IT RISK MANAGEMENT STANDARDS AND GUIDELINES
Area: IT Audit
(Appendix to Sec. 148 on Purpose and Scope, and on IT Risk Management Systems)

1. INTRODUCTION

1.1. BSFIs must plan, manage and monitor rapidly changing technologies to enable them to deliver and support new products, services, and delivery channels. The rate of these changes and the increasing reliance on IT make the inclusion of IT audit coverage essential to an effective overall audit program. The audit program should address IT risk exposures throughout the organization, including the areas of IT management and strategic planning, IT operations, client/server architecture, local and wide-area networks, telecommunications, physical and information security, electronic products and services, systems development and acquisition, and business continuity planning. IT audit should also focus on how management determines the risk exposure from its operations and controls or mitigates identified risks.

1.2. A well-planned, properly structured audit program[1] is essential to evaluate risk management practices, internal control systems and compliance with policies concerning IT-related risks at BSFIs of every size and complexity. Effective audit programs are risk-focused, promote sound IT controls, ensure the timely resolution of audit deficiencies and inform the Board of Directors of the effectiveness of risk management practices. An effective IT audit function may also allow regulators to place substantial reliance on and reduce the time spent reviewing areas of the BSFIs during examinations. Ideally, the audit program should consist of a full-time, continuous program of internal audit which may be further supported by a well-planned external audit program.

2. ROLES AND RESPONSIBILITIES

2.1. Board of Directors (Board) and Senior Management. The BSFI's Board or its Audit Committee has the overall responsibility for establishing and maintaining an independent, competent and effective IT audit function commensurate with the complexity of its IT risk profile. In order to properly oversee the IT audit function, the Board or its Audit Committee should:

a. Assign responsibility for IT audit function to an internal audit department or individual with sufficient audit expertise, knowledge base and skill level;
b. Ensure that IT audit maintains its professional and organizational independence[2]; and
c. Approve and review an audit program that would guide IT audit engagements.

Senior management is responsible for supporting IT audit by providing sufficient resources,

establishing programs defining and requiring compliance with IT planning practices, operating policies and internal controls. Likewise, senior management should not, in any manner, diminish or interfere with the candor of the audit findings and recommendations.

2.2. Audit Management and Audit Staff. The internal audit manager is responsible for implementing the Board-approved audit directives. The manager oversees the audit function and provides leadership and direction in communicating and monitoring audit policies, practices, programs, and processes. He should establish clear lines of authority and reporting responsibility for all levels of audit personnel and activities.

The internal audit manager should also ensure that members of the audit staff possess the necessary independence, experience, education, training, and skills to properly conduct assigned activities. This can be undertaken by providing auditors with an effective program of continuing education and development. As the information systems of a BSFI become more sophisticated or as more complex technologies evolve, the auditor may need additional training.

The primary role of the internal IT audit staff, on the other hand, is to assess independently and objectively the controls, reliability, and integrity of the BSFI's IT environment. Internal auditors should evaluate IT plans, strategies, policies, and procedures to ensure adequate management oversight. They should assess the day-to-day IT controls to ensure that transactions are recorded and processed in compliance with acceptable accounting methods and standards and are in compliance with policies set forth by the Board and senior management. Auditors also perform operational audits, including system development audits, to ensure that internal controls are in place, policies and procedures are effective, and employees operate in compliance with approved policies. Auditors should identify weaknesses, provide meaningful recommendations and review management's plans for addressing those weaknesses, monitor their resolution, and report to the Board material weaknesses, as necessary.

2.3. Operating Management. Operating management should formally and effectively respond to IT audit or examination findings and recommendations. The audit procedures should clearly identify the methods for following up on noted audit or control exceptions or weaknesses. Operating management is responsible for correcting the root causes of the audit or control exceptions, not just treating the exceptions themselves. Response times for correcting noted deficiencies should be reasonable and may vary depending on the complexity of the corrective action and the risk of inaction.

