ambitious baba .com
INDIA'S LARGEST TEST PREP PLATFORM

CAIIB PAPER-1
Module-D Unit-5

Advanced Bank Management (ABM)

CAIIB Paper 1 (ABM) Module D Unit 5 - Compliance Culture and GRC Framework

How To Create Compliance Culture Across the Organisation

- A culture of compliance is crucial for growth and profitability of an organisation.
- Compliance must be visibly embraced by senior management and built into the hiring and training process.
- Ideally, it should be linked to pay and promotions as well.
- Moreover, the right metrics can make the culture of compliance concrete.

It is important to address such questions as:

- ✓ Who delivers the compliance message – line or staff?
- ✓ How seniors are the messengers?
- ✓ How often do they address compliance issues?

- **Culture, like other aspects of compliance processes, can be managed and measured over time.**

Compliance Culture & Its Significance

- "Compliance culture" today represents the next generation of corporate compliance and ethics programs.
- Regulators, legal scholars, and businesses are urging organisations to develop a culture of compliance that aligns with external laws, internal policies, and increasingly with the ethical values.

Compliance Culture: can be defined as:

- ❑ "Workplace behavior that naturally meets ethical and legal norms.
- ❑ Compliance is adhering to established norms, which take the form of external laws, internal policies, and ethical values.
- ❑ Values depend on the organisation, but can take the form of things like reputation and employees' personal ethics and goals.
- ❑ Regulators are most concerned with an organisation meeting external laws and related policies whereas board members, employees, and **the public expect compliance according to internal policies and values,**
- ❑ Culture provides the foundation that shapes employee decisions in the moment.
- ❑ Culture informs compliance decision making through explicit and implicit reference to organisational values, norms and assumptions**.**

- In other words, employee decisions are made implicitly, or naturally, through the influence of corporate culture.
- A strong compliance culture should ensure adherence to fair practice codes, manage conflicts of interests, and treat customers fairly, with the larger objective of delivering efficient customer service.
- Thus, compliance shall go beyond what is legally binding and embrace broader standards of integrity and ethical conduct.
- The responsibilities of the Compliance Function are to be carried out under a Compliance programme that sets out its planned activities such as the review of compliance risk assessment in specific products/ processes for which Regulator attaches importance compliance testing and educating staff on compliance matters/activities.

Benefits of Good Compliance Culture:

It is important for banks and Financial Institutions to demonstrate a good compliance culture to retain their reputation and win the trust of customers, investors, other stakeholders, employees and regulators.

A good compliance culture can benefit banks in several ways which includes:

- ✓ Low organisational and individual risk;
- ✓ Low reputational risk;
- ✓ Increased confidence among employees while performing their jobs
- ✓ Helps attract and retain talent and ensure employees engagement.
- ✓ Improved transparency which enables better decisions;
- ✓ Enhanced relationship with regulators and other stakeholders and
- ✓ Enhanced valuation among investors;

Banks which have undergone the stress testing program reported that top most benefits of complying with stress testing principles are better informed capital planning decisions, and maintaining a forward-looking view of the organisation's risks.

Banks, therefore, need to embrace compliance if they want customer satisfaction which eventually leads to better Return on Equity.

Sign of Poor Culture

- ✓ Focusing on short-term profitability, including personal interests, with little or no consideration for the long-term interest of the entity.
- ✓ Dominance of individuals in decision making forums and lack of challenge.
- ✓ Sub-Cultures, which are not aligned with the organisational culture (especially during acquisitions/ mergers):
- ✓ Adherence to the letter of law/regulation, but not spirit (tick-box attitude)
- ✓ Treating internal control/risk management framework as an irritant and breaching them at will for short-term benefits.
- ✓ Ineffective incentive structures vis-a-vis poor management of risks;

- ✓ Tendency to cover up the problems, rather law/regulation than resolving the underlying causes of the problems.
- ✓ Follow the market attitude.
- ✓ Employees are not encouraged or reluctant to speak out when they have concerns about the way in which the entity operates; and
- ✓ Failing to challenge the status quo and consider alternative viewpoints resulting in a false sense of security and the risk blind spots

Costs of poor Compliance Culture:

- Compliance risk is 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. For better compliance culture a list of do's and don'ts must be created for all employees.

