STATE BANK OF PAKISTAN

GUIDELINES ON INTERNAL AUDIT FUNCTION

The Team

S. No	Name	Designation
1.	Syed Irfan Ali	Executive Director, Banking Policy & Regulations Group
2.	Mr. Muhammad Akhtar Javed	Director, 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

DEFINITIONS

Administrative Reporting: It covers matters like approval of leave, staff loans, advances and claims as per FI's approved policies. However, for CIA, any exceptions from these policies shall always be approved by the BAC.

Audit Assurance: In the context of these guidelines it is an independent and reasonable assertion provided by FI's internal audit function (IAF), based on sufficient, relevant and reliable evidence; that FI's implemented system of internal controls is adequate and effective.

Auditable areas or Auditee: Any unit or activity within a FI subject to an audit.

Audit Universe: The potential activities/processes/functions/departments/units subject to an audit as determined/categorized by Internal Audit Function of the FI after discussions with management. The audit universe can be determined/categorized using vertical i.e. top-down approach or horizontal i.e. cross functional approach or a mix of the two.

Effective: A process/activity that successfully achieves the objectives it was established/undertaken for.

Financial Institution (FI): For these guidelines, the FI means all banks, DFIs and Micro Finance Banks.

Internal Auditing: "an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes (IIA)".

Management Audit: Also referred to as value for money auditing, performance auditing and efficiency auditing to review and evaluate performance of management (at all levels) in managing and utilizing available organizational resources in an efficient and effective manner.

Risk Management: A logical and systematic method of establishing the context, identifying, measuring, treating, monitoring and communicating the risks associated with any activity, function or process in a way that will enable the organization to minimize losses and maximize opportunities.

System of Internal Controls: The whole system of controls established and implemented by management to conduct its business activities in an orderly and efficient manner; to ensure adherence to applicable laws, rules and regulations; as well as ensure completeness and reliability of financial and management information.

Senior Management: Refers to the Chief Executive Officer and other key executives of FI as defined in Prudential Regulations (PRs) for Corporate & Commercial banking as amended by SBP from time to time.

INTRODUCTION

1. Owing to a rising trend of risk management & internal control failures in Financial Institutions (FIs) - both in developed and developing world- the Governance, Risk and Compliance (GRC) practices in FIs have been under a strong and critical public spotlight in recent years. While many challenges still persist, however, there is no denial of the fact that banking industry in Pakistan has, in past several years, undergone a complete makeover in almost all areas of their operations; i.e. improved governance and risk management practices; modernization of operations, development of new products & services, adoption of modern technologies, better customer services, etc. In addition to such transformation, the FIs have also shown their resilience in facing unfavorable business conditions by adjusting their business models and continuously improving their internal controls to meet the dynamic and growing needs of market participants.

2. The SBP, being a dynamic regulator, has always strived to strengthen its regulatory framework for FIs various operational activities in the light of changing market dynamics and international best practices. However, Internal Audit Function (IAF) is an area where more detailed regulatory guidance was still required. The IAF, being the third line of defense, is one of the fundamental components of overall governance framework in FIs that works on behalf of FIs' Board of Directors (BoD) to provide it an independent assurance on the adequacy and effectiveness of FI's system of internal controls.

3. The instances of institutional failure around the globe have forced global standard setting bodies and relevant regulatory authorities to recognize the need of strengthening of internal controls as well as establish a more pro-active, strong and independent IAF. On the other hand, the fast changing technological & business landscape, enhanced regulatory expectations, competitive market forces, increasing complexity of operations and ever changes risk profile of a FIs have compelled their boards & management to realize the importance of strong internal controls and the value that IAF can add in this process.

4. These changes and allied challenges to achieve organizational objectives call for a more robust, pro-active, risk focused and dynamic audit process supported by strong audit governance; policies, processes, tools and methodologies along with professional, competitive and dedicated internal auditors to help FI achieve its goals and objectives. In order to save itself from internal controls surprises, it is high time for FIs to further invest in building robust internal control environment that commensurate with the volume and complexity of its operations taking into account the specific context under which a FI operates and the long-term business objectives that it plans to achieve.

OBJECTIVES

1. The IAF being the Third Line of Defense (TLD) in internal controls system is one of the most important elements of overall control environment that provides an independent assurance of the adequacy and effectiveness of implemented policies, systems, processes, controls and sharia compliance (where applicable[1]). Besides, the existence of a robust, independent and effective IAF can provide sufficient comfort to regulatory/supervisory authorities on the overall governance, risk and compliance environment in the FI leading to a more efficient allocation of supervisory resources.

2. These guidelines communicate minimum regulatory expectations for a strong, independent and effective IAF. In addition to various other requirements, these guidelines re-emphasize the role and responsibilities of Chief Internal Auditor (CIA), internal auditors, BAC; and provides guidance on various aspects/components of end-to-end internal audit process. The FIs are encouraged to build on the foundation provided by these guidelines by adopting advanced tools, methods, approaches and processes for their auditing activities. As these guidelines try to cover entire audit life cycle and requires FIs to comply with the relevant international standards and the best practices on internal auditing, it can serve as a valuable tool for performance appraisal of IAF by regulatory authorities and Board Audit Committee (BAC).

