Rural Bankers Association of the Philippines

Annual National Convention
May 19, 2015

1. BSP Circular 871 on Internal Control and Internal Audit Function
2. Evolution of Internal Audit
3. Risk-based Audit Methodology (Planning Stage only)
4. Q & A

BSP Circular 871 dated February 2015

Section 1. Internal Control Framework

(a) Section X185. Internal control framework

(b) Subsection X185.1 Management oversight and control culture

(c) Subsection X185.2 Risk recognition and assessment

(d) Subsection X185.3 Control activities

(e) Subsection X185.4 Information and communication

(f) Subsection X185.5Monitoring activities and correcting deficiencies

Section 2. Deleted (Minimum internal control measures provided under Annex A)

Section 3. Internal Audit Function

X186.1 **Qualifications of Chief Audit Executive (CAE)**

X186.2 **Duties and responsibilities of the CAE**

X186.3 Professional competence and ethics of the IA function

X186.4 Independence and objectivity of the IA function

X186.5 Internal audit charter

X186.6 Scope

Section 4. Trust

Section 5. Non-bank FIs

Sec.X186.1 Qualifications of the Head of the IA Function

Must have :

- **an unassailable integrity,**
- **relevant education/experience/training**
- **an understanding of the risk exposures of the bank**
- **competence to audit all areas of its operations.**

Sec.X186.1 Qualifications of the Head of the IA Function

He must also possess the following qualifications:

Complex	Simple and Non-complex
• must be a graduate of any accounting, business, finance or economics course with technical proficiency on the conduct of internal audit	
• must have at least five (5) years experience in the regular audit (internal or external) of a TB, national coop bank, QB or trust entity or, at least three (3) years experience in the regular audit (internal or external) of a UB or KB.	• must have at least two (2) years experience in the regular audit (internal or external) of a UB, KB, TB, RB, Coop bank, QB or NSSLA.

Sec.X186.2 Duties and responsibilities of the CAE

(3)To ensure that the internal audit function complies with sound internal auditing standards such as the **Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*** and other supplemental standards issued by regulatory authorities / government agencies, as well as with **relevant code of ethics**;

International Professional Practices Framework (IPPF)

Mandatory Guidance

The three mandatory elements of the IPPF are:

- **Definition of Internal Auditing**
- **Code of Ethics**
- **International Standards for the Professional Practice of Internal Auditing (Standards)**

Definition of Internal Auditing

Internal auditing is 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**.

Code of Ethics

- Integrity
- Objectivity
- Confidentiality
- Competency

Attribute Standards

1000: Purpose, Authority and Responsibility

1100: Independence and Objectivity

1200: Proficiency and Due Professional Care

1300: Quality Assurance and Improvement Program

Attribute Standards

1000: Purpose, Authority and Responsibility

1100: Independence and Objectivity

1200: Proficiency and Due Professional Care

1300: Quality Assurance and Improvement Program

- IA has to be audited by an independent validator once every 5 years.

Attribute Standards

1000: Purpose, Authority and Responsibility

1100: Independence and Objectivity

1200: Proficiency and Due Professional Care

1300: Quality Assurance and Improvement Program

- IA has to be audited by an independent validator once every 5 years.
- Big banks now have internal validators who do annual review of the internal audit function.

Performance Standards

2000: Managing the internal audit activity

2100: Nature of work

2200: Engagement Planning

2300: Performing the Engagement

2400: Communicating Results

2500: Monitoring Progress

2600: Communicating the Acceptance of Risks

Evolution of Internal Auditing

ART

Auditing Real Time

Evolution of Internal Auditing – Audit Approach

Control-Based

- Compliance with laws, regulations, policies & standards
- Financial accuracy of account balances
- Operations of specific controls or procedures

Process-Based

efficiency and effectiveness of key operational processes

Risk-Based

Key risks are mitigated to an acceptable level

NOTE: Maturity of auditors is a requisite

Risk Management Based

Risk management activities are effectively managing the key risks to an acceptable level

