IT RISK MANAGEMENT STANDARDS AND GUIDELINES
Area: Project Management/Development, Acquisition and Change Management
(Appendix to Sec. 148 on Purpose and Scope, and IT Risk Management Systems)

1. INTRODUCTION

1.1. Because technology is constantly evolving, Management of BSFIs should periodically assess their uses of IT as part of overall business planning. Such an enterprise-wide and ongoing approach should be formalized in the IT strategic plan to help ensure that all major IT projects are consistent with its overall strategic goals.

1.2. As part of their strategic goals, BSFIs may need to constantly introduce new or enhanced products and services, improve systems and processes and implement updates and innovations in IT to secure and manage voluminous information and maintain their competitive position. This necessity may oftentimes result to initiating IT projects[1]; which may be in the form of internal or external development of software applications or systems, acquisition and/or implementation of new or enhanced hardware, software, infrastructure or services with or without the help of third party providers.

1.3. IT projects, when managed improperly, often result in late deliveries, cost overruns, or poor quality applications. Inferior applications can result in underused, unsecure, or unreliable systems. Retrofitting functional, security, or automated-control[2] features into applications is expensive, time consuming, and often results in less effective features. Therefore, BSFIs should carefully manage IT-related projects to ensure they meet organizational needs on time and within budget.

2. ROLES AND RESPONSIBILITIES

2.1. The size and complexity of a project dictates the required number and qualifications of project personnel. Duties may overlap in smaller organizations or lower-risk projects; however, all projects should include appropriate segregation of duties or compensating controls.

2.2. **Board of Directors (Board) and Senior Management.** The BSFI's Board and senior management should review, approve, and monitor IT projects that may have significant impact on its operations, earnings or capital. They are responsible to ensure that IT projects support business objectives and adequate resources are available to complete these projects. Consequently, they should establish adequate policies and strategies to achieve these and ensure that risks related to IT projects are managed appropriately.

Senior management is expected to have more knowledge and involvement in the day-to-day operations of these IT projects to critically evaluate the design and oversee the related operation and activities. They should ensure that IT projects are coordinated and undertaken in adherence to appropriate policies, standards, and risk management controls. They should periodically inform the Board and/or IT Steering Committee of the IT initiatives and the related risks that these may pose to the BSFI. They should also review, approve, document and report deviations from established policies and standards.

2.3. **Quality Assurance.** An independent party (e.g., the quality assurance function, the TRM function or the technology audit team), who is not involved in the project development, should conduct a quality assurance review of major IT-related projects, with the assistance of the legal and compliance functions, if necessary. This review is to ensure compliance with the project life cycle[3] methodology, other internal policies, control requirements, regulations and applicable laws.

3. PROJECT MANAGEMENT STANDARDS AND METHODOLOGY

3.1. **Project Management.** The BSFI should establish a general framework for management of major technology-related projects. This framework should, among other things, specify the project management methodology to be adopted and applied to these projects. The methodology should cover, at a minimum, allocation of responsibilities, activity breakdown, budgeting of time and resources, milestones, check points, key dependencies, quality assurance, risk assessment and approvals.

A BSFI that needs to coordinate multiple IT projects should establish standards for coordinating and managing the projects from an enterprise-wide perspective. The standards should, at a minimum, include guidelines for project prioritization, resource coordination and progress reporting.

3.2. **Project Methodology.** The BSFI should adopt and implement a full project life cycle methodology governing the process of developing, implementing and maintaining major computer systems. In general, this should involve phases of project initiation, feasibility study, requirement definition, system design, program development, system and acceptance testing, training, implementation, operation and maintenance.

The project life cycle methodology should define clearly the roles and responsibilities for the project team and the deliverables[4] from each phase. It also needs to contain a process to ensure that appropriate security requirements are identified when formulating business requirements, built during program development, tested and implemented.

4. PROJECT PLANNING AND INITIATION

4.1. A formal project committee, to ensure the development of well-structured applications, should be established with clear details of its terms and reference. The committee should at least consist of the following representatives:

a. Senior management, to provide strategic direction and ensure full commitment;
b. User departments, to ensure that the application design meets their requirements;
c. Internal audit department, to act as an independent party to ensure adequate controls are diligently applied at all times. However, internal audit participation should only be on an advisory capacity; and
d. IT department, to provide technical knowledge and skills.

4.2. A feasibility study should be performed to identify the expected costs and benefits of developing a system, and also to decide either to utilize internal resources or to outsource to a vendor. In case of outsourcing, the responsibility of the senior management does not diminish in ensuring that a well-designed application is developed. The senior management maintains the responsibility for ensuring that minimum controls are in place and are in accordance with the BSFI's standards.

