ambitious baba .com
INDIA'S LARGEST TEST PREP PLATFORM

CAIIB PAPER-1
Module-D Unit-4

Advanced Bank Management (ABM)

CAIIB Paper 1 (ABM) Module D Unit 4: Framework for Identification of Compliance Issues and Compliance Risks

Introduction

- The banking landscape of India is changing rapidly.
- With the evolution of technology, the industry has undergone a massive transformation that has changed the way financial procedures are carried out, and the way financial institutions operate.
- The collaboration between finance and technology has led to a radical change in several aspects of banking.
- Financial technology is said to be a disruptive force that in the future is expected to reshape the financial sector, business models and banking structures.
- This paradigm change has posed significant challenges to the banks as well as the regulators.
- One of the important challenges is '**Compliance'**; a very important aspect for sustainable growth and become a success story for any banking and financial system.
- Compliance is defined as the act of following laws, rules, regulations, and various codes of conduct including the voluntary ones.
- Although most of these arise from external requirements, following the organisation's own internal rules, policies, and procedures, acting in accordance with ethical practices is equally important.

Compliance Issues

- The definition of compliance means following a rule or order.
- An example of compliance is when someone is told to go outside and they listen to the order.
- An example of compliance is when a financial report is prepared that adheres to standard accounting principles.
- Compliance issue means a single event during which any Accountable Employee is in violation of one or more processes **or procedures required under the Rules.**

Compliance Challenges in Present Times

- As the financial world gets more and more regulated every day, organisations are facing greater burden and stress to keep up with the pace of alterations and to comply with the evolving regulations.
- In 2020, the challenges of regulatory compliances will require latest technology and user-friendly strategies since the concepts like the geopolitical protectionism, the divergence in regulatory obligations, data processing, operational resilience, credit quality, shifts in capital, agility in compliance

procedures, financial crimes, customer trust, and ethical business would be some of the hot topics to be tackled effectively.

- With fast moving changes in the BFSI sector, e.g., Payment & Settlement system, banking products and processes, customers' expectations, and delivery system, there is a felt need to improvise the Compliance policies and implementation.

Some of the important challenges for the BFSI sector are:

Geopolitical Trends towards Nationalism

- As the popularity of "**globalisation**" started to fade away, the focus on protectionism, nationalism and sovereign rights re-emerged as an **"anti-"** movement and this created an uncertainty in the policy and regulation side as well.
- The change in the geopolitical area directly or indirectly affect the economic activities, trade businesses, monetary policies and eventually related regulations like Data Protection, KYC, beneficial ownership, etc.
- Therefore financial organisations must remain aware of what is to come and expect the disruptions in the process even if they think that they are addressing diverse policies and regulations and continuing to implement necessary changes.
- Another risk here is that in the countries of uncertainty, financial crime may thrive due to the facilities provided by the innovative technologies.
- Therefore financial organisations must remain aware of what is to come and expect the disruptions in the process even if they think that they are addressing diverse policies and regulations and continuing to implement necessary changes.
- Another risk here is that in the countries of uncertainty, financial crime may thrive due to the facilities provided by the innovative technologies.

Divergence in Regulation and the Need to "merge"

- The divergent nature of regulations thanks to local and global needs is to be understood and embraced by financial organisations and the term "merge the diverge" must be learned and adapted into their strategies.

The main areas of divergence are:

- Cybersecurity, data privacy regulation, servicing of loans, Customer and industry-related banking services
- Special regulatory and supervisory expectations to risk and complexity, deviating from global standards
- Innovative technological applications where new regulations may emerge
- Alignment with non-financial services and statutory regulators

Data Processing: Protection and Governance

- Financial services providers acknowledge data as something to be protected with governance and control within their organisation and through third-party organisations.

