State Bank of Pakistan

Banking Policy & Regulations Department

2017

Issued vide BPRD Circular # 07 dated August 09, 2017

Guidelines on Compliance Risk Management

The Team

S. No	Name	Designation
1.	Syed Irfan Ali	Executive Director, Banking Policy & Regulations Group
2.	Mr. Muhammad Akhtar Javed	Head of Department, Banking Policy & Regulations Department
3.	Mr. Muhammad Qaisar Raza Malik	Sr. Joint Director, Banking Policy & Regulations Department
4.	Mr. Zuhaib Pasha Khero	Joint Director, Banking Policy & Regulations Department

For queries, please contact qaisar.raza@sbp.org.pk and/or zohaib.pasha@sbp.org.pk

Table of Contents

Introduction

The banking industry in Pakistan in last over a decade has experienced significant changes in market dynamics in which it operates, on both regulatory as well as consumer front. These changes include major structural changes fostered by SBP leading to a more competitive, service oriented, financially sound and technologically advanced banking industry and its constituent Financial Institutions (FIs). Such structural changes have entirely reshaped the scope, complexity, outreach and nature of FI's business activities. At the same time, SBP being a progressive regulator has strived to foster the requisite Risk, Compliance & Governance (RCG) practices in the banking industry in line with changing consumer behavior and complexity of industry players to i) safeguard depositors' interest and ii) bring the domestic industry at par with international standards and best practices.

Given the increasingly complex nature of banking operations owing to wide spread use of technology, product innovations and competitiveness in the industry, FIs have confronted significant risk management and corporate governance challenges, particularly with respect to 'compliance risks' that transcend business lines, legal entities, and jurisdictions of operation.

In the absence of standards/guidelines on treating non-compliance as a 'risk' and applying risk management processes to manage it, the FI, its customers, shareholders and employees remain exposed to certain identified and/or unidentified risks. At present, the structure, scope, depth and breadth of compliance function (CF) varies grossly among FIs and there exists a wide gap between the understanding of 'compliance risk' and its management in the industry and the related 'regulatory expectations'. As such, the non-compliance is not considered as a 'risk' and the usual 'risk management process' of identifying, assessing, measuring and mitigating risks are not applied when it addresses compliance issues. Rather, CF generally serves only as a liaisoning unit responsible for managing regulatory returns and other regulatory issues that may arise from time to time.

Besides, generally, the CFs has not been provided with due importance, support, independence and adequate resources to carry out their functions effectively. Such state of affairs of CFs in FIs does not meet regulatory expectations of taking compliance to rules and regulations seriously at all levels of operations; in all geographical locations- even the remotest of all, in all business areas and in all jurisdictions.

The CF has attracted great attention from regulators internationally after the Global Financial Crises. Many giant international FIs have been levied massive penalties on account of non-compliance of regulatory requirements (in letter & in spirit), in response to which the FIs are now undergoing a major shift in their approach towards compliance risk and its management wherein more quality resources are being moved to CF to meet the ever increasing regulatory expectations and reduce cost of non-compliance.

To address these gaps and to further align the local banking practices with international standards, SBP has developed guidelines on 'compliance risk management' to provide the industry a uniform benchmark for identification, assessment and management of compliance risk in their operations.

Interpretations

"Board" means the board of directors of a financial institution.

"Management" refers to the chief executive officer and other key executives of financial institutions as defined in Prudential Regulations (PRs) for Corporate & Commercial banking as amended by SBP from time to time.

"Chief Compliance Officer (CCO"); the key executive that is head of compliance function/department in the financial institution and is the central point of authority for a financial institution's compliance risk matters.

"Compliance function" the department that carries out compliance function responsibilities of a financial institution, as prescribed in PR G-1 D and in these guidelines.

"Compliance risk" means the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a FI may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its banking activities (BIS).

"Compliance review" is defined as a comprehensive evaluation undertaken to ascertain/confirm FIs compliance to laws, rule, regulations, instructions, standards and practices as applicable to its activities.

"Financial Institutions (FIs)" here refers to all banks/DFIs and Micro Finance Banks.

Objectives

I. The objective of the guidelines is to promote the safety and soundness of FIs by minimizing potential financial, reputational and operational risks arising from legal and regulatory noncompliance. SBP's expectations regarding management of compliance risk as an important risk function are also consistent with international standards and best practices that are shaping a new world for FIs to operate in.

II. These guidelines aim to further strengthen the existing compliance standards, activities and practices by enhancing the effectiveness of CF in a way that the 'non-compliance' is considered as a 'risk' and proper risk management process is applied 'entity-wide' in identification, assessment and mitigation of non-compliance events. As such, this policy aims to bring CF under the broader ambit of 'entity-wide risk management' philosophy at each FI.

III. These guidelines will complement the roles and responsibilities of compliance officers (CO) and CFs, which have already been prescribed in prudential regulation G-1 D.

IV. While the guiding principles of sound risk management are the same for compliance risk as for other types of risks, the management and oversight of compliance risk presents certain challenges different from other types of risk faced by FIs. One of the challenges is that unlike other risks (i.e. Credit, Market, liquidity etc) the risk appetite for non-compliance to legal and regulatory requirements has to be 'zero' as all FIs have no option but to comply with laws, rules and regulations as applicable to its business.