4.3. When management proposes a new hardware, software or IT solution and/or changes to existing ones, it should ensure that functional, operational and regulatory requirements are accurately identified and clearly detailed in request for proposals (RFP[5]) or invitations-to-tender (ITT) that it distributes to vendors or third-party service providers (TSP) in the bid solicitation process. Moreover, relevant security requirements should be clearly specified before a new system is developed or acquired. A review should also be conducted to ensure an appropriate balance between security and other objectives (ease- of-use, operational simplicity, ability to upgrade, acceptable cost, etc.) is achieved.

4.4. During the development and acquisition of new systems or other major IT projects, project plans should address issues such as – a) business requirements for resumption and recovery alternatives; b) information on back-up and storage; c) hardware and software requirements at recovery locations; d) BCP and documentation maintenance; e) disaster recovery testing; and f) staffing and facilities. Likewise, during maintenance, where there are changes to the operating environment, business continuity considerations should be included in the change control process and implementation phase.

4.5. Proper planning should be employed to ensure IT projects meet their objectives. Project control systems should be employed to monitor specific target completion dates for each task of systems development against original targets. Periodic reports to senior management such as, project priorities and status, resource allocations, target deviations and budgets, should be in place to measure project effectiveness.

5. SYSTEMS DEVELOPMENT

5.1. Development projects involve the creation of applications, integrated application systems and other critical softwares. Software development projects are completed in-house, through outsourcing, or by a combined approach. To manage this type of projects, the BSFI should establish development standards that, at a minimum, address project management, system control, and quality assurance issues. Project management standards should address issues such as project management methodologies, risk management procedures, and project approval authorities.

System control standards should address items such as an application's functional, security, and automated control features. Quality assurance standards should address issues such as the validation of project assumptions, adherence to project standards, and testing of a product's performance.

5.2. Development standards should also include procedures for managing internally developed spreadsheets and database reports. BSFIs often rely on the spreadsheets and reports to make important budgeting and asset/liability decisions, but fail to implement adequate testing, documentation, and change-control procedures. Management's reliance on the spreadsheets and reports should dictate the formality of their development procedures, change controls, and backup techniques.

5.3. Programming standards should be designed to address issues such as the selection of programming languages and tools, the layout or format of scripted code, interoperability between systems, and the naming conventions of code routines and program libraries. These will enhance the BSFI's ability to decrease coding defects and increase the security, reliability, and maintainability of application programs.

6. SYSTEM ACQUISITION

6.1. Software package acquisition is an alternative to in-house systems development and should be subject to broadly similar controls as the project life cycle. A proper software selection analysis should be conducted to ensure that user and business requirements are met. In particular, the process should involve detailed evaluation of the software package and its supplier (e.g. its financial condition, reputation and technical capabilities). If financial stability is in doubt, alternatives should be developed to reduce the adverse impact from loss of a vendor’s service.

6.2. The contract agreement between the BSFI and vendor should be legally binding. The BSFI should ensure all contract agreements outline all expected service levels and are properly executed to protect its interest. It is also important to ensure that vendor technicians and third-party consultants are subjected to at least, or preferably more stringent policies and controls compared to the in-house staff. In the case where contract personnel are employed, written contracts should also be in effect.

6.3. To optimize use of acquired software and limit or minimize risks from unauthorized or obsolete software, guidelines and procedures on installation, use, maintenance and retirement should be formally defined. Installation should be controlled to minimize risks from unauthorized software (such as loss of data, reduced productivity and unnecessary consumption of network bandwidth). Licenses should also be adequately reviewed, safe kept and monitored to ensure proper usage and adherence to terms and conditions. As changes in the industry and updates to the computing environment occur, software retirement should also be defined in the guidelines to provide when and how acquired software will be removed from or upgraded in the BSFI’s existing portfolio.

7. CHANGE MANAGEMENT

7.1. Change management is the process of planning, scheduling, applying, distributing and tracking changes to application systems, system software (e.g., operating systems and utilities), hardware, network systems, and other IT facilities and equipment. The change management procedures should be formalized, enforced and adequately documented. Authorization and approval are required for all changes and the personnel responsible for program migration should be identified. For the purpose of accountability, proper sign-off should be adequately implemented where formal acknowledgement is obtained from all related parties.

7.2. An effective change management process helps to ensure the integrity and reliability of the production environment. To ensure IT-related modifications are appropriately authorized, tested, documented, implemented and disseminated, the change manage process should include the following:

a. Classification and prioritization of changes and determination of the impact of changes;

b. Roles and responsibilities of each relevant party, including IT functions and end-user departments, with adequate segregation of duties. This is to ensure that no single person can effect changes to the production environment without the review and approval of other authorized personnel;

c. Program version controls and audit trails;

d. Scheduling, tracking, monitoring and implementation of changes to minimize business disruption;

e. Process for rolling-back changes to re-instate the original programs, system configuration or data in the event of production release problems; and

f. Post implementation verification of the changes made (e.g. by checking the versions of major amendments).