- Although the quality of data and the way it is used are the most important aspects in the protection of personal or operational information, data is perpetually captured, monitored, processed and shared.
- Since the breaches in data sharing continues, the expectations for more stringent data privacy and security regulations are increasing in both local and global levels

Operational Resilience: Be Ready for the Unexpected and Adapt to Changing Patterns

- For the process of business transformation for the sake of regulatory compliance, the ability of the financial institutions to adapt to changing environments is one of the key concepts.
- Regulators expect Banks & FIs to have a highly broad view of operational resilience by both controlling the operational risks and managing the disruptions.
- Therefore, they need to operate an integrated approach including continuity planning, operational risk, and concentration risk analysis.
- Also, the Banks & FIs need to take into consideration that outside sources like cyber-crimes, environmental aspects or socio-political changes might create threats or disruptions to their businesses so, they must be ready for these as well.

Risks Related to Credit Cycles

Financial institutions should learn from previous credit cycles and apply the learnings into their operations to prevent the potential risks which are related to:

- Risk layering and leveraged lending
- Expanded delivery channels and payment options
- New products and services and technology applications
- Disclosures via securities or trading activities, lending to non-depository institutions, or partnership arrangements**.**
- It is time to take on board the increasing risks arising out of Climate Change, increasing air and water pollution, and health of employees in big organisations funded by banks & FIs.
- These elements have direct impact on production cycles and productivity in agriculture and industries and supply chain management.
- Insurance companies can offer policies for Risk mitigation of such risks

Easing of Regulatory Capital and Liquidity Requirements

In some countries there is a trend in easing the buffers in the capital and liquidity requirements; however, this does not necessarily mean weakening risk management because it seems that the regulatory focus on managing these activities together with risk management will resume.

In this scenario, financial institutions should expect:

- Upcoming final rulemakings for banks and nonbank entities
- Emphasis on governance over capital planning
- Creating a regulatory focus on capital and liquidity frameworks
- business strategies of the organisations change accordingly giving more attention to c**onsumer protection risks including privacy, accessibility, and prejudice** by taking AI and cloud systems into consideration.
- Eventually, the firms will bear the responsibility to understand the technological applications and their outcomes.
- On top of this, the challenges on the compliance side will remain in the centre of areas like **financial crimes, ethics, customer data protection, and geopolitical shifts.**

Fine Line in between Innovation and Financial Crime

- As the beneficial side of technology is undeniable for the financial organisations to deliver better service and value to their customers, it is also giving way to financial crimes and fraud.
- There is a huge regulatory pressure on Banking and Non-Banking **finance companies to work to identify the risks for the crimes.**
- The adoption of innovations to prevent these crimes like AI, fintech, or other cosourcing arrangements is accepted and supported the regulatory authorities.
- However, since the volume of data, diversity, and number of sources and control of data is hard to navigate, the companies are still struggling with these.

Building Consumer Trust

- The customer-centric business model involves a personalised service experience, mobility in between channels, data privacy, evidence of good corporate citizenship, and fair value.
- This is the model needed by financial service companies to build a loyalty-based relationship with their customers and it gained more importance in this evolving environment.
- Personal data protection is also at the centre of regulations as topics like use and/or sale of data for marketing purposes and similarly, data ownership and control are still hot topics when it comes to privacy concerns in the digital era.

Ethics in Business

- Financial companies are also expected to identify and prevent unethical conducts as stated by the regulations.
- Monitoring, surveillance, reporting, and governance will be added to the frameworks of misconduct identification procedures.
- The main points of concern will be personal data privacy, sales processes, fair treatment, incentive plans, market conduct, and third-party oversight, etc.
- These challenges on one hand would require extensive use of latest technological tools like AI, IOT, Data Analytics, Block Chain technology **and**

more and on the other hand upgrade in Skills set of employees at all levels.

COMPLIANCE RISK

The Basel Committee on Compliance Function defines Compliance risk as "the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its banking activities" (together, "compliance laws, rules and standards").

Identification of compliance risk

***Some common compliance risks include*:**

- Corruption
- Employee Behaviour
- Workplace Health and Safety
- Environmental Impact
- Data Management
- Quality
- Process
- Social Responsibility.