3. INDEPENDENCE OF THE IT AUDIT FUNCTION

3.1. The ability of the internal audit function to achieve desired objectives depends largely on the independence of audit personnel. Hence, the placement of the internal audit function in relation to the BSFI's management structure should be carefully assessed. The degree of auditors' independence, objectivity and impartiality entails the following key elements:

a. Direct reporting of audit results to the Board or its Audit Committee;

b. Full authority vested by the Board to the IT Audit Department/IT auditor to access all records and staff necessary to conduct the audit and require management to address significant findings in a timely manner. Said authority must be clearly specified in an Internal Audit Charter or Audit Program duly approved by the Board or Audit Committee;

c. Non-involvement of IT audit personnel in management/operational activities that may compromise or appear to compromise their independence; and

d. The Board or Audit Committee should decide on audit personnel performance evaluation and compensation matters.

4. INTERNAL IT AUDIT PROGRAM

4.1. A formal audit program or manual consisting of policies and procedures governing the IT audit function should be adopted commensurate with the BSFI's size, complexity, scope of activities and risk profile. The audit program should, at a minimum, encompass the following components:

a. A mission statement or audit charter[3] outlining the purpose, objectives, organization, authorities, and responsibilities of the internal auditor, audit staff, audit management, and the audit committee;

b. A risk assessment process to describe and analyze the risks inherent in a given line of business and drive the scope and frequency of audits. Auditors should update the risk assessment at least annually, or more frequently if necessary, to reflect changes to internal control or work processes;

c. An annual audit plan detailing IT audit's budgeting and planning processes to include audit goals, schedules, staffing needs and reporting;

d. An audit cycle that identifies the frequency of audits which should be based on a sound risk assessment process;

e. Well-planned and properly structured audit work programs[4] that set out the required scope and resources, including the selection of audit procedures, extent of testing and the basis for conclusions for each audit area;

f. Audit report preparation standards that require the use of an approved audit rating system;

g. Requirements for audit work paper documentation to ensure clear support for all audit findings and work performed, including work paper retention policies;

h. Follow-up processes that require internal auditors to determine the disposition of management actions to correct significant deficiencies;

i. Policies on outsourcing of some or all of IT audit function, including technical/ highly specialized reviews, to external third parties; and

j. Professional development programs for audit staff/personnel to maintain the necessary technical expertise.

Additionally, the BSFI should consider conducting its internal audit activities in accordance with professional standards, such as the Standards for the Professional Practice of Internal Auditing issued by the Institute of Internal Auditors (IIA), and those issued by the Standards Board of the Information Systems Audit and Control Association (ISACA), whenever possible.

5. IT AUDIT PHASES

5.1. Audit Planning. The BSFI should develop an overall audit plan[5] for all the audit assignments/engagements covering at least twelve (12) months to ensure adequate coverage of IT risks. The plan should be defined by combining the results of the risk assessments and the resources required to yield the timing and frequency of planned internal audits. The audit plan must be realistic and should cover a time budget for other assignments and activities such as specific examination, consulting/advisory services, training and provision for audit personnel leave of absences.

The audit plan must be formally approved and regularly reviewed by the Board or Audit Committee. The internal auditors should report the status of the planned versus actual audits and any revisions to the annual audit plan on a periodic basis.

For each audit assignment, an audit work program detailing the objectives, scope, nature and extent of audit procedures and outline of audit work should be prepared. This is to ensure that

appropriate attention is devoted to important areas of the audit, potential problems are identified and resolved on a timely basis, and the audit engagement is properly organized and managed to be performed in an effective and efficient manner.

5.2. Risk Assessment. The use of an appropriate risk assessment technique or approach is critical in developing the overall IT audit plan and in planning specific audits. An effective risk assessment methodology should be defined to provide the Board or its Audit Committee with objective information in determining audit priorities for the effective allocation of IT audit resources. The risk assessment for IT audit planning should:

a. Identify the BSFI's data, application[6] and operating systems[7], technology, facilities, and personnel;

b. Identify the business activities and processes within each of those categories;

c. Include profiles of significant business units, departments, and product lines, or systems, and their associated business risks and control features, resulting in a document describing the structure of risk and controls throughout the BSFI; and

d. Use a measurement or scoring system that ranks and evaluates business and control risks for significant business units, departments, and products.

The results of the risk assessments, in support of the audit plan, must be presented to the Board or Audit Committee for review and approval. A process must be in place to ensure regular monitoring of the results of the risk assessment and updating it at least annually for all significant business units, departments, and products or systems.