7.3. Requested changes should be screened before acceptance to determine alternate methods of making the changes, the cost of changes and time requirements for programming activity. System analysts should assess the impact and validity of the proposed changes and all critical change requests should be set as priority.

7.4. The actual cause that led to the request for change should be identified and adequately documented. Formal reports on analysis for problems raised and status of change requests (including closed and outstanding) should be reported to senior management on a periodic basis.

7.5. Audit trail of all change requests should be maintained. Programmers' activities should be controlled and monitored, and all jobs assigned should also be closely monitored against target completion dates.

7.6. To enable unforeseen problems to be addressed in a timely and controlled manner, the BSFI should establish formal procedures to manage emergency changes. Emergency changes should be approved by the information owner (for application system or production data-related changes) and other relevant parties at the time of change. If the change needs to be introduced as a matter of urgency and it is impracticable to seek the approval of the information owner, endorsement should be sought from the information owner after the implementation as soon as practicable (e.g., on the following business day).

7.7. Emergency changes should be logged and backed up (including the previous and changed program versions and data) so that recovery of previous program versions and data files is possible, if necessary. Emergency changes need to be reviewed by independent personnel to ensure that the changes are proper and do not have an undesirable impact on the production environment. They should be subsequently replaced by proper fixes through the normal acceptance testing and change management procedures.

7.8. Management should ensure that vendors permitted remote access to network resources are properly authorized. System logs showing activity on the system should be reviewed to ensure that unauthorized remote access has not taken place. Management may institute time of day restrictions for remote access, to limit the duration of time a user can access the network remotely (e.g., only during business hours). Vendors utilizing dial in access should be verified through call back procedures and/or through the use of a modem that can be turned on when authorization has been granted by the system administrator.

7.9. Data patching could severely compromise the integrity of the database in production systems and should strictly be avoided. The BSFI should adequately ensure the accuracy and reliability of its database and the integrity of its data. Good project management discipline requires validation of data input, data integrity testing, user sign-off, impact analysis and escalation of decision to senior management should be adopted to ensure accuracy and validity of data before live implementation.

8. SYSTEMS TESTING

8.1. A formal acceptance process should be established to ensure that only properly tested and approved systems are promoted to the production environment. System and user acceptance testing should be carried out in an environment separate from the production environment. Production data should not be used in development or acceptance testing unless the data has been desensitized (i.e., not disclosing personal or sensitive information) and prior approval from the information owner has been obtained. Performance testing should also be performed before newly developed systems are migrated to the production environment.

8.2. Sufficient testing is important to ensure that design and overall reliability of the application systems are in accordance with original specifications. Tests should be conducted using documented test plans that should encompass all predetermined data or processing problems and business scenarios.

8.3. User acceptance testing should be performed in a separate environment. All related users are responsible to ensure that adequate test scenarios are formulated and sufficiently tested. Successful test activities should be formally confirmed and accepted by users, before the modified programs can be transferred to the production environment.

9. SYSTEMS MIGRATION

9.1 A secured library for program pending migration to the production environment should be established. The secured library or quarantine area for all amended programs should only be accessible by the personnel who performed the migration process and restricted from the application programmers. This is to mitigate the risk of programmers changing the modified programs after user acceptance testing, but prior to the program migration.

9.2. Source compare procedure should be in place to verify changes and to ensure no unauthorized changes have been made. Modified programs should be compared to the authorized change documents to determine that only approved specification changes were implemented.

9.3. Updates or a version control for all applications should be maintained. Old versions of source codes[6] should be archived as contingency measure, with a clear indication of the precise date, time and all necessary information while the latest version of the source codes and databases should be strictly protected. Version controls may also be implemented to ensure only authorized programs are migrated to quarantine and production environments.

10. SOURCE CODE CONVERSION AND MAINTENANCE

10.1. Conversion of source codes into object codes should be adequately controlled in order to mitigate the risks of unauthorized changes and to ensure accurate and complete results. The conversion process should only be performed by designated personnel. In the case where the compiler programs or other systems development tools are used, it should be placed under restricted control and the access and execution rights are strictly monitored.

In cases where core applications are developed by vendors but the source codes were not released to the BSFI, the institution's interest should be protected in the form of a written agreement. The agreement, generally known as escrow agreement, should allow the BSFI to access the source programs under conditions, such as, but not limited to, discontinued product support or financial insolvency by the vendor. A third-party entity should be appointed to retain these programs and documents in escrow. However, it is important for the BSFI to periodically determine that the source code maintained in escrow is up-to-date. If the BSFI decides not to go into a source code escrow agreement, appropriate controls or contingency plans should be established as necessary, to continue adequate operation of the business or process the acquired program is supporting in case it becomes problematic, obsolete, or ceases to function.