[1] In case of full-fledged Islamic banks and conventional banks with Islamic banking operations, the Sharia audit shall be considered as an important part of scope of IAF activities. The relevant FIs shall take all possible measures to strengthen their sharia audit function in line with instructions of these guidelines.

BOARD AUDIT COMMITTEE (BAC)

1. The FI shall comply with all the relevant code/regulations (where applicable) with respect to establishment, composition, frequency of meetings and other related matters pertaining to the BAC. Besides, in order to be effective, the BAC members should, on collective basis, remain aware of latest trends and best practices of internal auditing enabling them to rigorously evaluate the effectiveness of audit processes and perform their roles & responsibilities more diligently.

Audit Committee Charter (ACC)

1. In order to streamline BAC operations, its affairs shall be governed under board approved 'Audit Committee Charter (ACC)' – commonly referred to as Terms of Reference(TORs) - that would serve as a 'blueprint' for its operations and delineate the basic framework for performing its assigned roles and responsibilities. While the ACC is supposed to be a uniquely customized document to capture the objectives, mission and overall organizational culture of the FI, it should at minimum, cover the following aspects of BAC:

- Objectives, Composition, Authority, and Frequency of meetings.
- Roles & Responsibilities.
- Frequency & mechanism of reporting to Board.
- Frequency & channel of communication with management.
- Performance evaluation mechanism of the Committee (by Board).
- Frequency of review of ACC.

The Board should, on an annual basis, review the performance & effectiveness of BAC[2] against the roles & responsibilities set forth in the charter and take immediate actions to fill the gaps.

2. In addition to existing roles and responsibilities as mentioned in relevant codes/regulations, the following shall be included in the relevant portions of ACC. The BAC shall;

1. Have complete authority & independence to perform its roles & responsibilities by either utilizing internal or external resources (if need be). Besides, the BAC should ensure independence of any investigations/disciplinary actions against CIA & internal auditors.
2. Facilitate Board in establishing an unambiguous & observable 'tone at the top' for strong and effective system of internal controls based on & supported by strong ethical practices, culture, comprehensive policies, procedures, processes and technological systems.
3. Establish, maintain and promote regular communication with senior management regarding deficiencies in internal controls; review actions taken by management to address identified deficiencies and ascertain new developments to achieve a uniform organization-wide commitment/buy-in for implementation of strong and effective internal controls.
4. Receive and review summary[3] of reported violations identified through internal audit activities and follow-up actions taken by management to ensure that audit observations/recommendations receive

[2] As stipulated in these guidelines, the expected role and responsibilities of a BAC is to provide a platform to CIA and IAF to present their findings and engage senior management to fill the identified gaps as swiftly as possible. However, the effectiveness, independence and how influential the BAC in a FI is, would, largely, depend upon the professional competence and relevant knowledge of the members of the BAC.

[3] The summary of audit observations presented to BAC should be comprehensive enough and must include all high risk or otherwise significant observations. The BAC should also be presented with a robust analysis and reports regarding the themes and trends of internal control breaches observed by IAF during the course of their audits including number & nature of identified medium & low

proper and timely attention by senior management. The BAC should also review the trends of audit observation from multiple dimensions to have deep insights into state of internal controls and must set specific, time bound action points/indicators to monitor improvements.

5. Report to board any significant matters identified by IAF/external auditors that warrant board's immediate attention.
6. Review effectiveness of whistle blowing procedures for receiving (through internal or external sources) complaints/concerns regarding business ethics/conduct practices, governance & risk management practices, controls over financial reporting, auditing practices etc. The BAC must ensure that such concerns are treated confidentially and that the reporting employee(s) are protected and not penalized in any manner whatsoever. The BAC should ensure that employees remain aware of i) existence of such procedures, ii) the procedure to utilize it and iii) are encouraged to be a 'whistleblower'.
7. Review and approve Internal Audit Charter (IAC) in the light of these guidelines. The IAC should include details on IAF's advisory role[4] providing the extent and nature of assignments/engagements that IAF may provide to management.
8. Provide its fullest support to IAF and internal auditors to perform their mandated activities independently and in objective manner.

MANAGEMENT

1. The management of the FI is primarily responsible for preparing, establishing, implementing and maintaining effective system of internal controls. In order to bring the needed improvements in the existing system of internal controls, the management should assimilate BAC thinking on internal controls and create desired 'tone' at management level by taking audit observations/ recommendations seriously and taking all necessary steps to fill the identified gaps as swiftly as possible. The IAF should also establish, formal or informal, regular communication channels with management as well as other internal control/governance functions (risk management, compliance, finance etc.) to remain aware of entity's future strategy/activities and allied risks.

2. In order to benefit from internal auditors' diverse experience, skill set and expertise in various areas of FI's business, the management is encouraged to engage IAF for consultative/advisory services under a clearly communicated and agreed upon scope of such assignments and nature of deliverables. Besides, if management intends to seek IAF[5] feedback on policies/new projects/other developments, it should do so at appropriate time so that the feedback of IAF can easily be incorporated at developmental stage. However, before accepting any such request of the management, the CIA should make it clear that internal auditors and/or IAF, individually or collectively, shall bear no responsibility of the subsequent implementation and/or consequences of the process/system/activity/product on which advice/feedback was provided to management.