The level of Compliance Risk in each business line, products and processes shall be identified based on:

- ❑ Regulatory Focus
- ❑ Customer Service aspect
- ❑ Control aspects
- ❑ Nature of activity – Whether inherently high risk in nature
- ❑ Bank's exposure to it – materiality
- ❑ Any major breaches reported in the past-history
- ❑ Penalty implications
- ❑ The Bank should put in place 'New product approval process". The Compliance department through New product approval process shall ensure that Compliance Risk in all new products and processes introduced get identified and appropriate risk mitigants are put in place before launching the same.
- ❑ The Compliance officer shall be a member of the "New product approval Committee" of the Bank.
- ❑ The Chief Compliance officer shall necessarily be a participant in the quarterly informal discussions held with RBI. The CCO shall continuously

- ❑ keep contact with SSM, RBI & team for issues related to compliance, regular reporting and submitting information if any.
- ❑ *The Compliance staff shall be empowered to have access to information required, to conduct compliance reviews/investigations.
- ❑ Staff accountability shall be examined for all compliance failures. Moreover, Bank shall endeavor to design a suitable system to give due weightage to the record of compliance during performance appraisal of all staff members.
- ❑ Principles of compliances management

Being one of the key elements in the bank's Corporate Governance Structure, the Compliance function shall be:

- ✓ Independent and sufficiently resourced.
- ✓ Its responsibilities shall be clearly defined.
- ✓ Its activities shall be subject to periodic and independent review by the internal audit function.
- ✓ Compliance function shall be regarded as a Core Risk management activity within the bank and shall not be outsourced.

Compliance Risk Management Function

- Historically the compliance function did not understand and model processes for risk management.
- Compliance documented and met requirements, and found and resolved issues.
- There was limited modeling of compliance issues and risk to determine business impact and prioritisation of resources.
- Most often compliance was reactive, putting out fires instead of actively interpreting and predicting compliance and ethics risk issues, and developing treatment plans to mitigate or avoid damage to the organisation. The present day approach is a risk based and due diligence is also essential.
- Due diligence is when an organisation is able to demonstrate that it had been duly diligent in meeting its obligations through developing, implementing and maintaining a management system.

The following points are critical to proving this due diligence:

- ✓ Systems must be "effective" and not "paper", "legalistic" systems.
- ✓ Systems that emphasises results not process.
- ✓ Systems are procedures that are in place and working procedures that outline what staff should do.

Essential ingredients of due diligence are:

- ✓ Real commitment to compliance.
- ✓ Culture in the Business (a pro-active culture that is not just about lip service)

- ✓ Consistent & effective enforcement – discipline, investigative, corrective/preventative action.
- ✓ Full and effective reporting and action on reports.
- ✓ Making sufficient resources available.
- ✓ Be satisfied system actually working – audits, monitor, inspect.
- ✓ Identify and assess requirements as they impact your business.
- ✓ Outsourcing/contractual obligations – establish required standard and monitor.
- ✓ Identify/analysis of risk exposure and manage/control.
- ✓ Measure/assess level of compliance.

The complete risk management function can be detailed as under:

- ✓ On a pro-active basis, to identify, document and assess the compliance risks associated with the Bank's business activities, including the development of new products and business practices, the proposed establishment of new types of business or customer relationships, or material changes in the nature of such relationships;
- ✓ To assist and advise all committees on operations related integrity and reputational issues, including – among others – checks on borrowing clients, project sponsors and other partners upon request;
- ✓ Under the guidance of the CMD the Head of the Internal audit & Compliance department shall lead and co-ordinate investigations into alleged unsatisfactory conduct or misconduct of Bank employees or consultants, and, where appropriate, recommend disciplinary or corrective action;
- ✓ To deal with and lead and co-ordinate investigations into issues of conflict of interest (of the Bank, staff, etc.), cases of alleged corruption, money laundering, terrorist financing, and complaints received with regard to Bank-financed operations;
- ✓ To consider ways to measure compliance risk and use such measurements to enhance compliance risk assessment;
- ✓ To assess the appropriateness and consistency of the Banks regulatory framework (statutory documents, policies, strategies, guidelines, **rules, regulations and procedures in force) related to compliance issues, promptly following up any identified deficiencies in the policies and procedures and, where necessary, formulating proposals for amendments;**
- ✓ To ascertain compliance with the provisions of the Banks Code of Conduct, to review and propose amendments to the Banks Code of Conduct and other policies and procedures, as necessary, to reflect ethical standards in all areas;
- ✓ The responsibilities of the compliance function shall be carried out under a risk based annual compliance programme that sets out its planned activities, subject to oversight by the head of compliance to ensure appropriate coverage and co-ordination among risk management functions.