Banks should also:

- ✓ Convert misconducts and violations into Case studies to be disseminated among the staff for education and entrenchment of desired attitudes.
- ✓ Eschew the tendency to treat compliance merely as cost and should recognise that proper conduct saves the bank from possible reputational loss and penalties – thus, generates hidden earnings **which most banks do not quantify, and hence do not realise.**

The risk of RBI Penalties arises due to noncompliance of

- ✓ Prudential and regulatory norms
- ✓ Integrity and Market Conduct
- ✓ Legal directions, related Acts
- ✓ Internal Poilcies & Procedures as approved by Bank's Board

Note: As per Sections 46(4)(i) and 51(1) of the Banking Regulation Act, 1949: RBI can impose penalty

Compliance Culture – Indian Scenario

- ✓ Reserve Bank of India had introduced a system of designating "Compliance Officer" in banks in August 1992, based on recommendations by the Committee on Frauds and Malpractices in Banks (Ghosh Committee).
- ✓ The role and responsibilities of Compliance function received a shot in the arm after the Basel Committee on Banking Supervision (BCBS) issued the High Level Paper on Compliance Risk and Compliance Function in Banks in April 2005.
- ✓ Subsequent to the financial crisis, the focus on compliance has gone up significantly, especially in the area of conduct, KYC/AML, suitability and appropriateness of banking products offered to a specific customer.
- ✓ It will not be an exaggeration to say that some of the big losses suffered by banks in India on account of frauds could have been avoided if a good compliance culture was ingrained in respective banks. In most cases of frauds, a common

thread is non-adherence to internal policies and procedures by employees concerned.

In order to build a compliance program in any organisation following 7 elements can be followed:

- Implementing written policies, procedures, and standards of conduct.
- Designating a compliance officer and compliance committee.
- Conducting effective training and education.
- Developing effective lines of communication.
- Conducting internal monitoring and auditing.
- Enforcing standards through well-publicised disciplinary guidelines.
- Responding promptly to detected offenses and undertaking corrective action.
- **Additionally, measurement and management of compliance risk is needed.**
- **It can help to anticipate where compliance mis-steps are most likely to surface.**

How well are compliance processes working?

- It is important to know the level of enterprise-wide compliance risk which helps to gauge the effectiveness of compliance.
- The Indian financial regulators always emphasise the importance of an organisation's "culture of compliance".
- Having a "robust" culture of compliance can help organisations avoid severe financial consequences.
- A "robust culture of compliance" is essentially an environment that fosters ethical behavior and decision-making.
- It is important to note that the most clearly written, comprehensive **compliance program is destined for failure without such an environment.**
- compliance". Having a **"robust**" culture of compliance can help organisations avoid severe financial consequences. **A"robust culture of compliance"** is essentially an environment that fosters ethical behavior and decision-making. It is important to note that the most clearly written, comprehensive compliance program is destined for failure without such an environment.
- The challenge, however, is that a **"robust culture of compliance"** can be an elusive concept. To take some of the guess work, out of developing a culture of compliance, **here are 10 typical attributes that regulators look for:**

- **Tone at the top**: This is the most important hallmark of a culture of compliance. Regulators are increasingly meeting with senior management during examinations to get a sense of their engagement in compliance. Tone at the top is often evidenced by the processes for making critical decisions.