---

risk observations. The reporting to BAC should be comprehensive enough, enabling BAC members to remain fully informed of the state of internal controls in FI.

[4] The IAF, after fulfilling the needs/requirements of its primary function of assurance, may utilize audit resources for consultancy/advisory services, however, the allocation of audit resources to consultancy/advisory services shall not be more than 10% of total audit resources at any given point in time. The decision for provision of advisory services by IAF and its extent shall rest with BAC (in consultation with CEO & CIA) to decide.

[5] It is a general practice in FIs that they include CIA as 'guest member' in various management committees to seek his/her feedback on various matters. While this practice may be easy to adopt, it may not be considered the most appropriate to seek IAF's input/feedback. Going forward, the FIs shall include CIA as 'guest member/observer' only in committees that pertain to risk & control functions like risk management, compliance, internal controls etc. Besides, the CIA may also attend all or part of FI's Management Committee (MANCOM) meetings as an observer to remain aware of the shift/changes in organizational goals and objectives or the strategy to achieve those goals and objectives.

3. The CIA should take all necessary steps to ensure that providing consultancy/advisory services by internal auditors does not in any way affect the independence of IAF as well as the availability of audit resources to conduct their primary function i.e. provision of independent assurance.

INTERNAL AUDIT CHARTER (IAC)

1. The 'Internal Audit Charter (IAC)' shall serve as a 'blue print' for IAF that defines the purpose, authority, scope, roles & responsibilities of IAF, roles & responsibilities of other stakeholders (senior management, auditees, other control functions) and other relevant information. The IAC should be reviewed & approved by BAC and should be updated on periodic basis to ensure its relevance.

2. The CIA in consultation with BAC should develop an IAC that caters to the specific needs of the FI in line with ACC and audit strategy, however, at minimum; an IAC should cover following areas:

a) The formal standing, authority, powers and responsibilities of IAF in the light of these guidelines, international best practices and Standards, FI specific factors etc.
b) The authority of IAF to openly and independently express its opinion on different affairs of the FI's overall control environment.
c) The purpose and scope of the IAF activities and roles & responsibilities of CIA, auditors and that of management (where relevant).
d) Internal auditors' unrestricted access to FI's records, files, data, information, meetings' minutes, people and properties.
e) The nature and extent of IAF's advisory/consultancy services provided by IAF, if any.
f) The organizational independence of IAF and independence & objectivity of auditors.
g) The IAF's reporting mechanisms to BAC and other relevant internal stakeholders.
h) The criteria for and the extent to which IAF may engage external consultants/experts to perform specific audit related tasks, if any[6].
i) The roles & responsibilities and performance evaluation mechanism of CIA.
j) The mechanism to ensure IAF's compliance with IIA Standards along with its periodic assessments.

ROLES & RESPONSIBILITIES OF CIA[7]

1. The Chief Internal Auditor (CIA) shall head the IAF and provide necessary direction & support to internal auditors in performance of their duties. In addition to roles and responsibilities of CIA given in various sections of these guidelines, the CIA shall have the following roles and responsibilities. The CIA shall;

1. Provide an independent assessment/opinion, without fear or favor, to BAC on annual basis on state of internal controls (including sharia compliance, where applicable) in the FI based on the audits conducted during the audit period supported by specific audit observations/conclusions.
2. Formulate the action plan and ensure its implementation to comply with IIA's International Standards for the Professional Practice of Internal Auditing (i.e. IIA Standards).

[6] However, such practices should be short-term in nature and only limited to such technical areas/risks where in-house expertise is not available. The CIA should hire/develop resources in IAF to address such risks/audit areas as early as possible. It must be noted that FIs can not outsource IAF activities in whole or any part there of.

[7] In case of Islamic Banking Institutions (IBIs) where, as per SBP's Sariah Governance Framework (SGF), the Sharia Audit is an independent function; it is the responsibility of Head of Sharia Audit department to comply with instructions of these guidelines in areas that are not covered in SGF. In case of any conflict between two instructions, the SGF instructions shall remain in force.

3. Ensure that the professional training needs of internal auditors are periodically identified & adequately met; the auditors demonstrate highest ethical and professional standards in performance of their duties and perform their work with dedication & diligence.
4. Ensure that FI's significant outsourcing arrangements are reviewed by IAF to protect FI's interests.
5. Ensure that IAF has adequate budget, systems, human resources[8] with relevant qualifications, expertise, competencies & skills, and other required resources to perform auditing activities.
6. Engage with internal audit teams on regular basis to provide guidance and to ensure that auditors performing the work have relevant technical and social skills, sufficient knowledge of the work being audited and are able to perform their responsibilities diligently.

ORGANIZATION OF IAF

1. All FIs shall establish and organize an IAF that best meets its objectives, complies with IIA Standards, does not hamper its independence and enhances its effectiveness & efficiency. The factors that determine the organization of IAF may include FI's size, jurisdictions served, complexity of operations, scope of audit activities, processes implemented etc. Whatever way the IAF is organized, it may be ensured that it shall not only be independent on 'paper' but its independence should also be 'visible' in practice. For this, the CIA must confirm[9] to BAC, at least annually, the organizational independence of IAF.