V. This idiosyncratic characteristic of compliance risk underscores the need for an independent, resourceful and dynamic CF supported by an entity wide, more formal, structured, risk focused and extensive compliance program/framework that plays a key role in managing and overseeing compliance risks starting from promoting 'compliance literacy' and inculcating a strong 'compliance culture' across all business activities/function and at all hierarchal levels in FI.

Applicability

The proposed guidelines will be applicable on all FIs.

Effective date:

The effective date of these guidelines is December 31, 2017. The FIs should, in the meantime align their CF, policies and procedures in line with the requirement of these guidelines. Keeping in view the process involved banks should meet the requirement given under section 4.2.1 (A) (XX) by June 30, 2018.

1. Compliance Risk Management

1.1 A strong compliance culture reflects high ethical standards and integrity starting at the top of the organization and cascading down the line in a manner that ensures seamless and effective implementation of regulatory requirements/standards/practices and other laws in letter and in spirit. Given the nature of its business & operations that are fundamentally based on the principles of 'Trust', a FI should hold itself to high standards in carrying on its business because its failure to manage its compliance risk effectively may result in adverse consequences for its customers, depositors, shareholders, employees and the FI itself.

1.2 Compliance laws, rules, regulations, instructions and standards have various sources, including legal and regulatory requirements issued by legislators and supervisors, market conventions, codes of practice promoted by industry associations, and internal codes of conduct applicable to staff members. Compliance risk in a FI, therefore, goes beyond what is legally binding and embraces broader standards of integrity and ethical conduct[1].

1.3 The management of compliance risk is the first and foremost responsibility of all officers in a FI, at all levels of hierarchy. However, the 'primary' responsibility of establishing an independent/effective/strong and resourceful CF in FIs capable of identifying and managing compliance risk on enterprise level remains with Board and senior management of the respective FI. The board and senior management of the FI should assume the 'leadership' role in implementing an adequate and effective compliance program in FI.

1.4 The 'leadership' role goes beyond simply 'tone-at-the-top' and requires that the compliance program of a FI must be built on a solid foundation of ethics that are fully practiced and openly endorsed by board and senior management. There should be a clear, visible and active commitment to compliance at senior level in a FI complemented by high-ranking Chief Compliance Officer (CCO) with the authority and resources to manage the program on a day-to-day basis.

1.5 The CF of a FI, under the stewardship and continuing guidance of its board and with full support of Compliance Committee of Management (CCM), shall lead the process for designing and implementing the enterprise-wide compliance program by joining hands with all stakeholders under an effective and constructive coordination/support mechanism.

[EXPECTATIONS]

[1] The ethical practices like transparency, integrity, honesty and compliance go hand in hand when it comes to financial industry and this area has emerged to be an essential element of overall compliance culture in any FI.

While all instances of non-ethical behavior may not essentially be instances of non-compliance, however, the FI must ensure that its employees at all hierarchal level remain committed to demonstrate superior ethical practices in their dealings with depositors, customers, regulators and all other stakeholders.

In order to promote ethical behavior in their day to day operations in the organization, the FI should appoint 'Ethics/conduct officers' (under CF or any other function as the FI deems fit) who shall serve as a central point to identify and collect information (mainly through customer complaints, incidents of frauds, seeking depositors/customers feedback directly through phone or in person, surprise visits of branches etc) of unethical behavior/conduct (that is not in line with FIs internal policies or regulatory instructions) on part of employees (at any hierarchal level). A coordinated action plan may then be devised to address the systemic gaps to encourage employees at all levels to act with integrity, in ethical manner and in best interest of depositors and other stakeholders.

The FIs may develop/revise their existing policies to further define the role and responsibilities of 'ethics/conduct officers' and the process through which they will perform their duties.

1.6 Given the growing complexity of operations of a FI and increased focus of regulatory authorities on compliance/risk culture of a FI, the role of CF has moved far ahead from the conventional approach (tick box). Rather, it is now considered as an important and critical function in a FI that aims to add positive value in increasing the overall efficiency and effectiveness of a FI by driving cultural changes in the organization towards understanding compliance risks.

1.7 The FIs are free to choose any risk management method/standard/process that suits the objectives of this guideline and is in line with FIs' overall risk management strategy, structure and complexity. However, the FIs are strongly encouraged to implement an entity wide 'Three Lines of Defense (TOD) model' of risk management to identify and manage their compliance risks. The TOD model is briefly described below:

(a) The line departments/managers/staff serve as 1st line of defense and are primarily responsible for managing compliance risk 'inherent' in their day-to-day activities, processes and systems for which they are accountable[2];

(b) The compliance function, being the 2nd line of defense, is responsible for assisting line managers/departments in designing and implementing adequate controls to manage risks of non-compliance. The CF is also responsible to closely coordinate with other risk management functions of the bank to monitor the adequacy and efficacy of compliance risk controls. The CF is also responsible for assessing the level of compliance risk (entity wide) faced by FI and reports such risk profile to Board and MCC on periodic basis. The other responsibilities of CF include escalation of instances of non compliance and following up with relevant functions to strengthen the implemented controls.

(c) The internal audit function, working on behalf of FI's board, is responsible for providing independent assurance to board or its audit committee on the quality, effectiveness and adequacy of FI's governance, risk management and control environment including the working of 1st and 2nd line of defense to achieve risk management and control objectives.

2. Governance Structure

2.1 The board and senior management of a FI have primary responsibility in maintaining and promoting a strong compliance culture by ensuring that all employees understand their responsibilities with respect to compliance and feel comfortable in raising any event of non-compliance without any fear of negative consequences. In this respect, the board and senior management should create an enabling compliance culture that not only ensures that its employees comply with legal & regulatory requirements, standards and market best practices but also encourages the required ethical conduct that underlies such requirements.