Inherent Risk And Control Risk

- ✓ We can define inherent risks as the risk to a company in the absence of any security controls or actions that might be taken to alter, mitigate, or reduce

either the likelihood or impact of a data loss. In other words, the inherent risk of a system is the risk that the system poses "**out of the box,"** before any processes, technologies, or people are put in place. Inherent risk is somewhat akin to operation risk.

- ✓ It is a function of threats and vulnerability.
- ✓ **Inherent Risk = Threats × vulnerability**.
- ✓ Residual risk is a function of inherent and control risk and be defined as 'The probability of loss that remains to systems that store, process, or transmit information after security measures or controls have been implemented.
- ✓ Implemented controls may include best practice control frameworks'**. Residual Risk = Inherent Risk × Control Risk,**
- ✓ a great example to illustrate the difference between inherent risk and residual risk is walking across the street.
- ✓ If you cross the street, there are a nearly infinite number of inherent risks.
- ✓ One of the inherent risks with a high probability and large impact would be getting hit by a car.

Some of the Inherent Risks and the Control are Discussed Below

Credit risk

Basic policies

- ✓ Credit risk is inherent in many banking activities and may lead to losses when the Bank's customers experience deterioration in financial condition, making it impossible to recover principal and interest on loans, securities, and other monetary claims outstanding.
- ✓ Management of this type of risk is the most fundamental task in banking operations.
- ✓ The Bank places the highest priority on ensuring the soundness of its assets and works to continually enhance its credit risk management capabilities.

Credit analysis Systems

- ✓ The fundamental pillars of the Bank's credit risk management systems are its credit rating system for ranking its customers and the self-assessment system.
- ✓ These systems are employed in quantifying credit risk and in setting various lending policies.

Market risk

Basic policy

- ✓ Market risk refers to the possibility that banks may incur losses due to movements in interest rates, foreign currency exchange rates, stock prices, and/or other market-related indicators.
- ✓ Market risk is defined to include credit risk inherent in market transactions that may lead to losses when counterparties fail to meet their obligations.

- ✓ The Bank conducts strict management and control of market risk based on the awareness that the possibility of substantial losses is inherent in the nature of market transactions.

Market Risk Management System

- ✓ The risk volumes in the Bank's operations (limits on the maximum volume of risk and loss limits) are decided by the Board of directors and the Executive Committee.
- ✓ Units engaging in market transactions conduct their operations within the various limits that have been assigned to them, based on the decisions of the Executive Committee.
- ✓ The results of operations and profit/loss are reported on a daily basis to the directors in charge, and reports are presented to the Executive Committee each month.

Liquidity risk

Basic policy

- ✓ Liquidity risk is the risk that a financial institution may run short of funds, owing to a decline in its creditworthiness or an extreme gap between its maturities in inflow and outflow of funds, and may therefore have to pay prohibitively high interest rates to bridge the gap.
- ✓ The Banks have recognised the management of liquidity risk to be a basic and vital aspect of its operations and developed effective monitoring systems to ensure sufficient liquidity to meet its needs.