INDEPENDENCE AND OBJECTIVITY OF INTERNAL AUDITORS

1. In order to perform their responsibilities without any fear or favor and to arrive at unbiased & impartial judgments/conclusions regarding the internal controls, it is essential that internal auditors enjoy individual independence and are objective in their approach. The CIA in consultation with BAC should take all necessary actions to ensure individual independence & objectivity of internal auditors at assignment/engagement and/or functional levels. Some of these steps may be the following:

1) Whenever possible and without jeopardizing the competence and expertise of internal auditors, the internal auditors may be rotated within various divisions/sections of IAF relevant to their skill set & expertise.
2) Under a board approved rotation policy, transfer staff (with required skill set and if needed by IAF) from other functional areas of FI to IAF on periodic basis and in a systemic way that does not have any major negative impact on operations and performance of IAF.
3) Devise procedures (i.e. SOP) to address the issues of individual independence & objectivity that may arise after completion of rotation exercise to IAF. The procedure should provide for means to remove any conflict of interest of newly rotated staff by not assigning them the audit of activity that they were previously involved in/responsible for in line with the 'cooling off' period requirements of IIA Standards.
4) Put a mechanism in place whereby the internal auditors are required to disclose any conflict of interest with the activity being audited, arising either from their professional or personal relationships, prior to starting their audit assignments.
5) Ensure that the team, which provided advisory/consultancy services to management, is not assigned to audit the same auditable activity until completion of one audit cycle.

[8] The requirement of human resources for IAF should be based on a comprehensive workload assessments such that internal audit teams are provided with sufficient time to conclude their audit assignments without compromising on audit quality.

[9] The confirmation shall be given by CIA at the time of provision of annual assessment/opinion on state of internal controls and shall be duly recorded in minutes of BAC meeting.

6) Ensure that there are no undue scope/timeline limitations and/or funding deficiencies for audit assignments enabling internal auditors to have complete and comprehensive review of activity/function/process being audited before finalizing their judgment/conclusion.

RESOURCES/TRAINING

1. The CIA should ensure that IAF has the mix of professionally competent, technically sound, knowledgeable and skilled internal auditors capable of auditing all the core and support functions of FI.

2. The BAC in consultation with CIA should ensure that IAF staff is equipped with relevant auditing skills, knowledge, tools, methodologies, technique and competencies to perform their respective roles and responsibilities in an audit assignment/at IAF. The CIA should develop a comprehensive and continuous training program[10] for auditors at all levels in line with SBP guidelines on Training & Development as issued vide BPRD Circular # 12 of 2016. The BAC should ensure that IAF has sufficient budget available to impart required training to internal audit staff.

3. In addition to managerial skills, the internal auditors at senior/managerial level should have sufficient audit and business knowledge to understand and derive linkages from audit reports of various audit functions to construct a macro picture of deficiencies in internal controls.

INTERACTION WITH REGULATORS & EXTERNAL AUDITORS

The CIA should maintain a close coordination with SBP inspection teams and external auditors to seek their input on the state of internal controls in the FI. The exchange of information between IAF and SBP and between IAF & external auditors may help in transfer of knowledge/information on state of internal controls. Such coordination may help IAF to update its audit strategy/plan, revamp audit processes, increase audit resources etc. leading to an optimal utilization of audit resources as well as help in expanding the underlying expertise.

[10] Another way of promoting and encouraging learning & development initiatives at IAF could be holding of regular knowledge sharing sessions of auditors. In these sessions, the auditors may share their experiences and exchange information on various existing and new/developing topics of interest (related to internal audit or business of banking) that can help other auditors in performance of their duties.

SCOPE OF AUDIT WORK

The scope of every audit assignment may be different and distinct given variety of factors pertaining to activity/unit/function/department/office being audited, however, some general guidance on scope of audit work[11] in any or all of audit activities is provided below. The areas below are not exhaustive and may be expanded by internal auditor to achieve specific or general objectives of any audit activity subject to the conditions that doing so does not impair auditor's ability to perform its auditing activities and achieve its objectives.

i. Adequacy & Effectiveness of Internal Controls

It is the primary responsibility of internal audit to provide assurance on the adequacy and effectiveness of internal controls to ascertain whether controls are enough vis-a-vis risks of activity being audited and if controls are working/yielding results as intended. The internal auditors shall, regardless of the nature/type of audit activity being conducted, must test the relevant financial, operational & compliance controls to satisfy themselves about their adequacy and effectiveness. While forming conclusions about internal controls weaknesses, the auditors must be guided by the fact that effectiveness of internal controls is greatly influenced by the overall control/risk/compliance culture and does not happen in isolation. Hence, the auditors must be specific in identification of reasons of control weaknesses, which may be either due to its flawed design or incomplete/improper implementation.

While it may not be the primary responsibility of internal auditors to detect financial corruption, frauds, manipulations and other irregularities (collectively herein referred to as malpractices) during course of audit, however, they should implement proper planning and sampling procedures to be able to identify large-scale control breaches/deficiencies/ process loop-holes hat may lead to such malpractices. The subsequent emergence of such instances, if any, warrant a comprehensive review of adopted audit processes by CIA in consultation with BAC.