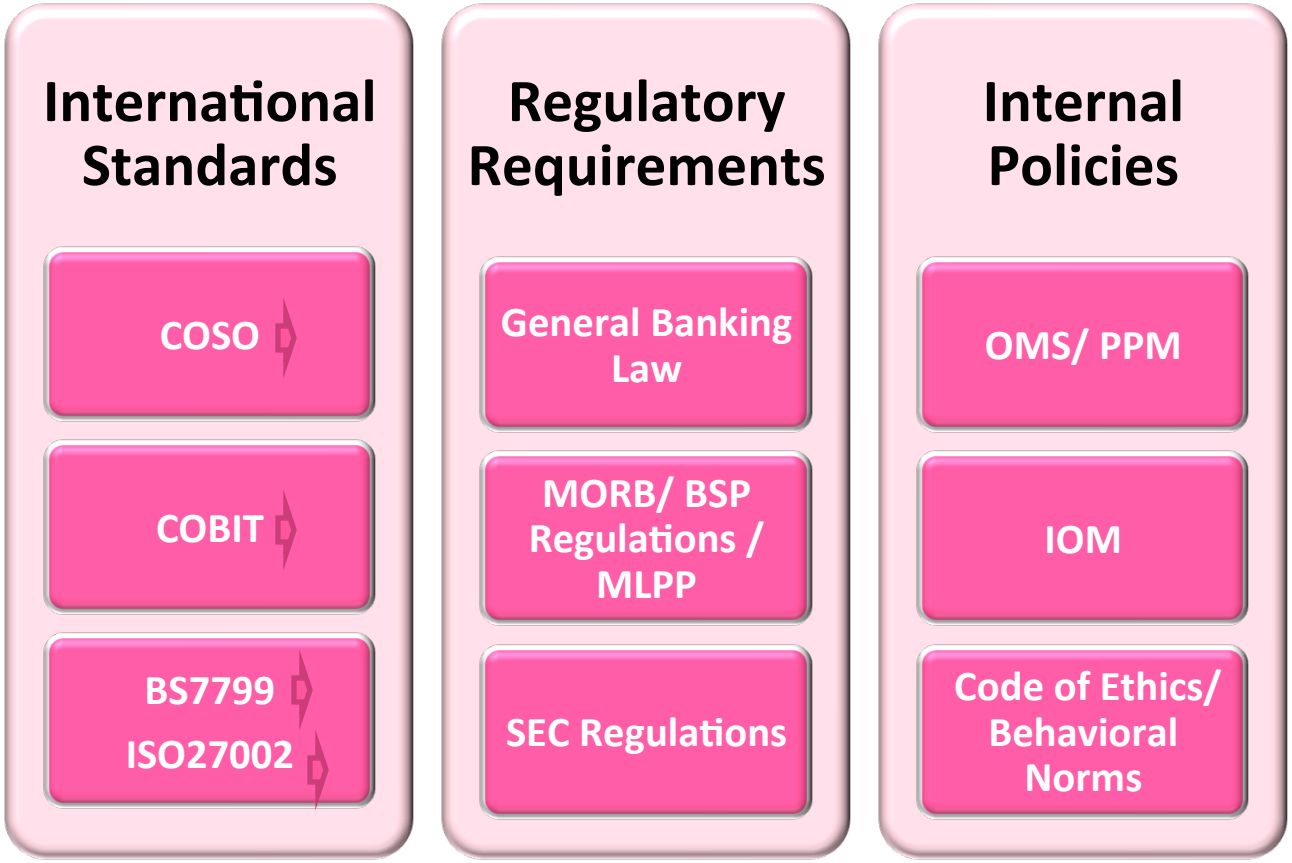
e.g. Risk and Control Self-Assessment (RCSA) is in place

Stakeholders-Based

The audit plan is **reflective of stakeholder expectations**, a risk-based prioritization , and the appropriate coverage of financial compliance , and operational **needs of the business**.