- **Integration across the enterprise is key**: Risks in banking are both complex and often inter-related. Credit can be accompanied by interest rate risk, market and other risks can aggravate liquidity risk, and compliance risk can overlap with other types of risk, especially operational risk. To ensure that risk is managed thoughtfully across the enterprise, compliance must work closely and communicate well with all risk areas and businesses.
- **Silos**: The compliance department should not be walled off from the rest of the organisation. It is important that compliance staff is present when business decisions are made? Does the firm seek their input? Firms with a strong culture of compliance would answer "yes" to both.
- **Powe**r: Regulators also look at who holds power in the firm. Is the chief compliance officer (CCO) part of senior management? Is the compliance department independent? Is it respected? or does the CCO sit in a back office, neither seen nor heard? When discussing an issue, who wins – business or compliance?
- **Cowboys:** Does the organisation reward risk-taking without limits? Are rewards based solely on financial performance? In a strong culture of compliance, risks are taken within the organisation's tolerance for risk and is seen as being bigger than any one individual.
- **Resources:** Compliance costs money. Is the compliance program appropriately structured and sufficiently funded? Is there a strong disparity in the organisation's investment in technology and other resources to make money versus its investment in technology and other resources to facilitate compliance?
- **Employee Buy-In:** Once the compliance infrastructure is established, it is the employees who carry out the mandate. The firm's culture of compliance must be embedded in the culture of the employees. To facilitate employee buy-in, organisations should have a Zero tolerance policy for employee misconduct and should have a continuing training program to ensure that employees understand their obligations and that the firm takes compliance seriously.
- **Living Compliance Program**: The compliance program should not be a stagnant checklist of procedural requirements. It must be tailored to the organisation's business and risks; it must be tested and modified; and it must be enforced. Are the policies actually working? Are issues escalated to senior management?
- **Technology:** Is compliance handled with pencil and paper? Does the organisation look for ways to automate compliance and limit human error, as it does with portfolio and risk management? How are workflows and documents managed? Technology allows organisations to spend less time in managing papers and people and more time in actively managing risk.
- **Documentation:** Regulators love documentation and so should organisations. Good record keeping reflects a strong compliance culture. When testing compliance policies, can the organisation prove that they work? Is testing documented? Is a documented workflow in place to track the process of marketing materials being approved, and to show that sign-off was received from the legal department?

Governance, Risk and Compliance – GRC Framework

- Growing regulatory environment, higher business complexity and increased focus on accountability have led enterprises to pursue a broad range of governance, risk and compliance initiatives across the organisation.
- However, these initiatives are uncoordinated in an era when risks are interdependent and controls are shared.
- As a result, these initiatives get planned and managed in silos, which potentially increases the overall business risk for the organisation.
- In addition, parallel compliance and risk initiatives lead to duplication of efforts and cause costs to spiral out of control.
- Governance, Risk, and Compliance process through control, definition, enforcement, and monitoring has the ability to coordinate and integrate these initiatives.
- **The span of a Governance, Risk and Compliance process includes three elements.**

GRC Solution's Overview of Working

GRC solution provides an integrated platform for standardizing and managing strategic and operational risk, as well as consolidating information from all financial risk management systems (e.g., credit risk, market risk, etc.) to develop an enterprise view of your risk exposure throughout all common risk management stages – including risk identification, assessment, response and monitoring.

The following modules may be generally implemented in GRC application

- Incident Management Module
- Risk Control Self-Assessment (RCSA) Module
- Key Risk Indicators (KRI) Module
- Issues and Action Plan Module
- Compliance/Policy Management Module
- Governance/Audit Management Module
- Regulatory Reports – Basic Indicator Approach (BIA) & The Standardised Approach (TSA)& Other MIS Reports

Benefits Of An Integrated GRC Approach

- Many organisations find themselves managing their governance, risk and compliance initiatives in silos, each initiative is managed separately even if reporting needs overlap.
- Even though, each of these initiatives individually follow the governance, risk and compliance process outlined above, when they deployed software solutions to enable these processes, the selections were made in a very tactical manner, without a thought for a broader set of requirements.
- As a result, organisations have ended up with dozens of such systems to manage individual governance, risk and compliance initiatives, each operating in its own silo.