The internal auditors shall take due care in planning and execution of audit activity so that control breaches/deficiencies are timely identified. It is the responsibility of the audit team to recommend enhancement of audit scope and/or requires audit resources for business activities where the likelihood of occurrence of such malpractices is high. Besides, the IAF should conduct independent investigations or remain aware of such investigations (in FIs where fraud investigation unit is not housed in IAF) related to such malpractices (excluding immaterial errors or omissions) and major breach of controls.

ii. Reliability & Integrity of Management Information Systems (MIS)

The capacity, capability and reliability of MIS including that of its various components is of critical importance for any FI since majority of financial & operational decisions/actions taken are primarily based on or supplemented by the information generated from these systems. The internal auditors should, therefore, put special emphasis on the integrity and authenticity of information generated from these systems as well as the information/cyber security processes that are implemented to protect data & information so generated. The internal auditors should also evaluate the adequacy and effectiveness of such systems in identification, classification and reporting of captured data & information. The internal auditors should evaluate the control mechanism implemented by management for regulatory reporting using information systems and determine whether such controls are adequate and effective.

[11] All the mentioned areas here may not be applicable *in toto* on each and every audit activity that IAF undertakes, however, most of these areas may apply on majority of audit activates that audit undertakes. . However, the CIA/regional audit head/section audit head etc. and in-charge of audit team should ensure that the planned coverage & depth of audit assignment in hand commensurate with the risks involved in the activity being audited i.e. an activity or function with 'high risk' rating during audit planning shall have wider/expanded scope than it otherwise would have. Besides, in situations where there is a logical reason for expanding or limiting the scope of ongoing audit assignment, the reasons/justifications of the same must be documented and approved by competent authority as per audit policy/manual.

The internal auditors should review the accounting records maintained at respective department(s) of FI and ascertain the adequacy and effectiveness of controls implemented over financial data capturing, classifications, processing, valuations, and reporting. The internal auditors should also evaluate the communication policies, processes and procedures implemented by management to provide timely and relevant information across the organization to all concerned stakeholders.

iii. Expenditure Control & Safeguarding of Assets

The 'assets' referred here primarily include physical assets that a FI owns/controls to conduct its business activities. The internal audit must determine if the management has put in place adequate control mechanism to safeguard FIs physical assets against losses from theft, fire and unauthorized use. Besides, the internal audit shall assess & evaluate, in sufficient detail, the material[12] administrative expenditure incurred vis a vis budget and procurement process of capital assets (physical assets or otherwise like acquisition, development & implementation of technology solutions/systems, transformation projects etc.) and must identify and report anomalies and control deficiencies in such processes.

iv. Adequacy & Effectiveness of Risk Management Activities

The internal audit shall assess the adequacy and effectiveness of FI's risk management framework i.e. risk governance structures, policies, practices, processes, systems, activities etc. across the organization. Since the risk management activities may be performed by several different departments of the FI, the IAF should conduct an end-to-end review of cross-departmental processes (thematic reviews of risk management practices/activities in the FI) to take a holistic view of entity-wide risk management practices and to ascertain whether these are synchronized with each other, aligned with organizational objectives & risk exposures and are effective.

Besides, the internal auditors shall include, at minimum, the following points into audit scope of risk management functions/activities:

1) Adequacy and effectiveness of entity-wide risk governance framework vis-a-vis organizational risk profile especially in managing individual/inter-dependent/overlapping risks.
2) The adequacy and effectiveness of risk management structures, policies, practices, systems and processes for identifying, measuring, assessing, managing and reporting all kind of material risks (financial and non-financial) of the FI.
3) The risk management function(s) to have required stature and authority as well as sufficient physical, financial and human resources to carry out their mandated functions.
4) The overall risk/compliance culture in the FI and efforts made by risk management/compliance function(s) to inculcate risk/compliance culture in FI.
5) The capacity, relevance, integrity, reliability, completeness and comprehensiveness of risk management information systems and timely reporting of such information to all relevant stakeholders across the FI for informed decision-making.
6) Evaluate adopted stress testing processes to ascertain their reasonableness, reliability, frequency, scenarios used, assumptions employed and if its results are used in decision-making.
7) Evaluate the validity of adopted risk models based on which several management decisions are based. The evaluation may include, among other relevant things, the verification of consistency, timeliness of data used in the model and independence and reliability of data sources.

[12] The term materiality may have different interpretations/thresholds at different FI and even in same FI for different functions/activities/units/activities/processes that are present in audit universe. The IAF may determine the materiality of any administrative of capital expenditure in the given context/audit assignment.

8) Evaluate whether risk management processes adapts to the internal and external changes and takes into account the impact of emerging risks and whether decision makers consider those risks in making decisions.

v. Information Technology (IT) and Shari'ah Audit

The scope of the audit of FI's IT operations and reporting of its audit observations shall be same as given in SBP's instructions on Information Security audit issued vide BSD Circular # 8 of 2005 and SBP Guidelines on Enterprise Technology Governance issued vide BPRD Circular # 05 of 2017. The CIA should enhance the scope of IT audit to include other IT related operations that are not covered in above-mentioned guidelines. The IT audit program given in above-mentioned guidelines shall be made part of annual risk based audit plan in light of these guidelines. Besides, the IAF shall follow SBP's instruction on Sharia Audit as given in Sharia Governance Framework issued vide IBD Circular # 1 of 2018 and all other regulations on the matter issued by SBP from time to time.