[EXPLANATION]

[2] As such, the FI must make it clear in the compliance policy that the primary responsibility to manage compliance risk lies with the business lines. This includes the responsibility of business lines to own, develop and update systems, policies, processes and procedures to manage compliance risk inherent in their day to day activities.

2.2 Responsibilities of the board

2.2.1 The Board of Directors of the FI has the ultimate responsibility of guiding and overseeing the design and implementation of enterprise wide compliance risk management program in the FI. In order to fulfill its responsibilities, the board, either itself or through any of its sub-committee must:

(a) approve compliance risk strategy (as part of FI's overall risk strategy) and allied policies of the FI and oversee its implementation across the entity in letter and spirit;

(b) ensure establishment of a robust CF compatible with FI's overall risk management strategy, risk profile and complexity of operations, with required authority, independence, financial resources and quality human resources;

(c) approve an end-to-end compliance program[3] that promotes and supports compliance risk management across the organization, at every hierarchal level of the FI. The compliance program should also clearly define the roles and responsibilities of different functions, the coordination mechanism, the processes, methods and tools adopted to identify, mitigate and report entity wide compliance risk.

(d) maintain and promote a high compliance culture and values of honesty and integrity in FI.

(e) discuss compliance issues regularly, ensuring that adequate time and priority is provided in the board agenda to deliberate compliance issues and that such issues are resolved effectively and expeditiously.

(f) evaluate the effectiveness of FI's overall management of compliance risk, at least annually; keeping in view the regulatory observations in onsite examinations, regulatory enforcement actions, internal assessments/feedback from internal audit, compliance reviews, as well as interactions with the CCO.

(g) on advice of CEO, approve the appointment of CCO with sufficient experience, expertise, skills and qualifications to perform CCO's functions in an effective manner.

(h) Approve any disciplinary action or termination of CCO.

(i) Ensure that the seat of CCO does not remain vacant for more than 60 days.

(j) ensure that CCO has the appropriate stature, authority, resources (physical, financial and human) and support to fulfill the duties, is sufficiently independent of line departments, and has the capacity to offer objective opinions and advice to Senior Management and the Board on matters of compliance risk.

(k) engage with CCO on half yearly basis to provide him the opportunity to discuss issues faced by the CF in implementation of board approved compliance program.

(l) review the minutes of Compliance Committee of Management (CCM) meetings to ascertain its effectiveness in managing compliance risk.

(m) Review the progress in implementing remedial actions taken with respect to instances of non-compliance or control weakness as identified by CF through its regular 'compliance reviews' and /or various other sources.

(n) satisfy itself of receiving the accurate as well comprehensive information required to perform its compliance risk oversight responsibilities, including seeking assurances from Senior Management that the compliance risk controls have been implemented and are working effectively.

[3] The term 'compliance program' and its minimum components have been defined in sufficient detail in section 4 of this document.

2.3 Compliance Committee of Management (CCM)

2.3.1 The FIs are required to establish a CCM led by CEO of the FI and may include all important key executives like head of risk, head of operations, head of credit and investment operations, head of legal, head of HR, head of IT etc[4]. The CCO will serve as secretary to CCM. The committee should meet at a set frequency (at least once in a quarter) as defined in FI's compliance program to discuss compliance risk issues faced by the FI at cross functional/departmental level and/or in any particular department/function, as the case may be.

2.3.2 The CCM should also ensure that the CF is able to secure assistance from other functions with specific expertise (for example, legal, Shariah review, trade, treasury, credit or risk management) as and when needed.

2.3.3 Among various other important functions that CCM may perform, one of the important functions that it can help enhance the buy-in of compliance risk management by senior management in individual as well as cross functional/departmental level. This in turn will help CF to better understand the drivers/sources of risk and devise targeted strategy to bridge the shortcoming as and when identified.

2.3.4 This form of education from key executives to other officers of their department/function will help keep compliance at forefront, increase its awareness at all hierarchal levels, and would make employees feel the need of compliance risk management as and when new processes/products are developed.

2.3.5 Besides, at minimum, the TORs of CCM should include the following:

a) oversee the management of entity wide compliance risks of the FI and ensure that FI's management understands the compliance risks to which the FI is exposed to.
b) promote a high compliance culture, and assist FI's compliance function in discharging of its duties and achievement of its objectives.
c) facilitate CF in successful and effective implementation of compliance program in their respective functions and/or across different functions and establish a mechanism to ensure that the desired results are achieved as envisaged in compliance program.
d) assist and facilitate CF in implementing policies, processes and procedures to manage compliance risk;
e) assist CF and human resource department in developing and implementing an organization-wide training program on compliance risk matters to ensure that relevant staff maintains a satisfactory level of knowledge of laws, rules and regulations;
f) report to the board at least annually on the effectiveness of FI's overall management of compliance risk in such a manner as to assist the board in carrying out its responsibilities as set out in section 2.2 of these guidelines.

[EXPLANATION]

[4] This is just an indicative list and FIs can include as many key executives (except head of Internal Audit) who are looking after important business activities as the need be, in the CCM. Besides, other key executives can be invited in specific meeting to discuss compliance issues pertaining to their respective areas.