Risk-based Auditing

Internal Control Framework



Methodology used to select areas of coverage and frequency of audit

Methodology used to select areas of coverage and frequency of audit

Step 1

Identification of Audit Universe

	As of XXXX
Branches	XXX
Head Office Units	XXX
Information Systems: -General Controls -Application Systems	 XX XX
TOTAL	XXX

Step 2

Risk Assessment

Key Variables for Risk Assessment Measurement Evaluation:

40% Vulnerability	30% Control Environment	30% Materiality

Vulnerability – prone to attack, degree of automation, complexity of unit, volume of transaction, risk inherent to type of business, where the transactions take place
Control Environment – last audit rating, organization, outstanding risk issues, adequacy of system, customer impact, RCSA, policies and procedures
Materiality – severity of impact to bank (balance sheet), types of clients being serviced, potential financial loss

Methodology used to select areas of coverage and frequency of audit

Step 2

Risk Assessment – 2

Perform risk assessment using the corresponding defined matrix

Step 2

Risk Assessment – 3

Determine the Audit Cycle of each auditable unit

Risk Level	Risk Score	Frequency of Audit
High	4.00 to 5.00	Annually
Medium	2.50 to 3.99	Once every 2 years
Low	Below 2.5	Once every 3 years

Step 2

Risk Assessment – 4

Other Criteria in determining the Audit Cycle thru Risk Assessment

- ❑ The following shall be audited annually:
  - Those obtaining 'Below Acceptable' or 'Unsatisfactory' Rating in the previous audit.
  - Those required by Regulations to be reviewed annually

- ❑ No unit shall remain unaudited for more than X years.
- ❑ A unit may be audited more than once a year as deemed necessary.
- ❑ Requests from senior management and audit committee should also be considered in this phase.

Methodology used to select areas of coverage and frequency of audit

Steps 3 & 4

1. Alignment of Audit Plan with the Bank's strategic goals (Refer to the Book of Mandates prepared annually)
2. Obtain inputs from Senior Management and the Audit Committee.

Steps 6 , 7 & 8

1. Prepare the Audit Work Plan
2. Match with Audit Resources
3. Secure approval from the Audit Committee
4. Continuous monitoring of the audit work plan

Steps 5

Other Activities Performed by Audit

A. With Risk Assessment
1.Post Implementation Reviews
2.System Development Life Cycle Reviews
B. Without Risk Assessment
1. Continuous Audit activities
2. Fraud Investigations
3. Products and Channels Review
4. Consultancy services (with prior Audit Committee approval)
5. Other senior management requests (bidding, promos, etc.)

Risk-based Methodology

1. Planning
2. Selection and Training of Auditors
3. Audit Program Development
4. Implementation / Recommendation
5. Reporting / Assurance / Audit Rating
6. Monitoring / QA / Corrective Actions

1. BSP Circular 871 on Internal Control and Internal Audit Function
2. Evolution of Internal Audit
3. Risk-based Audit Methodology (Planning Stage only)
4. Q & A

Reminder

" The superior man, when resting in safety, does not forget that danger may come.

When in a state of security he does not forget the possibility of ruin.

When all is orderly, he does not forget that disorder may come.

Thus his person is not endangered, and his States and all their clans are preserved."

Confucius

THANK YOU!

WHAT IS COSO

- Stands for Committee of Sponsoring Organization - of the Treadway Commission
  - A voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls and corporate governance.
  - Formed in 1985
- Internal Control – Integrated Framework
  - A process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding achievement of objectives.

COSO Integrated Internal Control Framework

CONTROL ENVIRONMENT	Control environment refers to the foundation for all other components of internal control. Broadly divided into *hard controls* (organizational structure, assignment of authority and responsibility, and HR policies and practices) and *soft controls* (ethics, commitment to competence and management operating style).
RISK ASSESSMENT	Management's identification and assessment of relevant risks from all sources related to the achievement of established objectives. Management may avoid, diversity, control, share, transfer or accept risks.
CONTROL ACTIVITIES	Control activities which are the policies and procedures throughout the organisation to help ensure management directives and risk mitigation strategies are carried out.
INFORMATION & COMMUNICATION	Information required to run and control the business including those for business decision making and external reporting. Communication includes internal communication throughout the organisation and interactions with all external parties.
MONITORING	Management's monitoring of the internal control systems to assess the quality of the systems performance over time.

CONTROL ENVIRONMENT

- Sets the tone of the organization.
- The foundation for all other components.
- It includes the integrity, ethical values and competence of the people.
- Reflects: management's philosophy & operating style, the way management assigns authority and responsibility and organizes and develops its people, and the attention and direction provided by the board of directors.