All such instructions of IAF guidelines that are not covered in any of the above guidelines/instructions (with respect to IT & Sharia Audit) shall remain applicable on FIs for IT & Sharia audit as well.

Besides, keeping in view the increasing dependence FIs operations on the IT & allied infrastructure in conduct of its normal business operations, the CIA should ensure that its IT audit function is strong and robust enough to identify the weaknesses/deficiencies in FI's systems in the light of relevant regulatory instructions and best international practices.

v. Management Audit

The internal auditors shall, during management audits, focus on the conduct of senior/middle management with a focus on **i)** appropriateness of the process through which material or important decisions are made **ii)** the level of understanding (at senior & middle management level) of regulatory requirements pertaining to their area of operations, **iii)** level of risk/compliance awareness at senior & middle management level; **iv)** the extent of use of business and/or risk information in making decisions **v)** issue of understaffing/overstaffing and **vi)** ability & willingness of senior & middle management to use resources optimally and **vii)** compliance of regulatory policies, internal policies, processes and procedures in conduct of their responsibilities.

The internal audit shall highlight in their audit reports, the instances of non-productive & redundant policies, activities & processes; processes that could be automated to increase efficiency; deficiencies in planning, design and implementation of material or important projects/initiatives and deficiencies in overall decision-making processes that led to or resulted into the undesired outcomes. In addition to above, the auditors shall review whether:

1) Clear and measurable objectives and goals are set for business functions/activities and are properly communicated to all employees and are being regularly monitored.
2) Evaluation yardsticks (Key Performance Indicators-KPIs) are established for the department/function/unit/activity concerned, communicated to staff and used at the time of annual performance appraisal.
3) Any major deviations from planned activities are timely identified, properly documented, analyzed, investigated and reported to the senior management and the Board (where necessary).
4) Business functions have adopted a thorough decision making process before initiating any major project/program by considering the risks, opportunities & threats involved.

5) The assumptions used by management for developing business/strategic plan for a particular function/activity and/or for FI as a whole are relevant, appropriate and reasonable and if the targets/objectives set, are clear and achievable.
6) Established system/procedures for planning, evaluating, authorizing and controlling the use of resources are operational and effective.

AUDIT STRATEGY & PROCESSES

INTERNAL AUDIT STRATEGY

1. The CIA shall develop a multiyear audit strategy for IAF that can further be divided into annual risk based audit plans. The audit strategy is to be approved by board on recommendations of BAC and must set out the long-term vision, mission and objectives of IAF. The audit strategy shall be aligned with organizational vision, mission and objectives such that it helps senior management to achieve goals and objectives.

2. The audit strategy must determine the priority areas/risks/activities for audit and other contribution that IAF can make, through improvement of control environment, leading to achievement of organizational goals. The CIA could review the allocation of audit resources to various audit activities over past many years and come up with areas that may not have been properly reviewed or audit resources that may have been underutilized/mis-utilized and can thus be made part of strategy going forward.

3. The audit strategy shall be developed after thorough consultations with board, BAC, & CEO (through BAC) of FI keeping in view the objectives of audit activities as well as expectations of these stakeholders. The strategic plan shall be flexible enough to adapt to changes in organizational strategy, business activities, risk exposures, organizational structures, mergers, acquisitions, etc.

RISK BASED AUDIT PLAN (RBAP)

1. The CIA should develop a risk based audit plan on annual basis in line with FI's internal audit charter and strategy. The annual RBAP should be approved by BAC and must provide for best and efficient use of available audit resources enabling CIA in providing an objective opinion on the state of internal controls. Since the audit resources would always be limited against the demand of assurance (and advisory services, if any) from various internal stakeholders and/or regulatory authorities, the formulation of a balanced RBAP may thus be a challenging task for CIA. The CIA shall make all efforts to strike a balance[13] between RBAP's breadth and depth such that it sufficiently covers all important areas to provide valuable insight into state of internal controls.

2. The audit plan should set out the audit universe, scope of coverage, frequency of audit, resources required and duration of each audit assignment. The frequency and scope of an audit assignment as well as resources required should be based on the prior risk assessments[14] of auditable areas by IAF. Such risk assessments should be conducted only for the purpose of risk based audit planning and may not be used for any other purpose outside IAF.

3. Besides, the CIA must describe in audit plan, the extent of IAF's reliance (if any) on other assurances providing functions i.e. risk management, internal control and compliance functions, while performing audit activities. Any such reliance, however, should be well thought out, well founded, reasonable & limited in nature, fit to meet audit objectives and in no way compromise the independence & objectivity of auditors. Even when auditors are relying on the output of these functions, the internal auditors should evaluate their accuracy & relevance on test-check basis and should not accept or act on the content of their reports/information blindly. Nonetheless, all the audit observations that are based on or supported by these

[13] The CIA in consultation with BAC should determine what needs to be audited from within the audit universe. Besides, keeping in view the maturity of risk management and state of internal controls in FI, the CIA may choose to develop a blended internal audit plan that includes both 'risk based audits' and 'conventional control audits' depending on the nature and objectives of each specific audit assignment in the plan.