Specific Liquidity Risk Management Activities

- ✓ To manage liquidity risk, the Bank first periodically examines the structure of fund sources and uses and implements measures **needed to improve this structure.**
- ✓ In addition, taking into consideration the size of assets, the Bank's funding capabilities, and other factors, guidelines are established for the funds gap (the amount of funds that must be raised).
- ✓ Through these and other activities, the Bank works to structure systems to prevent unforeseen developments**.**

Liquidity Risk Management Systems

- ✓ Information on the funds gap, the market environment, and other matters related to liquidity risk is reported by all units involved in managing the Bank's cash flow to the Risk management department, which is in overall charge of managing the cash flow.
- ✓ Reports on the overall cash flow are made periodically to the Executive Committee.
- ✓ In the event a sudden change in the market funding environment leads to the emergence of a possible liquidity shortage, the Banks have contingency plans to respond flexibly and quickly in response to the seriousness of the emergency.

Operations Risk

Basic policy

- ✓ Operations risk is inherent in the handling of customer transactions, and errors, unethical conduct, and certain other circumstances that may lead to losses.
- ✓ Typical examples are disparities between actual cash and cash balances and customer complaints concerning transactions.
- ✓ Accurate and rapid fulfilment of transactions requested by customers is the foundation of trust in the Bank's services, and, as banking activities become more diverse, proper management of these activities to lessen and minimise operations risk is essential.

Operations Risk Management Systems

- ✓ The Bank should have established the operations department to be in overall charge of operations risk management.
- ✓ The department's activities include improving operating procedures and implementing systems upgrades as well as supervising branch operations and providing specific guidance.
- ✓ In addition, the Bank has set up the Inspection department to perform internal checking functions, and this department conducts examinations and provides guidance to prevent operations problems before they occur at all the Bank's offices, including overseas offices and operations centres.

Systems risk

Basic policy and Risk Management Systems

- ✓ Systems risk is inherent in computer systems, and losses as well as damages may be incurred owing to malfunctions and unethical conduct.
- ✓ For financial institutions, which are highly dependent on these systems, there is a possibility that systems risk may have an impact on society at large.
- ✓ Systems risk is, therefore, one form of risk that may have a major impact on management.
- ✓ Aware of this, the Bank does not regard the management of systems risk as simply a systemic or technological issue but, as one form of management risk, is working to supervise and control it as part of a unified, bank wide management system.
- ✓ Specific activities Specific measures for the management of systems risk have included the installation of multiple telecommunications lines for online operations and backup computer centres to prevent systems failures and prepare for possible natural disasters.
- ✓ In addition, the Bank has established the System office within the planning department, which is responsible for undertaking periodic monitoring based on fundamental policies for Bank wide systems risk management.
- ✓ Compliance Risk Assessment is the process of assessing the level of compliance of regulatory directives impacting the banks and the major compliance risks faced by the bank.

- ✓ For better understanding, we may identify few areas related to, observations in Regulatory Examination reports, Compliance testing, implementation of regulatory guidelines, regulatory reporting, enhancing compliance culture, etc.
- ✓ Further at overseas establishments few parameters covering regulatory examination reports, enforcement action, closure of the audit reports, implementation of regulatory guidelines, regulatory reporting, AML CFT compliance, training, etc., may be taken.

Accordingly, the compliance risk score can be assessed on a scale of 1–10 as per table below

Compliance Risk Score	Compliance Risk Level
7.1- 10	Needs significant improvement
5.1- 7	Needs improvement
3.1- 5	Meets requirement
1-3	Well controlled

Based on the results of the Compliance Risk assessment, a plan may be prepared to mitigate the risks with actions:

- To conduct assessment of the compliance risk activity-wise (at least once a year) and to develop a risk-oriented activity plan for compliance assessment. The activity plan should be submitted to the ACB for approval and be made available to the internal audit.
- To report promptly to the Board/ACB/MD & CEO about any major changes/observations relating to the compliance risk.
- To periodically report on compliance failures/breaches to the Board/ACB and circulating to the concerned functional heads.
- To examine sustenance of compliance as an integral part of compliance testing and annual compliance assessment exercise.
- To ensure compliance of Supervisory observations made by RBI and/or any other directions in both letter and spirit in a time bound and sustainable manner.