A risk scoring model or system may be adopted to provide a sound basis for the risk assessment. Among the major risk factors that may be used in scoring systems include the following: a) Adequacy of internal controls; b) Nature of transactions and operating environment; c) Age of the system or application; d) Physical and logical security of information, equipment, and premises; e) Adequacy of operating management oversight and monitoring; f) Previous regulatory examination and audit results and management's responsiveness in addressing issues; g) Human resources, including the experience of management and staff, turnover, technical competence, management's succession plan, and the degree of delegation; and h) Senior management oversight.

Written guidelines on the use of risk assessment tools and risk factors should be approved and reviewed by the Board or its Audit Committee. IT auditors should use the guidelines to grade or

assess major risk areas and to define the range of scores or assessments (e.g. groupings such as high, medium or low risk or numeric risk ratings). At a minimum, the written assessment guidelines should specify the following elements: a) Maximum length for audit cycles based on the risk scores; b) Timing of risk assessments for each department or activity; c) Documentation requirements to support scoring decisions; and d) Guidelines for overriding risk assessments in special cases and the circumstances under which they can be overridden.

5.3. Performance of Audit Work.

Depending on the complexity of IT risk profile, IT auditors may perform all or a combination of any of the following IT audit procedures:

a. IT General Controls Review – This entails the review of the adequacy of general controls[8] in place to ensure proper management and monitoring of IT risks/environment and the effective functioning of the BSFI's IT systems and infrastructure. The following areas should be covered, among others: a) IT management and strategic planning; b) IT operations; c) Client/server architecture; d) Local and wide-area networks; e) Telecommunications; and f) Physical and information security.

IT general controls review may be carried out through the audit of each IT unit or department in the institution (e.g., IT Operations, Network and Communications, etc.).

b. Application Systems Review – The purpose of this review is to identify, document, test and evaluate the application controls[9] that are implemented to ensure the confidentiality, integrity and accuracy of the system processing and the related data. The application-level risks to the system and data addressed by this review are the following, among others: a) System availability risks relating to the lack of system operational capability; b) System security risks relating to unauthorized access to systems and/or data; c) System integrity risks relating to incomplete, inaccurate, untimely or unauthorized processing of data; d) System maintainability risks relating to inability to update the system when required in a manner that continues to provide for system availability, security and integrity; and e) Data risks relating to its completeness, integrity, confidentiality, privacy and accuracy.

c. Technical Reviews – BSFIs with complex IT risk profile such as those providing electronic products and services and web-enabled facilities, also require IT auditors to perform highly technical/specialized reviews such as the conduct of periodic internal vulnerability assessment and penetration testing, computer forensics and review of emerging technologies, e.g., cloud computing, virtualization, mobile computing.

IT auditors frequently use computer- assisted audit techniques (CAATs) to improve audit

coverage by reducing the cost of testing and sampling procedures that otherwise would be performed manually. CAATs include many types of tools and techniques, such as generalized audit software, utility software, test data, application software tracing and mapping, and audit expert systems. These tools and techniques can also be used effectively to check data integrity by testing the logical processing of data "through" the system, rather than by relying only on validations of input and output controls.

Audit software programs should remain under the strict control of the audit department. For this reason, all documentation, test material, source listings, source and object program modules, and all changes to such programs, should be strictly controlled. Computer programs intended for audit use should be carefully documented to define their purpose and to ensure their continued usefulness and reliability.

All audit procedures forming part of the assignment should be documented in working papers. These must reflect the examinations that have been made and emphasize the evaluations formulated in the report. The working papers must be drawn up according to a well-determined method. Such method must provide sufficient information to verify whether the assignment was duly performed and to enable others to check the manner in which it was performed.

5.4. Reporting. A written audit report of each assignment is to be issued to the auditee and Audit Committee within a reasonable timeline. The audit report should state the scope, objectives, period of coverage and the nature, timing and extent of the audit work performed. It should state the findings, conclusions and recommendations and any reservations, qualifications or limitations in scope that the IT auditor has with respect to the audit. The IT audit should discuss the draft report contents with management in the subject area prior to finalization and release of the final report. This should be signed, dated and distributed according to the terms of the audit charter/audit program or engagement letter.

5.5. Post-closing/Monitoring Activities. Senior management should ensure that the internal audit department's concerns are appropriately addressed. Therefore, they should approve a procedure established by the internal audit department to ensure the consideration and, if appropriate, timely implementation of audit recommendations.