RISK ASSESSMENT

- Every entity faces internal & external risks.
- Every entity sets objectives.
- Risk assessment is the identification and analysis of relevant risks to achievements of the objectives.
- Risk analysis
  - Risk assessment
  - Risk management
  - Risk monitoring – at the process level, activity level and entity level.

CONTROL ACTIVITIES

- The policies and procedures that help ensure management directives are carried out.
- They help ensure that necessary actions are taken to address risks.
- Control activities occur throughout the entity at all levels and in all functions.
- They include activities such as approvals, authorization, reconciliations and segregation of duties.

INFORMATION AND COMMUNICATION

- Relevant information must be identified , captured and communicated in a form & timeframe that enables people to carry out their responsibilities.
- Information systems produce reports containing operational, financial and compliance –related information that make it possible to run and control the business.
- Effective communication must occur in a broader sense, flowing down, across and up the organization. All personnel:
  - must receive a clear message from top management that control responsibilities must be taken seriously.
  - must understand their own role in the internal control system, as well as how individual activities relate to the work of others.
  - must have a means of communicating significant information upstream.

INFORMATION AND COMMUNICATION

- Communication takes such forms as:
  - policy manuals
  - memoranda
  - bulletin board notices
  - Another powerful medium is the action taken by management in dealing with subordinates
- Examples:
  - Open discussion of problems
  - Dissemination of information
  - Availability of sources of information and assistance
  - Systems that give data in the form that help management of activities
  - Data readily accessible to those who need it.

MONITORING

- Internal control systems need to be monitored to determine whether it continues to be relevant and able to address new risks.
- Types of monitoring:
  - ongoing during the course of operations.
  - evaluation for which the scope and frequency will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures.
- Examples:
  - Branch Head reviews deposit balance vs. trial balance
  - System-generated reports are checked vs. physical assets
  - Review of expenses against budget
  - Addressing cited issues

COBIT FRAMEWORK

Control Objectives for Information and related Technology published by IT Governance, Institute to provide a framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.

PLAN & ORGANIZE

- PO1 Define a Strategic IT Plan
- PO2 Define the Information Architecture
- PO3 Determine Technological Direction
- PO4 Define the IT Processes, Organization & Relationships
- PO5 Manage the IT Investment
- PO6 Communicate Management Aims & Directions
- PO7 Manage IT Human Resources
- PO8 Manage Quality
- PO9 Assess and Manage IT Risks
- PO10 Manage Projects

ACQUIRE & IMPLEMENT

- AI1 Identify Automated Solutions
- AI2 Acquire & Maintain Application Software
- AI3 Acquire & Maintain Technology Infrastructure
- AI4 Enable Operation and Use
- AI5 Procure IT Resources
- AI6 Manage Changes
- AI7 Install & Accredit Solutions

DELIVER & SUPPORT

- DS1 Define & Manage Service Levels
- DS2 Manage 3rd Party Services
- DS3 Manage Performance & Capacity
- DS4 Ensure Continuous Service
- DS5 Ensure Systems Security
- DS6 Identify and Allocate Costs
- DS7 Educate and Train Users
- DS8 Manage Service & Incidents
- DS9 Manage the Configuration
- DS10 Manage Problems
- DS11 Manage Data
- DS12 Manage the Physical Environment
- DS13 Manage the Operations

MONITOR & EVALUATE

- ME1 Monitor & Evaluate IT Performance
- ME2 Monitor & Evaluate Internal Control
- ME3 Ensure Regulatory Compliance
- ME4 Provide IT Governance

BACK TO MAIN

WHAT IS BS7799

The 10 Sections of BS7799:

1. Security Policy
2. Organization/Objectives
3. Asset Classification Control
4. Personnel Security
5. Physical and Environmental Security
6. Computer and Network Management
7. System Access Controls
8. System Development and Maintenance
9. Business Continuity and Disaster Recovery Plan
10. Compliance

BS 7799

Security Policy	To provide management direction and support on security.
Security Organization	1)To manage information security within the Company ; 2)To maintain the security of organizational information processing facilities and information assets accessed by third parties ; 3)To maintain the security of information when the responsibility for information processing has been outsourced. to another organization
Asset Classification	To maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.
Personnel Security	1)To reduce risks of human error, theft, fraud or misuse of facilities; 2)To ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work; 3)To minimize the damage from security incidents and malfunctions and learn from such incidents