3. Structure of compliance function

3.1 Organization

3.1.1 A FI must organize its CF in a manner that allows compliance risk to be managed effectively entity-wide, taking into account the size, geographic diversity (domestic as well as international), target market, nature of operations and complexity of its business and the legal & regulatory environment under which it operates.

3.1.2 The larger FIs with extensive networks of branches deal with large number and diverse nature of customers and provide a wide range of banking services are therefore naturally exposed to greater risks of non-compliance as compared to FIs with smaller number of branches and fewer activities. However, the management of compliance risk is of the same importance to both small and larger FIs and its organization must be consistent with the overall strategy, risk profile and structure of the FI.

3.1.3 Where the FIs have international branch operations, the compliance officers at international jurisdictions shall maintain matrix reporting structure by reporting to their country/regional heads as well as CCO at Head office on all compliance related matters (subject to local regulatory rules and regulations).

3.1.4 In order to increase the efficiency, the CF may collect information from internal audit department regarding incidences of non-compliance observed in a specific branch/function/department during their audit. Besides, the CF, either independently or in close coordination with operational risk unit may conduct independent compliance risk assessments of key/critical functions where likelihood of non-compliance event happening is high (lending operations, investment operations, AML & CFT, fair dealing of customers/depositors etc) or has a high impact on FIs compliance risk profile[5], on regular basis.

3.1.5 Apart from having a centralized compliance department at head office level and any other compliance structure down the line in branches or regions (according to the needs of the FI as determined by the FI itself), the CF may also have subject experts[6] on various critical areas to provide guidance to business areas as and when required. The subject experts may provide guidance/advice/training to business units on compliance issues relevant to their area and may be highly instrumental in identifying and managing the compliance risk in his/her area of expertise. These areas may include, risk management, credit operations, product compliance, customer service, international trade, outsourcing, corporate governance, financial disclosures, business continuity, Information technology, general banking operations, AML & CFT etc.

[EXPECTATIONS]

[5] This shall be covered in compliance risk policy in sufficient detail as to which activities shall be reviewed by CF, what will be the scope and frequency of such reviews. Besides, the CF can decide on collecting information from internal audit function depending on FI's risk profile, the effectiveness of internal audit function, overall risk management strategy and complexity of its operations. Besides, the CF should not 'overly' rely on internal audit reports and should conduct assessments either independently or in coordination with operational risk unit of all important/key/critical areas/functions/activities.

[6] It is expected that having 'subject experts' will add great value in enhancing the level of compliance risk management in FIs. FIs compliance functions are strongly encouraged to have these experts in all important fields that will not only make 'advising' and review function of CF more effective but will also help it in implementing the compliance risk processes that cut across different business functions/departments.

3.2 Independence

3.2.1 The CF must be independent of business lines to carry out its compliance activities effectively. As such, a FI must ensure that the CF is not placed in a position where there are real or perceived conflicts in respect of its scope of responsibilities, reporting lines or remuneration.

3.2.2 The CF staff shall have clear authority and unrestricted access to the information and personnel necessary to carry out their responsibilities.

3.2.3 The FI must ensure that the performance appraisal of COs is primarily based on the achievement of their CF responsibilities instead of linking it to financial performance of any other business line or function.

3.2.4 A constructive and cooperative working relationship between the CF and business lines should be implemented to facilitate overall identification and management of compliance risk within and across different departments/functions. In practice, this can involve the direct participation of the CF in providing related input to business functions on a product, service, process or activity through representation on relevant management committees.

3.2.5 Where such arrangements referred to in paragraph 3.2.4 exist, a FI must ensure that–

(a) the CF is not placed in a position of conflict;

(b) the accountability of the CF is properly documented i.e. CF's role must be explicitly mentioned in TORs of such committee; and

(c) the CF is not prevented from highlighting compliance issues relating to any business decisions to the board or senior management, where necessary.

3.3 Resources

3.3.1 Officers undertaking CF responsibilities should have the necessary qualifications, experience and skill set. In particular, they must have a sound understanding of relevant legal and regulatory requirements and the implications of such requirements on FI's overall operations and/or respective function/(s). In such cases where the FI has overseas operations, the central CF should devise a mechanism to at least have an understanding of relevant local legal and regulatory requirements applicable in these jurisdictions.

3.3.2 The CF must be provided with required physical and financial resources and all other resources as the case may be to carry out its assigned activities properly.

3.3.3 A FI must ensure that the CF is kept abreast of developments in legal and regulatory requirements by undertaking regular and systematic training programs.

3.3.4 As one of the means to develop a strong CF, a FI may consider encouraging CF officers to possess accredited qualifications in the area of compliance/risk management or relevant working experience.

4. Compliance Program (CP) – Overview

4.1.1 The CP is a set of tools/methods/processes/procedures to translate and actually implement the board approved compliance risk strategy and compliance risk policy across the organization. The CP can be viewed as 'blue print' that describes 'how' the compliance risk strategy and policy is to be translated into tangible actions to achieve policy objectives. The CP is supplemented with a strong, independent, well organized and resourceful CF, relevant & clear board approved compliance risk strategy and compliance risk policies. The CP, at minimum, should describe and

define (in sufficient detail) all necessary procedures, processes and methodologies to implement an effective compliance risk management framework in the FI[7].

4.1.2 The CP of a FI should, among other things, also focus on creating and encouraging a viable risk/compliance culture in the FI – a task that may take considerable time, management buy-in, and sustained communications by CF across the FI.