By taking an integrated GRC process approach and deploying a single system to manage the multiple governance, risk and compliance initiatives across the organisation, the issues listed above can be easily addressed. Such an approach can:

- ✓ Have a dramatic positive impact on organisational effectiveness by providing a clear, unambiguous process and a single point of reference for the organisation
- ✓ Eliminate all redundant work in various initiatives
- ✓ Eliminate duplicative software, hardware, training and rollout costs as multiple governance, risk and compliance initiatives can be managed with one software solution
- ✓ Provide a "single version of the truth" available to employees, management, auditors and regulatory bodies
- ✓ An integrated GRC approach enables an organisation to integrate and streamline these individual compliance initiatives. So it can significantly reduce the cost of compliance. It is critical that a GRC solution must be able to address a wide range of compliance and risk management initiatives so that an organisation can leverage GRC to deploy a consistent framework across the organisation for compliance and risk management.

Whistle-Blower Mechanism/Policy

Introduction to a Model Whistle-blower Policy In an organisation whistleblowing policy means that the company gives freedom and allows their employees to report or telling the management the Facts and putting a Stop on all unethical immoral or illegal work.

Objective:

- ✓ To give employees, investors, contractors, vendors, and other stakeholders a platform whereon they can raise their concern against any wrongdoing done by the company.
- ✓ To protect employees against retaliation due to whistleblowing policy
- ✓ The company is committed for doing business in ethical ways and therefore an employee should raise their concern if they come across any behaviour, activity which is suspected to be unethical and dangerous for the company.
- ✓ The whistleblowing policy is a crucial policy which gives stakeholders the liberty to raise concern against any suspected illegal activity.
- ✓ The employees of the company can report any concern by an authorised channel operated under the audit committee.

Areas covered under whistleblowing policy:

Below mentioned list gives some examples of the area where the breach of the code of conduct is observed. However, there can be reasons beyond the list as well:

- ✓ Any kind of Harassment or discrimination
- ✓ Sharing of confidential information
- ✓ Any breach of privacy

- ✓ Any kind of Fraud or Fraudulent
- ✓ Misrepresentation of financial data
- ✓ Any kind of illegal activity
- ✓ Corruption
- ✓ Invalid promotion
- ✓ Illegal sales activity
- ✓ Conflict of interest
- ✓ Trading within the company
- ✓ Illegal competitive behaviour
- ✓ Improper use of company assets.

Whistle-blowing Policy in India

The whistle-blower policy in India is aimed to safeguard the interest of the general public. Employees who reveal fraud, corruption or mismanagement to the senior management are called internal whistle blowers. Employees who report fraud or corruption to the media, public or law authorities are external whistle-blowers. Indian whistle-blowers are protected under the Whistle-blower Protection Act India. Laws relating to whistleblowing and protection of whistle-blowers are inadequate in India. However, the Companies Act, 2013 lays down provisions for whistleblowing and corporate governance in India and the elimination of fraud by establishing adequate vigil mechanism. Sections 206 to 229 of the Companies Act, 2013 lay down laws relating to Inspection, Inquiry, and Investigation incorporate. Section 208 of the Act empowers an Inspector to inspect company records and furnish any recommendations to conduct investigations. **Section 210 states that the Central Government may order an investigation into the affairs of the company in the following cases:**

- ✓ On receipt of a report by Registrar or Inspector of the company.
- ✓ On intimation of a Special Resolution passed by a company that the affairs of the company must be investigated.
- ✓ To uphold the public interest.
- ✓ The Serious Fraud Investigation Office (SFIO), a statutory body is created under Section 211 of the Act which has the power to arrest any person for fraud in the company. The auditors have the responsibility to report to the Central Government if they have reason to believe a fraud committed or being committed to the company.