BS 7799

System Access Control	**1)To control access to information ; 2)To prevent unauthorized access to information systems ; 3)To ensure the protection of networked services ; 4)To prevent unauthorized computer access ; 5)To detect unauthorized activities; 6)To ensure information security when using mobile computing and tele-networking facilities**
System Development and Maintenance	**1) To ensure security is built into operational systems; 2) To prevent loss, modification or misuse of user data in application systems; 3) To protect the confidentiality, authenticity and integrity of information; 4) To ensure IT projects and support activities are conducted in a secure manner; 5) To maintain the security of application system software and data**

BS 7799

Business Continuity and Disaster Recovery Planning	**To counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.**
Compliance	**1) To avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements 2) To ensure compliance of systems with organizational security policies and standards 3) To maximize the effectiveness of and to minimize interference to/from the system audit process.**

WHAT IS ISO27002

- **ISO/IEC 27002** is an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), entitled *Information technology – Security techniques – Code of practice for information security management*.
- ISO/IEC **27002**:2005 has developed from BS7799, published in the mid-1990s. The British Standard was adopted by ISO/IEC as ISO/IEC 17799:2000, revised in 2005, and renumbered (but otherwise unchanged) in 2007 to align with the other ISO/IEC 27000-series standards.
- ISO/IEC 27002 provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS). Information security is defined within the standard in the context of the C-I-A triad:
- *the preservation of confidentiality (ensuring that information is accessible only to those authorized to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorized users have access to information and associated assets when required)*

BACK TO MAIN

WHAT IS ISO27002

The 15 Sections of ISO27002:

1. Structure
2. Security Policy
3. Organization of Information Security
4. Human Resources Security
5. Asset Management
6. Access Control
7. Cryptography
8. Physical and Environmental Security
9. Operations Security
10. Communications Security
11. Information Systems Acquisition, Development, Maintenance
12. Supplier Relationships
13. Information Security Incident Management
14. Information Security Aspects of Business Continuity
15. Compliance

BSP Circular 871

Section 1. Internal Control Framework
(a) Section X185. Internal control framework
(b) Subsection X185.1 Management oversight and control culture
(c) Subsection X185.2 Risk recognition and assessment
(d) Subsection X185.3 Control activities
(e) Subsection X185.4 Information and communication
(f) Subsection X185.5Monitoring activities and correcting deficiencies
Section 3. Internal Audit Function
X186.1 Qualifications of CAE
X186.2 Duties and responsibilities of the CAE
X186.3 Professional competence and ethics of the IA function
X186.4 Independence and objectivity of the IA function
X186.5 Internal audit charter
X186.6 Scope
Section 4. Trust
Section 5. Non-bank FIs

BSP Circular 871

Section 1. Internal Control Framework

(a) Section X185. Internal control framework

(b) Subsection X185.1 Management oversight and control culture

(c) Subsection X185.2 Risk recognition and assessment

(d) Subsection X185.3 Control activities

(e) Subsection X185.4 Information and communication

(f) Subsection X185.5Monitoring activities and correcting deficiencies

BSP Circular 871

Section 1. Internal Control Framework

(a) Section X185. Internal control framework

(b) Subsection X185.1 Management oversight and control culture

(c) Subsection X185.2 Risk recognition and assessment

(d) Subsection X185.3 Control activities

(e) Subsection X185.4 Information and communication

(f) Subsection X185.5Monitoring activities and correcting deficiencies

BSP Circular 871

Section 1. Internal Control Framework

(a) Section X185. Internal control framework

Internal control is a process designed and effected by the board of directors, senior management, and all levels of personnel to provide reasonable assurance on the achievement of objectives through efficient and effective operations; reliable, complete and timely financial and management information; and compliance with applicable laws, regulations, supervisory requirements, and the organization's policies and procedures.

Banks shall have in place adequate and effective internal control framework for the conduct of their business taking into account their size, risk profile and complexity of operations. The internal control framework shall embody management oversight and control culture; risk recognition and assessment; control activities; information and communication; and monitoring activities and correcting deficiencies.