4.1.3 The FI should note the fact that non-compliance with applicable regulatory requirements can have significant negative effects on its reputation and/or soundness and may lead to increased regulatory intervention. Therefore, the CP so developed should be comprehensive and robust enough to address all the existing and emerging compliance risk that FI may face in its operations.

4.1.4 The CP adopted by FI should enable it to apply a risk-based approach for identifying, assessing, communicating, managing and mitigating regulatory compliance risk. The compliance risk strategy and its allied policies/procedures/compliance program should be reviewed and updated regularly, at least annually, to address: any need for improvement, new and changing regulatory compliance risk, new business activities and any changes to corporate/management structure of FI. The review methodology should include a mechanism that holds individuals accountable for their assigned duties or functions.

4.2 Components of Compliance Program (CP)

4.2.1 The CP should, at minimum, include the following, with clear and established lines of responsibility: (A) roles and responsibilities of CF, (B) role of Board and Compliance Committee of Management (C) role and responsibilities of the Chief Compliance Officer (CCO); (D) procedures for identifying, assessing, communicating, and managing compliance risk (E) independent monitoring mechanism; (F) internal reporting; (G) role of Internal Audit and (H) training program on compliance risk management. Each of these items (except point (B) which is already given above in section 2 of these guidelines) is described in further detail below. The process for bringing the 'cultural change' would be an overarching one that needs to be embedded in all components of the CP.

A: Roles and responsibilities of compliance function (CF)

The CF must conduct its activities and discharge its responsibilities in a manner that reflects the assessment of the level and impact of the compliance risk faced by the FI. Accordingly, the CF must give greater focus to areas where compliance risk is assessed to be high i.e. areas like corporate governance, lending operations, deposit taking, risk management, AML & CFT, fairness & transparency in dealings with customers etc; while preserving appropriate coverage of all compliance risks identified.

The CF must work pro-actively and identify & assess the compliance risk associated with FI's activities. This can only be possible when CF staff, including CCO, has adequate operational knowledge and exposure to key business processes of the FI and keep up with material changes

[EXPLANATION]

[7] This can be achieved by ensuring that CP clearly identifies the governance structure, reporting lines, responsibilities and accountabilities for identifying, assessing, measuring, mitigating and reporting of compliance risk in line with these guidelines. The CP should be complemented with process flows, reporting charts, checklists etc. to make it clear for the users to clearly understand and interpret its roles and responsibilities in whole compliance risk management process.

in its structure and operations. For this purpose the COs should be provided with sufficient and continued training on all relevant areas of their responsibilities.

In addition to the responsibilities given in PR G-1 D, the CF should perform the following responsibilities:

I. formulate a comprehensive compliance program and allied policies & procedural manuals; develop required systems, tools/methods; design compatible processes, and ensure that these are reviewed periodically;

II. ensure that guidance and vision provided by board and senior management are effectively translated into operational goals/activities/plans to institute an effective compliance culture in the FI that promotes and encourages identification and flagging of non-compliance events without any fear of negative consequences.

III. assist board/board sub-committee and CCM in monitoring the entity-wide implementation of compliance program and the level of compliance risk that a FI is faced with at any given point in time[8].

IV. maintain robust systems and procedures to carry out AML & CFT related responsibilities as stipulated in relevant SBP instructions as issued from time to time.

V. organize its activities in a way that the approved compliance program is rolled out seamlessly and successfully across the organization and it covers all business segments & areas, functions, branches (domestic as well as overseas) where compliance risk exists[9].

VI. develop and implement a communications process to ensure laws, regulations, rules and policies are shared with relevant functions of the FI.

VII. ensure that all employees, especially the line staff understands the regulatory compliance risks inherent in the activities they perform and that policies, processes and resources available are sufficient and effective in managing those risks.

VIII. ensure that it remains aware of any organizational restructuring/developments or business processes reengineering to facilitate timely identification of new compliance risk;

IX. develop and implement a mechanism for collection/ reporting of incidence of non-compliance from line departments/functions on periodic basis[10],

[EXPECTATIONS]

[8] For FIs with overseas branch operations, the CF should submit a separate report to board or any of its designated committee (on half yearly basis) regarding the compliance risk issues in each overseas jurisdiction and their mitigation plans to address the identified deficiencies.

[9] This means that a FI which conducts business internationally through its branches must also ensure compliance with all local (host country) legal and regulatory requirements applicable in those jurisdictions. The CF at HO, however, should be very much aware of the nature and magnitude of compliance risk that exists in FI's overseas operations (jurisdiction-wise) and should work closely with local compliance unit to formulate mitigation plan to address the identified deficiencies.

[10] Although, there is greater tendency in employees to not report any incidence of non-compliance (with regulatory instructions directly-which provides for 'minimum' requirement- or with the internal policies developed in line with a regulatory instruction-over and above the minimum requirements given by regulator), however, the FI needs to increase the awareness and create a compliance and risk culture that encourages reporting of such incidents as and when they occur. The reporting of such incidents should not resort to any penal action(s) for the employees reporting it but should be viewed as a chance of fixing the actual control weakness to avoid such recurrences in future. CF needs to give proper time and effort to help initiate the change in risk/compliance culture of the organization.

X. where a FI has branch operations in more than one jurisdiction, the CF must establish appropriate mechanisms for coordination and sharing of information between the local compliance unit/department in that jurisdiction and FI's CF at HO to ensure that organization-wide compliance risk is managed effectively.