Independent Testing and Effective Audit Programme

Compliance units in banks may evaluate the compliance risk in each business line at periodical intervals and put up the results to the Board/Management Committee.

An effective audit programme is the key to a successful compliance policy. Its key components are:

- Have appropriate policy for the institutions risk profile
- Cover all applicable regulations and guidance
- Have effective scoping and planning
- Ensure adequate transaction testing
- Have no gaps in the program – program covers all appropriate areas

- Be well-organised with work papers
- Establish clear paper trails
- Communicate exceptions effectively
- Identify violations and explain risks
- Recommend appropriate corrective action
- Track corrective action
- Communicate results to Board of directors/audit Committee and senior management
- Document resolution of audit observations not carried to audit report.

On the other hand to have an efficient and effective compliance policy it needs to:

- Document your understanding of the AML risk profile
- Identify high risk services, products and clients
- Identify new regulations and regulatory guidance issued since prior audit
- Consider results of the most recent audit and regulatory examinations
- Consider results of other independent or self-compliance reviews
- Identify resolution of past recommendations

Consider factors that have changed since prior audit, such as:

- Changes to organisation's risk profile since last audit
- Changes in the compliance function since prior audit
- New regulations introduced since the prior audit
- New regulatory guidelines issued since the prior audit
- IT enhancements introduced
- Changes in monitoring parameters
- Changes in key compliance and operation staff
- New products or services

The success of a compliance policy needs a system of independent testing of the existing policies/ procedures/activities.

The areas/activities to be tested are:

- Adequacy of policies and procedures
- Ensure comprehensive test procedures
- Adequacy of High Risk Customer identification
- Adequacy of Customer due diligence (CDD)
- Adequacy of Enhanced Due Diligence (EDD) and compliance with documented policies and procedures
- Adequacy of Customer Identification Program (CIP)
- Adequacy of Internal Controls and Reporting
- Investigation and suspicious activity monitoring process
- Reporting & Record keeping
- Bank Risk assessment
- Cash activities and Cash Transaction Reports (CTRs)

- Cash aggregation, ATM transactions Track & monitor Corrective actions
- Track all actionable issues
- Document responsibility for resolution of issues
- Ensure completeness of corrective action
- Validate closure of audit issues
- Maintain adequate support on all closed issues

Where the corrective action involves the implementation of a new system, validate successful implementation and ensure data integrity audit Resources & auditor's expertise

- Independent audit Function within the Institution
- Head office audit (Foreign Financial Institutions)
- Outside audit firm
- Staff performing the testing should possess the expertise to assess **compliance regulations – Technical expertise – Specialised training – Familiar with new regulations/guidance**

Reporting Framework And Monitoring Compliance

Effective implementation and monitoring of compliance function calls for proper reporting framework. The reporting system is devised considering the changes in the organisational structure. Reporting framework may be structured on following lines:

Reporting of status/extent of compliance

(i)	Gist of the Reporting System	Gist of the Reporting System Submitted by & to	Periodicity
(ii)	Certificate by the branches and other operating units confirming compliance to all regulatory/ statutory/internal guidelines including a separate certificate for KYC and AML compliance.	Branches to RO/ ZO. Note: RO/ZO to make the copy of the certificate available to Risk officer for test checking on random basis.	Quarterly as on last working day of the quarter within 5 days of closure of the quarter
(iii)	Based on certificate from branches, a consolidated Certificate by RO/ZO confirming compliance to various regulatory/internal guidelines	RO/ZO to Compliance department at Central office on quarterly basis. RO/ZO to make the copy of the certificate available to Risk officer for test checking on random basis.	Quarterly within 10 days of closure of quarter.
(iv)	Certificate by Functional departments at HO/ Corporate Office confirming compliance with regulatory/statutory guidelines and RBI/ MOF circulars to the extent applicable to their Functional area For giving such certificate, basis will be the list of compliance issues already sent and RBI/MOF circulars sent during the quarter.	Head of Functional department to Compliance department.	Quarterly within 10 days of closure of the quarter.
(v)	Certificate by overseas Branch(es) confirming compliance with local laws, statutory/regulatory guidelines applicable to the respective countries to Compliance Department, Corporate Office/ HO	From overseas Branch(es) to Compliance department, Chief Executive of the Centre with a copy to International Dept H.O.	Monthly within in 5 days of completion of month.