BSP Circular 871

Section 1. Internal Control Framework

(a) Section X185. Internal control framework

(b) Subsection X185.1 Management oversight and control culture

(c) Subsection X185.2 Risk recognition and assessment

(d) Subsection X185.3 Control activities

(e) Subsection X185.4 Information and communication

(f) Subsection X185.5 Monitoring activities and correcting deficiencies

BSP Circular 871

Section 1. Internal Control Framework

(b) Subsection X185.1 Management oversight and control culture

(1) The **board of directors**
(2) The **audit committee**
(3) **Senior Management**
(4) **All personnel**

BSP Circular 871

Section 1. Internal Control Framework

(a) Section X185. Internal control framework

(b) Subsection X185.1 Management oversight and control culture

(c) Subsection X185.2 Risk recognition and assessment

(d) Subsection X185.3 Control activities

(e) Subsection X185.4 Information and communication

(f) Subsection X185.5Monitoring activities and correcting deficiencies

BSP Circular 871

Section 1. Internal Control Framework

(c) Subsection X185.2 Risk recognition and assessment

An effective internal control system shall identify, evaluate and continually assess all material risks that could affect the achievement of the bank's performance, information and compliance objectives. The potential for fraud shall be considered in assessing the risks to the achievement of said objectives. Further, the risk assessment shall cover all risks facing the bank, which include, among others, credit; country and transfer; market; interest rate; liquidity; operational; compliance; legal; and reputational risks.

Effective risk management identifies and considers both internal (e.g., complexity of the organization's structure, nature of the bank's activities and personnel profile) and external (e.g., economic conditions, technological devt. and changes in the industry) factors that could affect the internal control framework.

BSP Circular 871

Section 1. Internal Control Framework

(a) Section X185. Internal control framework

(b) Subsection X185.1 Management oversight and control culture

(c) Subsection X185.2 Risk recognition and assessment

(d) Subsection X185.3 Control activities

(e) Subsection X185.4 Information and communication

(f) Subsection X185.5Monitoring activities and correcting deficiencies

BSP Circular 871

Section 1. Internal Control Framework

(d) Subsection X185.3 Control activities

(1) Clear arrangements for delegating authority.
(2) Adequate accounting policies, records and processes.
(3) Robust physical and environmental controls to tangible assets and access to information assets.
(4) Segregation of conflicting functions.

BSP Circular 871

Section 1. Internal Control Framework

(a) Section X185. Internal control framework

(b) Subsection X185.1 Management oversight and control culture

(c) Subsection X185.2 Risk recognition and assessment

(d) Subsection X185.3 Control activities

(e) Subsection X185.4 Information and communication

(f) Subsection X185.5Monitoring activities and correcting deficiencies

BSP Circular 871

Section 1. Internal Control Framework

(e) Subsection X185.4 Information and communication

An effective internal control system requires that there are adequate and comprehensive internal financial, operational and compliance data, as well as external information about events and conditions that are relevant to decision making. Information shall be reliable, timely, accessible, and provided in a consistent format. Banks shall have in place a reliable management information system that covers significant activities of the bank and has the capability to generate relevant and quality information to support the functioning of internal control.

Banks shall also establish effective channels of communication to ensure that all personnel fully understand and adhere to policies and procedures and control measures relevant to their duties and responsibilities and that relevant information is reaching the appropriate personnel.

BSP Circular 871

Section 1. Internal Control Framework

(a) Section X185. Internal control framework

(b) Subsection X185.1 Management oversight and control culture

(c) Subsection X185.2 Risk recognition and assessment

(d) Subsection X185.3 Control activities

(e) Subsection X185.4 Information and communication

(f) Subsection X185.5Monitoring activities and correcting deficiencies

BSP Circular 871

Section 1. Internal Control Framework

(f) Subsection X185.5Monitoring activities and correcting deficiencies

The overall effectiveness of the internal controls shall be monitored on an ongoing basis. Monitoring functions and activities shall be adequately defined by management, integrated in the operating environment and should produce regular reports for review. In this regard, all levels of review shall be adequately documented and results thereof reported on a timely basis to the appropriate level of management.

Evaluations of the effectiveness of the internal control system and the corresponding monitoring activities may be done by personnel from the same operational area in the form of self-assessment or from other areas such as internal audit; *Provided*, That, self-assessment done by business units shall be subject to independent validation.

