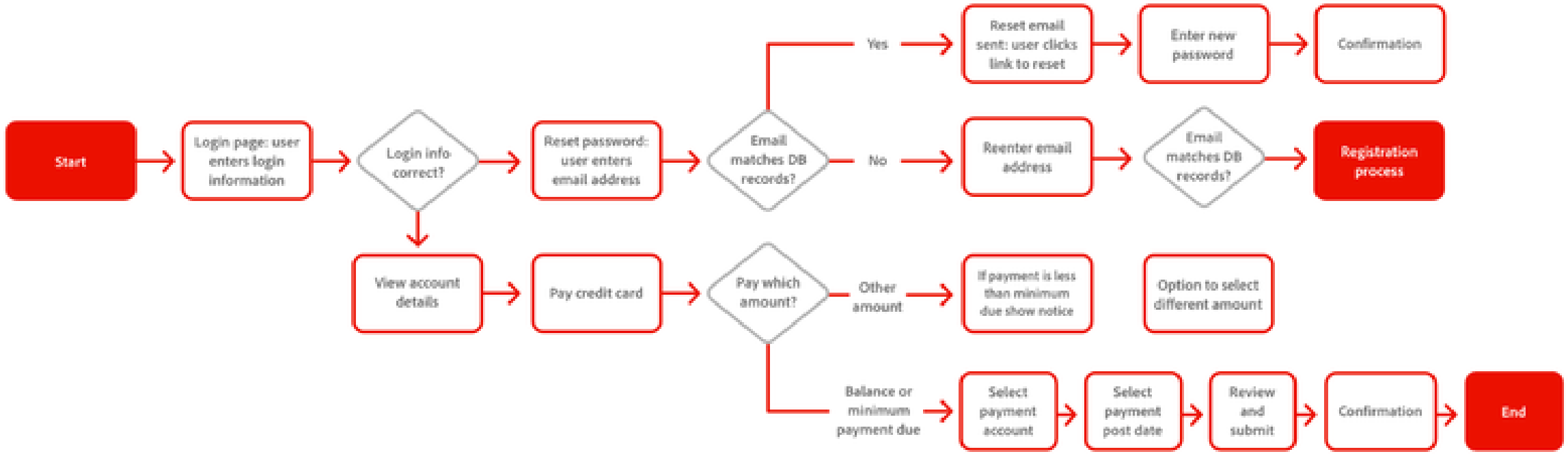
User ID	Password	Password hash value
ORACLE	ORACLE	38E38619A12E0257
ORADBA	ORADBAPASS	C37E732953A8ABDB
DBSNMP	DBSNMP	E066D214D5421CCC
DEMO	DEMO	4646116A123897CF
ADMIN	JETSPEED	CAC22318F162D597

Logical access control – Encryption



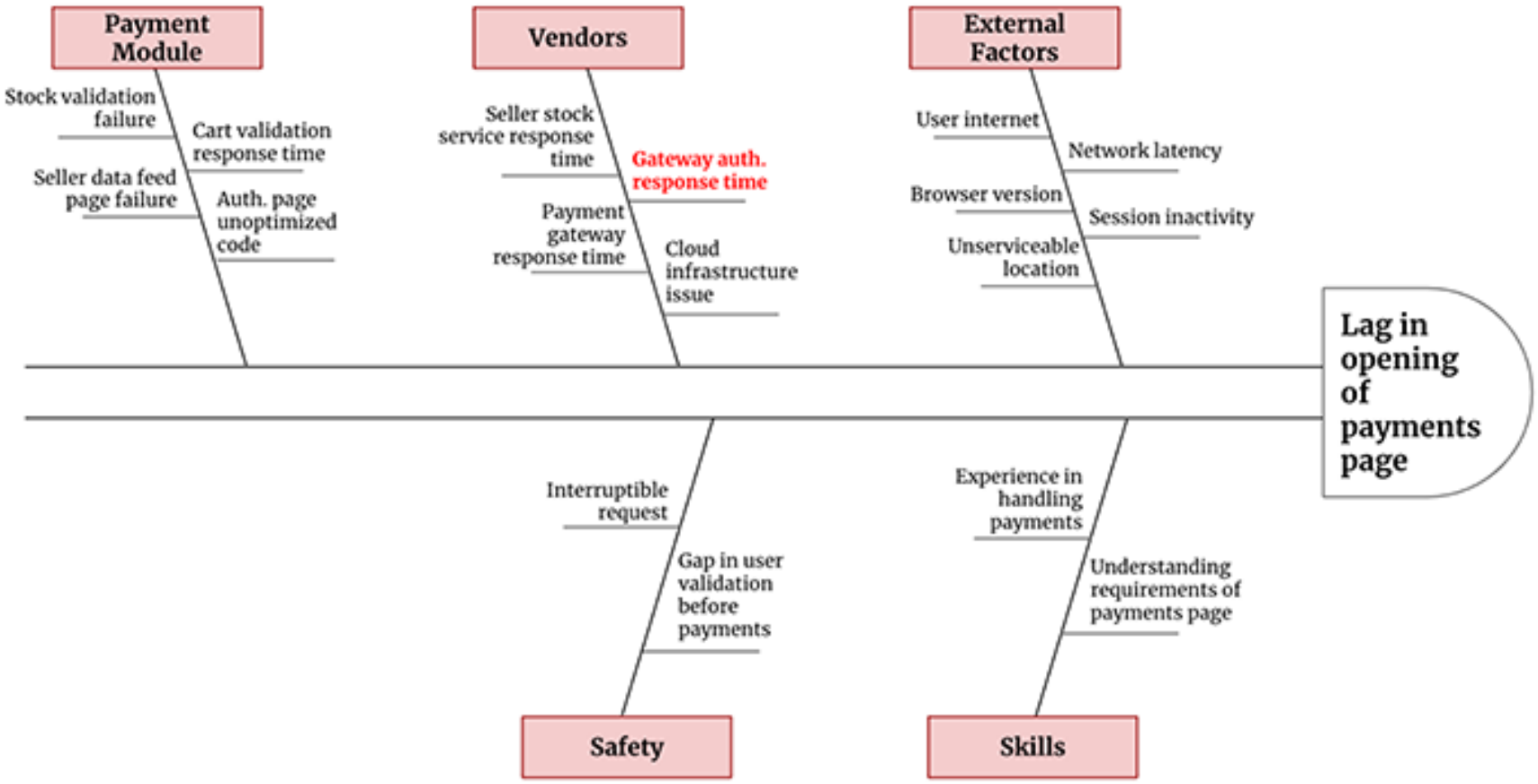
Process flow mapping – Component diagram

Process flow mapping



ISHIKAWA - RCA

Problem: Customers are facing lag while checking out from their cart. The app takes two minutes to move from the cart page to the payment page when a customer clicks on the continue button.



Q&A!



nagappankn8@gmail.com

THANK YOU!