Reporting of breaches/non-compliances

- Wherever breaches/non-compliances are observed, the same should be reported in the structured format as approved vide compliance policy and the same should be sent Compliance department at Central office with a copy to FGMO and respective Functional department.
- Ro should make the copy of the certificate available to Risk officer for test checking on random basis.
- Such breaches/non-compliances can be reported not only on the basis of reporting by the branches but also by the RO/ZO officials as observed during their visit or through audit report or through survey conducted for specific compliance issue.
- Functional depts. at Central office shall also report non-compliance/ breaches observed by them to CCO, Compliance department at HO.
- Similar reporting system should be followed for reporting of breaches/ non-compliances as regards overseas branches. Also, audit dept. should provide to the Compliance dept. a copy of its Report on breaches observed during the branch audit furnished to the controlling Regional office.

Framework for Test Checking on Random Basis

- Based on compliance certification received from the branches, Compliance deptt. should identify on random basis the branches/departments for independent compliance testing and see the correctness of the certification.
- While selecting the sample size, the level of compliance risk as assessed through the following parameters shall be kept in mind.

✓ Based on regulatory focus
✓ Whether the activity inherently have high risk?
✓ Bank's exposure to it.
✓ Whether any major Breaches are reported in the past?
✓ Care should be taken to ensure that branches in the sample are not repeated each time.
✓ KYC AML norms/compliance at branch level

Role Of Inspection and Audit

- An inspection is typically something that involves a visit to the site and is required to be done as part of compliance obligation.
- An audit is the process of checking that compliance obligations have been met, including that the required inspections have been done. In general, inspections deal with things that can cause immediate accidents or other problems, while audits cover the root causes of these problems.
- These are both vital processes.

The Checker Software will help a great deal in streamlining and maximizing the value to an organisation.

Types of Audits

✓ Risk Based Internal Audit
✓ Concurrent Audit
✓ Statutory Audit & Tax Audit
✓ Credit Audit
✓ Forensic Audit
✓ RBI Inspections
✓ System Audit
✓ Stock Audit
✓ Foreign Exchange Audit
✓ Snap Audit

- Banks conduct Risk Based Internal Audit thru their Inspection & Audit Departments.
- Internal auditors during their inspection should continue to capture breaches/non-compliances and report the same to the Chief Compliance Officer, at Head office of the bank under copy to Risk management department at administrative/controlling offices

- Risk management department at administrative offices should make use of such reporting from audit during their random sample testing of compliances.

The role of the audit committee shall include the following:

- ✓ It should provide direction and oversee the operations of the total audit function in the bank and maintain quality of internal audit and inspection
- ✓ Follow up on the observations of statutory audit of the bank and inspection (ISE) of the Reserve Bank of India.
- ✓ Strengthening housekeeping.
- ✓ Fixing accountability of inspecting/auditing officials for failure to detect serious irregularities.
- ✓ Periodical review of the accounting policies/internal control systems in the bank with a view to ensuring greater transparency in the bank's accounts.
- ✓ Sensitizing the Board about risk prone areas.
- ✓ Review of Risk management measures to mitigate the risk.
- ✓ Ensure implementation of various statutory compliances applicable to the bank.

The audit Committee should have discussions with the auditors periodically about internal control systems, the scope of audit including the observations of the auditors and review the quarterly, half-yearly and annual financial statements before submission to the Board and also ensure compliance of internal control systems.

The audit Committee shall have authority to investigate into any matter in relation to the items specified in this section or referred to it by the Board and for this purpose, shall have full access to information contained in the records of the company and external professional advice, if necessary.


CAIIB
NEW
SYLLABUS
Video Course
Mock Tests
Capsule PDFs
New Syllabus
JOIN NOW
Visit us for more information