XI. use a range of indicators to identify, assess and systematically monitor the level of compliance risk in FI[11].

XII. ensure that all concerned units/divisions/departments/functions of the FI are applying processes and tools that have been developed by CF to manage compliance risk.

XIII. ensure that all regulatory returns are submitted to regulators in timely manner with maximum accuracy. In addition, the CF should establish a mechanism for responding and making follow ups on all regulatory correspondence in timely manner.

XIV. assess FI 's compliance culture, identify gaps and make all possible efforts including providing trainings, arranging seminars and workshops, issuing regular communiqué to all employees of the FI on the matters pertaining to compliance risk in general as well as specific matters (compliance risk related) pertaining to FI.

XV. advise the board, senior management and officers on regulatory requirements as and when required[12].

XVI. review new products and services (and marketing materials) to ensure compliance with applicable laws, rules, regulations and instructions.

XVII. develop and implement a thorough and well documented process which assures the timely correction of identified violations (internally by compliance reviews, internal audit report, regulatory inspection repots or any other source) of all applicable laws, rules, regulations and instructions[13].

XVIII. perform appropriate compliance reviews to evaluate the adequacy of controls put in place to manage compliance risk and promptly follow up on any identified deficiencies, and coordinate plans to address such deficiencies.

XIX. the CF should maintain an up-to-date data base of applicable laws, rules, regulations and instructions to help it in performing its responsibilities. Such data base may include the following:

(a) All laws, regulations, rules, standards and instructions issued by regulatory and supervisory authorities[14].

(b) All relevant commercial, financial and investment laws and instructions applicable to FI.

[EXPLANATION]

[11] These indicators may be qualitative or quantitative in nature and may include, but are not limited to, trends in customer complaints, increasing number of frauds and forgeries, repeated occurrence of observations/violations highlighted in regulatory inspections/assessments, increase in regulatory penalties and other enforcement actions, instances of litigation against FI etc.

[EXPECTATIONS]

[12] This includes keeping them informed on the developments affecting regulatory requirements and providing the board and senior management with an assessment of their implications on a financial institution's existing compliance risk profile and capacity to manage compliance risk going forward.

[13] As such the CF may conduct 'root cause analyses' of certain high risk instances of non-compliance as identified by COs, internal audit, regulatory inspections or external audit reviews.

[14] This shall also include all enforcement directives issued by regulatory authority from time to time that the FI is required to implement as per given timelines.

(c) Rules and code of conduct and sound professional practices in force.
(d) Compliance-related decisions of the FI's senior management and board of directors.

XX. the CF should develop an automated system to capture and consolidate (at minimum) the following enterprise wide data/information:

- Reference of laws, rules, regulations, standards, enforcement directives and instructions and the requirements that they impose,
- The sensitivity (risk) of each legal/regulatory requirement given FI's existing compliance risk profile
- The line managers/process owner(s) to which such requirements pertain,
- The FI's function/unit/department responsible for the process
- The existing compliance risk profile of the each unit/department/division based on the incidence of non-compliance
- The action plan to be designed and implemented by respective unit/function/department with active involvement of CF and FI's Operational Risk Management (ORM) unit, if any, to bring risk profile within acceptable limits.

C: Role and responsibilities of the Chief Compliance Officer (CCO)

The CCO should have a clearly defined and documented mandate, unrestricted access, and for functional purposes, a direct reporting line to the CEO of the FI. The CCO is responsible for assessing the adequacy of, adherence to and effectiveness of FI's controls, and provide an opinion to the Board whether, based on the independent monitoring and reviews conducted, the compliance risk management controls are sufficiently robust to achieve compliance with the applicable regulatory requirements enterprise-wide. In addition to ensuring compliance to areas as mentioned in PR G-1 D of corporate commercial banking, the CCO should perform following minimum responsibilities:

a. Ensure compliance with applicable laws, rules, regulations and instructions.
b. Develop end-to-end compliance programs and all allied policies, procedures, methods, tools etc. in the light of these guidelines and ensure/monitor/oversee their entity-wide implementation.
c. Determine the resources required for CF to carry out all its roles and responsibilities (as given in these guidelines) professionally and of desired quality.
d. Develop, coordinate, and participate in a multifaceted educational and training program that focuses on the elements of the compliance program, and seek to inculcate a conducive compliance/risk culture in the FI.
e. Provide summary data and report findings on compliance issues to board or its sub-committee and CCM on periodic basis.
f. report to the board/board sub-committee promptly on any material incidents of non-compliance (for example, failures that may attract a significant risk of legal or regulatory sanction);
g. Liaise with SBP and serve as focal person on all matters pertaining to FI.
h. ensure that regulatory enforcement actions (domestic or foreign as the case may be) are implemented in letter and in spirit within given time frame and in manner as prescribed by the regulatory authority.
i. Oversee fraud investigations involving customer accounts and recovery of funds, and coordinating investigations with external investigation and enforcement officials.
j. Establish a close working relationship with all key executives of the FI to facilitate effective implementation of FI's compliance program.

k. Ensure that a documented code of ethics is periodically disseminated to and is acknowledged by all employees of the FI and its board.
l. Ensure dissemination of updates in regulations and compliance procedures to relevant business units, control units, the CEO and the board (as the case may be).
m. Ensure integration of compliance risk management in overall entity wide 'enterprise risk management' framework in FI.