[14] In addition to results of risk assessments, the IAF may also define other criteria like, management's request, mandatory audits, legal & regulatory requirements, etc. based on which audit of an activity/function/unit may be included in the annual audit plan

functions' reports shall invariably be owned & defended by audit team at the time of finalization of audit reports.

4. While developing RBAP, the CIA must ensure that all areas of regulatory importance are covered in sufficient detail. Some of such activities/functions may include all those policies, processes, systems and governance structures that are established in response to various laws, rules, regulations, instructions and guidelines of regulatory authority.

5. The CIA shall ensure that audit plan is implemented as planned and shall review and submit its implementation status to BAC on quarterly basis. Any deviations of the plan should be documented and presented to BAC on regular basis. In addition, the CIA shall ensure that the audit plan is reviewed subsequent to significant change(s) in FI over time i.e. mergers & acquisition, structural changes, establishment of new business lines, reorganization of functions etc. so that the plan remains relevant.

RISK BASED INTERNAL AUDIT (RBIA)[15]

1. RBIA is a systematic process and an approach that ensures efficient utilization of internal audit resources by allocating greater audit resources to the more risky areas where the existing or potential weaknesses/deficiencies in internal controls may have serious financial or operational consequences for the FI. RBIA shall be designed to start from big picture[16] and trickle down to various processes/systems/audit activities thereby understanding and defining linkages of one activity to the other and assessing its importance in overall control environment/audit universe. The RBIA if designed & implemented properly would make the contribution of IAF duly 'visible' in improving risk management & control processes to 'manage[17]' entity wide risks, thereby contributing in achieving organizational goals.

2. Besides, the success of RBIA greatly depends on the design and implementation on the risk assessment policy as well as the sampling methodology adopted by IAF. Hence, the risk assessment and sample selection methodologies/processes are of critical importance in risk based auditing. The IAF shall use the guidance of international standard setting bodies for developing risk assessment and audit sampling policies/methodologies/processes.

RISK ASSESSMENT FOR THE PURPOSE OF INTERNAL AUDIT

[15] RBIA emphasizes management's responsibility for managing risks and is meant to add value to organization by identifying deficiencies in risk management processes where they matter the most. RBIA is in fact a change of mindset on part of internal auditors requiring them to enhance their engagement with auditee, to understand the way they conduct their business, obtain different pieces of information from different sources and integrate the same to take a holistic view of the activity being audited and provide specific risk driven audit opinions/findings.

[16] The RBIA approach requires a broad understanding and in-depth experience of business as well as audit processes and hence may require CIA to invest in new/existing internal auditors by providing them relevant trainings on skills and competencies required to conduct audits under RBIA regime.

[17] The management of risks is, primarily, the responsibility of management. The IAF is responsible to provide independent assurance on the adequacy & effectiveness of the internal controls implemented by management. Hence, the auditor's job is to i) assess the adequacy & effectiveness of implemented controls against identified risks and ii) to assess whether all material risks in a process/activity/function have been duly identified by management or not. If audit identifies a risk that was not identified (and therefore not managed i.e. no implemented controls) by management before, the audit should identify such control deficiencies and form their opinion on state of internal controls in the respective activity/process/department/function etc. In FIs where risk management processes/systems are strong and mature, risk registers are in place and risk awareness is high; the implementation of RBIA is more smooth and successful.

1. The risk assessment is fundamental tenet of 'Risk Based Internal Audit (RBIA)' framework. The CIA shall develop a robust, BAC approved, risk assessment policy[18] delineating the processes, methodologies and internal mechanism for conducting such risk assessments. The risk assessment policy adopted by IAF should be in line with IIA's Standards and must provide for risk assessments at various levels e.g. entity-wide and auditable unit/activity/function/processes level keeping in view the size and complexity of FI's operations. Besides, these risk assessments should be broad based and cover all essential elements of auditable unit being assessed. The results of such risk assessment shall be used by IAF as a basic and important input for formulation and execution of audit strategy and/or annual RBAP.

2. The risk assessments conducted by IAF must be independent[19] of risk assessments conducted by 'risk management and/or compliance departments' of the FI and may be supplemented with feedback of BAC, other board committees and senior management (if so desired by BAC). The adopted risk assessment methodology should be robust enough to not only assess the risks of certain activity/process in isolation (which may declare it as low risk and out of IAF radar), but also takes into account the interactions/combinations[20] of other risk factors which, if considered, may change the results of the risk assessments. The risk assessment exercise should be conducted on at least annual basis or when IAF receives new information or identifies (before start of audit assignment) issues that may warrant a revision in risk assessments.

3. While implementation of RBIA may warrant significant changes in audit planning phase and the 'approach' of individual internal auditors in execution of audit activity and reporting of its results, however, the typical audit techniques/methodologies used to collect and analyze information/evidence may largely remain the same[21].

AUDIT RESULTS & REPORTING

1. The internal auditors must prepare a comprehensive internal audit report to communicate their observations/conclusions/findings on the state of internal controls and make recommendations to management for improvements. Before finalizing audit report, the audit team should discuss the draft audit report with management and must maintain complete record of discussions held and the decisions taken along with reasons/justifications. Besides putting their observations in audit report, where required, the internal auditors should immediately report any significant control breaches identified during the course of audit to CIA. Keeping in view the gravity of the matter, the CIA may refer the matter to BAC and CEO to take necessary and timely action.