BSP Circular 871

Section X186. Internal Audit Function

X186.1 Qualifications of CAE

X186.2 Duties and responsibilities of the CAE

X186.3 Professional competence and ethics of the IA function

X186.4 Independence and objectivity of the IA function

X186.5 Internal audit charter

X186.6 Scope

BSP Circular 871

Section X186. Internal Audit Function

X186.1 Qualifications of CAE

X186.2 Duties and responsibilities of the CAE

X186.3 Professional competence and ethics of the IA function

X186.4 Independence and objectivity of the IA function

X186.5 Internal audit charter

X186.6 Scope

Sec.X186.1 Qualifications of the Head of the IA Function

The head of the internal audit function must have an unassailable integrity, relevant education/experience/training, and has an understanding of the risk exposures of the bank, as well as competence to audit all areas of its operations. He must also possess the following qualifications:

(1) xxx

(2) The head of the internal audit function of a complex thrift bank (TB), rural bank (RB) and cooperative bank (coop bank); quasi-bank (QB) and; trust entity must be a graduate of any accounting, business, finance or economics course with technical proficiency on the conduct of internal audit and must have at least five (5) years experience in the regular audit (internal or external) of a TB, national coop bank, QB or trust entity or, at least three (3) years experience in the regular audit (internal or external) of a UB or KB.

(3)The head of the internal audit function of a simple or non-complex TB, RB and coop bank; and non-stock savings and loans association (NSSLA) must be a graduate of any accounting, business, finance or economics course with technical proficiency on the conduct of internal audit and must have at least two (2) years experience in the regular audit (internal or external) of a UB, KB, TB, RB, Coop bank, QB or NSSLA.

BSP Circular 871

Section X186. Internal Audit Function

X186.1 Qualifications of CAE

X186.2 Duties and responsibilities of the CAE

X186.3 Professional competence and ethics of the IA function

X186.4 Independence and objectivity of the IA function

X186.5 Internal audit charter

X186.6 Scope

Sec.X186.2 Duties and responsibilities of the CAE

(1) To demonstrate appropriate leadership and have the necessary skills to fulfill his responsibilities for maintaining the unit's independence and objectivity;

(2) To be accountable to the board of directors or audit committee on all matters related to the performance of its mandate as provided in the internal audit charter. The head of the internal audit function shall submit a report to the audit committee or board of directors on the status of accomplishments of the internal audit unit, including findings noted during the conduct of the internal audit as well as status of compliance of concerned departments / units.

(3) To ensure that the internal audit function complies with sound internal auditing standards such as the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing* and other supplemental standards issued by regulatory authorities / government agencies, as well as with relevant code of ethics;

(4) To develop an audit plan based on robust risk assessment, including inputs from the board of directors, audit committee and senior management and ensure that such plan is comprehensive and adequately covers regulatory matters. The head of the internal audit function shall also ensure that the audit plan, including revisions thereto, shall be approved by the audit committee;

(5) To ensure that the internal audit function has adequate human resources with sufficient qualifications and skills necessary to accomplish its mandate. In this regard, the head of the internal audit function shall periodically assess and monitor the skill-set of the internal audit function and ensure that there is an adequate development program for the internal audit staff that shall enable them to meet the growing technical complexity of banking operations.

BSP Circular 871

Section X186. Internal Audit Function

X186.1 Qualifications of CAE

X186.2 Duties and responsibilities of the CAE

X186.3 Professional competence and ethics of the IA function

X186.4 Independence and objectivity of the IA function

X186.5 Internal audit charter

X186.6 Scope

Sec.X186.3 Professional competence and ethics of the internal audit function

The internal audit function shall be comprised of professional and competent individuals who collectively have the knowledge and experience necessary in the conduct of an effective internal audit on all areas of bank's operations. The skill set of the internal audit staff shall be complemented with appropriate audit methodologies and tools as well as sufficient knowledge of auditing techniques in the conduct of audit activities .

All internal audit personnel shall act with integrity in carrying out their duties and responsibilities. They should respect the confidentiality of information acquired in the course of the performance of their duties and should not use it for personal gain or malicious actions. Moreover, internal audit personnel shall avoid conflicts of interest. Internally-recruited internal auditors shall not engage in auditing activities for which they have had previous responsibility before a one-year "cooling off" period has elapsed. The internal audit personnel shall adhere at all times to the bank Code of Ethics as well as to an established code of ethics for internal auditors such as that of the Institute of Internal Auditors.