11. SYSTEMS DOCUMENTATION

11.1 All standards and procedures on systems development and documentation on user manuals should be formally established and properly maintained to ensure consistency of approach.

Accessibility to these documents should be strictly confined only to those who are authorized to receive such information in order for them to effectively discharge their duties.

11.2 Management should identify the type and level of documentation personnel must produce during each project phase. Project documentation of major IT projects, especially development and acquisition, should include project requests, feasibility studies, project plans, testing plans, etc. System documentation, which focuses on system analysis and design, should include system concept narratives, data flow charts, and database specifications. Application documentation should include application descriptions, programming flowcharts, and operations and user instructions. The documentation should be revised as needed throughout the project life cycle.

11.3 Documentation standards should identify primary documentation custodians and detail document authoring, approving, and formatting requirements. Personnel should document all changes to system, application, and configuration documentation according to prescribed standards. Additionally, management should control access to documentation libraries with appropriate library and version controls.

11.4 All standards and documentation should be kept secured to prevent unauthorized access. The BSFI should maintain a central storage (of either hardcopy or softcopy) of all standards and documentation onsite as well as in an offsite premise for contingency purposes. In the case where the application is developed by a vendor, management should ensure that adequate training and manuals are provided as part of the package, stated in writing and clearly understood by all parties. The BSFI should also ensure complete and updated system documentation is provided.

12. POST-IMPLEMENTATION REVIEW

12.1. A post implementation review should be conducted at the end of a project to validate the application's operational performance, after it has begun to operate. The relative success of the project should be gauged by comparing planned and actual cost, benefits and completion time. If the planned objectives do not materialize, reasons should be reviewed and documented in a post implementation evaluation report that should be presented to senior management highlighting any operational or project management deficiencies noted.

12.2. The responsibilities for conducting post-implementation review can be assigned to the BSFI's IT audit function. In larger IT organizations, formal quality assurance or change management groups may have primary responsibility for post-implementation reviews. In such cases, the IT auditor may choose not to perform a separate review but instead to participate in establishing the test criteria and evaluating results of any other independent reviews.

13. DISPOSAL

13.1. The BSFI may sometimes need to remove surplus or obsolete hardware, software, or data. Primary tasks include the transfer, archiving, or destruction of data records. Management should transfer data from production systems in a planned and controlled manner that includes appropriate backup and testing procedures. The BSFI should maintain archived repository of data in accordance with applicable record retention requirements and system documentation to facilitate reinstallation of a system into production, when necessary. Management should destroy data by overwriting old information or degaussing (demagnetizing) disks and tapes.

14. ROLE OF AUDIT, INFORMATION SECURITY AND QUALITY ASSURANCE OFFICERS

14.1 **Audit.** The BSFI's auditors assist user departments, project managers, and system designers in identifying system control requirements and testing the controls during development and after implementation. Please refer to Item 6.1 of *Appendix 73* for the detailed guidelines on audit's participation in the development, acquisition, and maintenance of major systems.

14.2 **Information Security.** The BSFI should ensure that systems are developed, acquired and maintained with appropriate security controls. To do this, management should ensure that – a) systems are developed and implemented with necessary security features enabled and based on established security control requirements; b) software is trustworthy by implementing appropriate controls in the different project phases; and c) appropriate configuration management and change control processes exist, including an effective patch management process. Management should establish security control requirements based on their risk assessment process evaluating the value of the information at risk and the potential impact of unauthorized access, damage or other threats.

14.3 **Quality Assurance.** Independent quality assurance function is a critical part of well-managed IT projects. Comprehensive quality assurance, risk management, and testing standards provide the best means to manage project risks and ensure IT projects, especially software, include expected functionality, security, and operability, as applicable.

(Circular No. 958 dated 25 April 2017, and 833 dated 28 May 2014)

Footnotes

[1] An *IT project* is a task involving the acquisition, development or maintenance of a technology product.

[2] *Automated controls* are software routines designed into programs to ensure the validity, accuracy, completeness and availability of input, processed and stored data.

3. *Project life cycle* refers to a logical sequence of activities to accomplish a project’s goals or objectives.
4. *Deliverables* are project goals and expectations. They include broadly-defined, project or phase requirements and specifically-defined tasks within project phases.
5. *RFP* is a document that a BSFI sends to a vendor inviting the vendor to submit a bid for hardware, software, services, or any combination of the three. An institution typically issues the RFP in order to assess competing bids.
6. Source codes are software program instructions written in format (language) readable by humans.