D: Procedures for Identifying, Assessing, Communicating and Managing Compliance Risk

The CF should develop appropriate procedures & processes and ensure their proper communication to relevant line managers/staff at all levels to ensure that they are provided with all current and accurate information required to:

- Maintain knowledge of applicable regulatory requirements.
- Identify areas where risk of non-compliance exists,
- Assess/measure the nature and magnitude[15] of non-compliance,
- Communicate incidents of non-compliance to CF, and
- Make effective plans to manage and mitigate compliance risk.

These procedures and processes should be developed jointly by business departments/function and CF and should enable a FI in adopting a risk-based approach to manage compliance risk so that appropriate resources are allocated to higher risk areas. The information provided to line managers/staff should be updated, as necessary, to reflect new and changing regulatory requirements. In addition, such procedures and processes should assure that when changes are made in products, services, strategic plans, corporate structure and other activities of the FI, the same are reflected in revised compliance risk map of the FI.

Some of the techniques/tools that FI can use to identify, asses and measure compliance risks on entity level are given below. FIs, however, are free to use any risk management tools/methods/processes that cater their needs to manage compliance risk.

[EXPLANATION]

[15] Unlike other risks, the risk appetite for compliance risk for any FI happens to be 'zero'. As such knowing the 'magnitude' of non-compliance would only let the line management to understand the 'weaknesses' of controls that make non-compliance possible and take appropriate measures to manage the same.

a) Risk and Control Self Assessments (RCSA)[16]

I. The RCSA is the most widely used tool for identification of particular risks and assessment of implemented control to mitigate those risks. The self assessment exercise should be carried out by the individual unit/department/function or by more than one functions/units/department if the process cuts across different functions. The self assessments identify various potential events that may lead to non compliance of regulatory instructions and/or requirements if implemented controls are not adequate. A key advantage of self assessments is that it involves all staff working in a particular unit/department/function and may greatly help in raising the compliance risk awareness for people undertaking it.

II. The active involvement/engagement of CF is mandatory in RCSA process with special focus on areas where regulatory compliance risk is high like AML & CFT, lending operations, investment operations, risk management, corporate governance etc. The CF being expert of regulatory risk and having first hand information of FI's entity-wide compliance risk management practices may be well in a position to guide line managers and any other independent unit conducting RCSA [operational risk (OR) unit, Internal Control Units (ICU) etc] in conducting 'self assessment of compliance risk' that is uniform in approach, standardized and comparable in content; and consistent across different functions of the FI. The CF may challenge the outcome of RCSA where there are plausible reasons to do so to reduce the risk of regulatory non compliance. In case where there is a significant difference of opinion, the position taken by CF would be treated as final.

III. SBP has already issued detailed guidance for banks on conducting RCSA through its Operational Risk Management (ORM) Guidelines issued vide BPRD circular # 4 of 2014. While the operational risk is present in almost each and every activity/process of the FI (whether its credit, market, liquidity or reputational risk—each of these have some operational risk (and hence compliance risk) aspect that may lead to financial/non financial loss), however, all those operational risk incidents that may render the FI in breach of a regulatory requirement are classified as the compliance risks. The compliance risk is the most important type of operational risk that, if not managed properly, may have serious consequences for the FI.

IV. Given the unique nature of compliance risk and the fact that it can stem from any important/key activity of the FI, it is the responsibility of CF to have a full and complete

[EXPECTATIONS]

[16] The detailed procedures/processes/techniques/approaches/format of conducting RCSA is provided in detail in SBP's Operational Risk Management Framework issued in 2014. Generally, two approaches are adopted by FI for RCSA 1) where self assessment exercise is done by business unit themselves and are then validated by operational risk unit, and 2) the operational risk unit independently conducts the risk assessments and control testing exercise in coordination of concerned business unit/function/department. The second approach is preferred over the first one in that it generates more objective and relevant results. Whatever approach is adopted by FI, the primary responsibility of coordinating/facilitating RCSA rests with operational risk unit, however, the CF must ensure that the objective of RCSA exercise (under these guidelines) is essentially achieved by enabling operational risk unit to capture compliance risk during RCSA exercise.

picture of FI's compliance risk irrespective of the originating risk factors involved. In order to do so, the CF should actively coordinate with OR unit during RCSA exercise so that assessment of existing/potential compliance risks and testing of implemented controls is properly evaluated by CF. The CF may also help OR unit in development of common language[17], risk matrices that identify the compliance risk events and their sources/drivers, the functions/units/departments to which these events pertain, the likelihood & impact of each risk event over FI's compliance risk profile, and the risk mitigation plans to remove control weaknesses/deficiencies. These matrices may be complemented with qualitative risk assessment for each business department/function and for the FI as a whole.

V. The CF should also coordinate with concerned function/department/unit and OR unit to develop appropriate Key Risk Indicators (KRIs) that may serve as 'trigger points' or 'early warning signals' for an event of regulatory non compliance and require CF to intervene or escalate the matter to appropriate level. While developing KRIs, it may be ensured that these reflect the distinct nature and characteristics of each of the business function/department of FI.

b) Risk Maps and Process Flows

I. The outcome of RCSA can be translated into risk maps, summary charts and diagrams (compliance risk dashboard) that can be reviewed by CF, CCM and FI's board[18]. These charts and diagram may greatly help FI to identify, discuss, understand and address risks with a clear picture of their sources/drivers, types of risks and functions involved.