BSP Circular 871

Section X186. Internal Audit Function

X186.1 Qualifications of CAE

X186.2 Duties and responsibilities of the CAE

X186.3 Professional competence and ethics of the IA function

X186.4 Independence and objectivity of the IA function

X186.5 Internal audit charter

X186.6 Scope

Sec.X186.4 Independence and objectivity of the internal audit function

The internal audit function must be independent of the activities audited and from day-to-day internal control process. It must be free to report audit results, findings, opinions, appraisals and other information through clear reporting line to the board of directors or audit committee. It shall have authority to directly access and communicate with any officer or employee, to examine any activity or entity of the bank, as well as to access any records, files or data whenever relevant to the exercise of its assignment.

If independent or objectivity of internal audit function is impaired, in fact or appearance, the details of the impairment must be disclosed to the audit committee. Impairment to organizational independence and individual objectivity may include, but is not limited to, personal conflict of interest, scope limitations, restrictions on access to records, personnel, and properties, and resource limitations, such as funding.

The internal audit function shall inform senior management of the results of its audits and assessment. Senior management may consult the internal auditor on matters related to risks and internal controls without tainting the latter's independence. *Provided*, That; the internal auditor shall not be involved in the development or implementation of policies and procedures, preparation of reports or execution of activities that fall within the scope of his review.

Staff of the internal audit function shall be periodically rotated, whenever practicable, and without jeopardizing competence and expertise to avoid unwarranted effects of continuously performing similar tasks or routine jobs that may affect the internal auditor's judgment and objectivity.

BSP Circular 871

Section X186. Internal Audit Function

X186.1 Qualifications of CAE

X186.2 Duties and responsibilities of the CAE

X186.3 Professional competence and ethics of the IA function

X186.4 Independence and objectivity of the IA function

X186.5 Internal audit charter

X186.6 Scope

Sec.X186.5 Internal audit charter

Banks shall have an internal audit charter approved by the board of directors. The internal audit charter shall be periodically reviewed by the head of the internal audit function and any changes thereto shall be approved by the board of directors.

The internal audit charter shall establish, among others, the following:

(1) Purpose, stature and authority, and responsibilities of the internal audit function as well as its relation with other control functions in the bank. The charter shall recognize the authority of the internal audit function, to initiate direct communication with any bank personnel; to examine any activity or entity; and to access any records, files, data and physical properties of the bank, in performing its duties and responsibilities.

(2) Standards of independence, objectivity, professional competence and due professional care, and professional ethics;

(3) Guidelines or criteria for outsourcing internal audit activities to external experts;

(4) Guidelines for consulting or advisory services that may be provided by the internal audit function;

(5) Responsibilities and accountabilities of the head of the internal audit function;

(6) Requirements to comply with sound internal auditing standards such as the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing* and other supplemental standards issued by regulatory authorities / government agencies, as well as with relevant code of ethics; and

(7) Guidelines for coordination with the external auditor and supervisory authority.

BSP Circular 871

Section X186. Internal Audit Function

X186.1 Qualifications of CAE

X186.2 Duties and responsibilities of the CAE

X186.3 Professional competence and ethics of the IA function

X186.4 Independence and objectivity of the IA function

X186.5 Internal audit charter

X186.6 Scope

Sec.X186.6 Scope

All processes, systems, units and activities, including outsourced services, shall fall within the overall scope of the internal audit function. The scope of internal audit shall cover, among others, the following:

(1) Evaluation of the adequacy, efficiency and effectiveness of internal control, risk management and governance systems in the context of current and potential future risks;
(2) Review of the reliability, effectiveness and integrity of management and financial information system, including the electronic information system and electronic banking services;
(3) Review of the systems and procedures of safeguarding the bank's physical and information assets;
(4) Review of compliance of trading activities with relevant laws, rules and regulations;
(5) Review of the compliance system and the implementation of established policies and procedures; and
(6) Review of areas of interest to regulators such as , among others monitoring of compliance with relevant laws, rules and regulations, including but not limited to the assessment of the adequacy of capital provisions; liquidity level; regulatory and internal reporting.