2. The CIA should put in place a robust 'quality assurance mechanism' in IAF to ensure that the audit report and the 'audit rating/integrated audit rating' assigned to an audited area and/or administrative units

[18] This policy and allied procedures can be a separate document or part of Internal Audit manual.

[19] The IAF should, keeping in view the adopted business strategy, form an independent view if the key risks to the FI are being identified, including emerging and systemic risks, and assess how effectively these are being managed. The audit department can, however, use the results of risk or compliance functions' risk assessments, if any, as an input in their risk assessments. However, the extent of such reliance should be disclosed in annual audit plan of respective year and due professional care be exercised to ensure that IAF's independent view is not influenced by the management or risk function views.

[20] There may be various business processes/activities where the residual risk impact might be low/high but the frequency of occurrence may be high/low, in such cases when seen in combination with other risks with similar characteristics the resultant risk may transform into something that may have a very different impact as compared to its actual potential.

[21] This may hold true only if the implemented audit process/techniques/methodologies are up to date and in line with international standards on internal auditing.

representing collection of auditable areas (like regions to manage certain number of branches/other operations) meet the set quality standards (as given in audit manual or any other relevant policy). The audit reports must be backed by sufficient evidence/supporting material to justify auditors' findings/conclusions/judgments as well as overall audit ratings. The auditors should, in addition to highlighting breaches, must also ascertain and highlight in audit report the 'root cause' of the high risk observation and give proper recommendations that address that 'root cause'.

3. During discussions of draft audit report, there may arise a situation where there could be a difference of opinion on the observations/conclusions/judgments made by internal auditors in audit reports and management's point of view on these audit results. In such a scenario, the position taken by internal auditors/CIA would be considered as final and management shall implement all such audit recommendations in letter and spirit. However, in order to provide management a chance to present its point of view, CIA in consultation with BAC may establish a mechanism where such exceptional and significant cases of disagreement may be elevated at BAC level and decisions be taken accordingly.

4. The CIA should put in place a mechanism to ensure that final audit reports are objective, clear, relevant & comprehensive in content, written in positive tone to the extent possible (without compromising the criticality of the issue) and must provide strategic & specific insights to help management improve processes/controls to increase efficiency. The audit reposts should be free from errors and distortions and must communicate a fair, impartial and unbiased view on state of internal controls at audited activity. The CIA is free to decide the format, structure and contents of audit report depending on the nature of assignment, however, in general the audit report of a full scope audit assignment should, at minimum, contain the following;

a) An executive summary.
b) The audit team, scope, period covered, objectives and audit techniques/methodologies used.
c) The processes/systems/policies/data/information reviewed & evaluated; level & nature of engagement with auditee.
d) The significant/key findings of the internal auditors, risks involved and possible impacts.
e) The underlying weaknesses/control deficiencies/root causes of identified high risk audit findings (the audit team should include allied factors like shortage of staff, system unavailability, excessive workload, training deficiency of employees etc. in their audit reports that serve as basis of control breaches/violations).
f) Recommendations to correct identified deficiencies along with action owners & timelines.
g) Management comments on the deficiencies highlighted/recommendations made; remedial measures taken or proposed to be taken by management to implement recommendations.
h) Major changes that have taken place during the audit period, if any (related to activity being audited)
i) Any other information that needs to be conveyed by internal auditors to management and/or other users of audit report.

FOLLOW UP OF AUDIT REPORT/RECOMMENDATIONS

1. The CIA must establish a robust follow-up, validation and escalation mechanism for audit findings & recommendations at IAF. After issuance of final audit report, the IAF should actively monitor the compliance of audit findings & recommendations by management and regularly report the summary of compliance status to BAC. In cases where the management is not taking serious note of audit observations or the action plan is vaguely designed that may not adequately cater to risks/control deficiencies highlighted by audit team; the CIA should take up the matter with BAC & CEO to implement audit recommendations.

2. Instances, where the same deficiency/control breaches of critical nature are also highlighted in next audit of the audited activity, a comprehensive review may be conducted by IAF to identify and understand the root cause of the recurrence and make appropriate recommendations. The control breaches of critical nature that keep on occurring in at-least two audit periods despite implementation of audit recommendations should be tagged accordingly and submitted to BAC on regular basis. The CIA in consultation with BAC should identify the problem and evaluate whether there were issues in audit recommendations or if the management's action plan was flawed that the problem persists. Such a scenario also indicates that either the IAF is not effective in performing its tasks or the management is unable and/or unwilling to perform its responsibilities with respect to internal controls. The BAC must take strict note of such situation and take all necessary actions/steps to correct the problem.

RECORD KEEPING OF AUDIT REPORTS & WORKING PAPERS

The CIA should establish a robust mechanism for filing/record keeping of audit reports and audit working papers at a safe and secure place, preferably in a system, to ensure that their contents remain confidential and are only accessible, at all times, by authorized persons. The internal audit working papers should be properly filed, indexed and stored/archived in a secured place that can be easily accessed and retrieved by authorized persons as and when needed. A physical or electronic logbook should be maintained to record the movement of audit report & working papers.