II. The utility of RCSA exercise can greatly be enhanced through having a 'compliance risk dashboard' at CF/CCO with access to senior management. This will greatly enhance the ability of the FI to monitor number of compliance risk management activities/processes (risk exposure, relevant functions, resolution timelines, action taken etc) across different business lines/functions at a given point in time. Having accurate, comprehensive and timely information will enable CF and senior management to take necessary steps for comprehensive implementation of compliance program by changing/adding risk mitigation plans, allocation of more resources, and requiring more frequent reporting form identified functions/departments.

[EXPECTATION]

[17] It means defining the different terms pertaining to compliance risk management explicitly, such that they mean the same thing to all people across different business functions. Developing such common language will enhance level and quality of communication between CF and other functions/departments of the FI by providing a common platform to discuss compliance issues in easy way.

[EXPLANATION]

[18] Reviews of the risk maps and process flows by the CF and senior management of a FI will enable them to timely identify the compliance related issues/areas and apply appropriate mitigation procedures where necessary. Risk maps will also enable senior management and board to focus on 'high risk' areas within a business function and across the FI and allocate risk management resources accordingly in an efficient manner.

E: Independent Monitoring & Review Mechanism

I. The independent monitoring and review procedures and processes adopted by CF should be standardized, uniform, relevant and sufficiently consistent on enterprise-wide basis enabling it to aggregate information in a systemic way to identify any patterns, themes or trends in compliance controls that may indicate weaknesses. Compliance control processes should include verification of key information (including significant remediation activities) used in compliance reports to Senior Management and the Board.

II. In addition to periodic RCSA exercise conducted by OR unit of a FI, the CF should carry out independent compliance reviews (on the basis of a representative and relevant sample) of material and high risk activities of the FI on regular basis where non-compliance may have serious regulatory implications on FI's reputation, financial stability and standing in the market.

III. The compliance reviews should, at minimum, cover the areas like awareness of compliance risk in the subject unit/department/function, adequacy of compliance controls, accuracy of returns submitted to regulatory authority and the actions required to fulfill the control gaps.

F: Internal reporting of compliance risk

I. The CCO should decide the general areas of content addressed in, and frequency of, regular compliance risk reports to CF by line managers. Based on such reports and other information available with CF, the CCO must report to CCM and Board on the findings and analyses of compliance risk in the FI.

II. These reports should be in a manner and formats that allow the CCM and Board to clearly understand the regulatory compliance risks to which the FI is exposed, and the adequacy of key controls to manage those risks. These reports should facilitate the board in performance of its oversight responsibilities for compliance risk. The Board should review and determine the type, content and frequency of reports to satisfy itself of receiving the necessary information to carry out its oversight role. The reports, at minimum, must include:

(a) the results of the compliance risk assessments (including monitoring and review of controls) undertaken during the assessment period, highlighting key changes in the compliance risk profile of a FI as well as areas where greater attention by senior management would be needed;

(b) a summary of incidents of non-compliance (obtained through compliance reviews, internal audit reports, regulatory examinations and as reported by various units/functions/departments) and deficiencies in the management of compliance risk in various parts of the FI during the period;

(c) an assessment of the impact (both financial and non-financial) of such incidents on FI (for example, penalties or other enforcement actions taken by any regulatory authority against FI or its board or management);

(d) compliance issues involving any department/function of the FI and/or member of senior management of the FI, and the status of any associated investigations or other actions being taken;

(e) an update on changing landscape of compliance risk for the FI owing to changes in

regulatory approach/instructions etc. and plans to manage resultant compliance issues, as well as the need for any additional policies or procedures to deal with any new compliance risk.

(f) recommendations of corrective measures to address incidents of non-compliance and deficiencies in the management of compliance risk, including disciplinary actions;

(g) a record of corrective measures already taken and an assessment of the adequacy and effectiveness of such measures;

(h) Insights and observations regarding the compliance culture that exists in the organization or in specific parts of the organization that may give rise to compliance concerns.

G: Role of Internal Audit

I. The activities carried out by CF should be subject to periodic review by Internal Audit function of the FI. The scope of work should consider the adequacy, relevancy and completeness of compliance program, which includes CF's identification of material regulatory compliance risks and implementation of corresponding controls, the accuracy of reporting on compliance to Senior Management and the Board, the adequacy of resources available with CF, its independence and ability to perform its roles and responsibilities, the adequacy of CCO's authority and level to carry out its roles and responsibilities and an assessment of the effectiveness of the compliance oversight, data collection, regulatory return submission etc.

II. The findings of Audit report that are considered significant from compliance risk perspective should be shared, as appropriate, with CF. The internal audit department and CF can coordinate to ensure that proper and timely remedial actions are taken by responsible departments/units/function of the FI to address these deficiencies.

H: Training programs on compliance risk management

I. The CF is responsible for ensuring that need based/targeted training programs are designed to help spread the message of importance and significance of compliance risk management. This will help CF in creating the buy-in for activities of COs and will also enable recipients to understand the 'need' of compliance risk management.

II. To enhance the awareness of compliance risk, the CF may arrange in-house/outsourced training programs for employees at different hierarchal levels which covers, at minimum; 1) the nature and stock of regulations/policies/standards/market best practices under which they perform their activities 2) practical description of how the regulations affect the FI's operations, 3) the risks associated with non-compliance and their potential impacts on FI 4) a review of the FI's approach to manage its compliance risk, 5) their roles and responsibilities with respect to compliance risk, 6) the importance of creating a conducive compliance culture, 7) the significance of reporting incidents of non-compliance; and 8) suggestions for updates or changes to the FI's approach for managing compliance risk.

****