The IT audit department should monitor the implementation of management's corrective actions for proper disposition of its findings/recommendation. The status of the recommendations is communicated at least on a quarterly basis to the Board or Audit Committee.

6. OTHER IT AUDIT ACTIVITIES/ PARTICIPATION

6.1. Development, Acquisition, Conversions and Testing. The BSFI's Board-approved audit policy should include guidelines detailing what involvement internal audit will have in the development, acquisition, conversion, and testing of major applications. This includes describing the monitoring, reporting, and escalation processes (when internal controls are found to be insufficient or when testing is found to be inadequate). For acquisitions with significant IT impacts, participation of IT audit may be necessary early in the due diligence stage.

It is necessary that audit's participation in the development process be independent and objective. Auditors can determine and should recommend appropriate controls to project management. However, such recommendations do not necessarily "pre- approve" the controls, but instead guide the developers in considering appropriate control standards and structures throughout their project.

6.2. Review of Technology Service Providers (TSP). The BSFI should effectively manage its relationships with key TSPs through review and assessment of adequacy of IT controls employed by such TSPs. When circumstances warrant, the BSFI's internal audit function may be utilized to directly audit TSP's operations and controls. In some instances, the services of external auditors may be employed. A BSFI using external audit to complement its own coverage should ensure that the independent auditor is qualified to perform the review, that the scope satisfies its own audit objectives and that any significant reported deficiencies are corrected.

7. OUTSOURCING OF IT AUDIT FUNCTIONS

7.1. The Board and senior management of a BSFI that outsources its internal IT audit function should ensure that the structure, scope and management of the outsourcing arrangement provides for an adequate evaluation of the system of internal controls. Management should ensure that there are no conflicts of interest and that the use of these services does not compromise independence.

7.2. When negotiating the outsourcing arrangement with a service provider, the BSFI should carefully consider its current and anticipated business risks in setting each party's internal audit responsibilities. To clearly define the BSFI's duties and those of the audit provider, it should have a written contract, often referred to as an engagement letter[10].

8. COMPLIANCE WITH EXISTING BANGKO SENTRAL RULES AND REGULATIONS

8.1. The provisions of the IT audit guidelines prescribe in detail the essentials and elements of an effective IT audit which complement and are consistent with Sec. 162 Independence of the Internal Auditor. Likewise, the IT audit- related tasks of the Audit Committee are in addition to the tasks prescribed under Sec. 133 Powers/responsibilities and duties of directors, Item "*c(7)(d)(i)*".

(Circular No. 969 dated 22 August 2017, and 958 dated 25 April 2017)

Footnotes

1. Audit program encompasses audit policies, procedures, and strategies that govern the audit function, including IT audit.
2. Independence means self-governance, freedom from conflict of interest and undue influence. The IT auditor should be free to make his or her own decisions, not influenced by the organization being audited, or by its managers and employees.
3. Audit charter is a document approved by the Board of Directors that defines the IT audit function's responsibility, authority and accountability.
4. Work program is a series of specific, detailed steps to achieve an audit objective.
5. Audit plan is a description and schedule of audits to be performed in a certain period of time (ordinarily a year). It includes the areas to be audited, the type of work planned, the high-level objectives and scope of the work and includes other items such as budget, resource allocation, schedule dates, and type of report issued.
6. Application system is an integrated set of computer programs designed to serve a well-defined function and having specific input, processing, and output activities (e.g., CASA, general ledger, loans and treasury systems).
7. Operating system is the program that manages all the basic functions and programs in a computer.
8. General controls are controls, other than application controls, that relate to the environment within which application systems are developed, maintained, and operated, and that are therefore applicable to all the applications at an institution. Like application controls, general controls may be either manual or automated. Examples of general controls include the development and implementation of an IT strategy and an IT security policy, the organization of IT staff to separate conflicting duties and planning for disaster prevention and recovery.
9. Application controls are controls related to transactions and data within application systems. Application controls ensure the completeness and accuracy of the records and the validity of the entries made resulting from both programmed processing and manual data entry. Examples of application controls include data input validation, agreement of batch totals and encryption of data transmitted.
10. In general, the contract between the institution and the audit provider may or may not be the same as the engagement letter.