



BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR
SUPERVISION AND EXAMINATION SECTOR

MEMORANDUM NO. M-2015-018

To : **ALL BSP-SUPERVISED FINANCIAL INSTITUTIONS**

Subject : **INFORMATION TECHNOLOGY RATING SYSTEM**

The Monetary Board, in its Resolution No. 458 dated 19 March 2015, approved the issuance of the attached detailed guidelines on BSP's Information Technology Rating System (ITRS) aligned with the requirement under Subsections X177.4 and 4177Q.4/4196S.4/4193P.4/4196N.4 of the Manual of Regulations for Banks (MORB) and the Manual of Regulations for Non-Bank Financial Institutions (MORNBFi), respectively. The ITRS shall serve as a tool to enable BSP to have a comprehensive and consistent approach in the measurement of BSP-supervised financial institutions' (BSFIs) existing practices against acceptable level given their risk profile.


The attached document is composed of the following parts:

1. ITRS overview, which provides an introduction of the rating system and general application guidelines;
2. Composite ratings table; and
3. Appendix A, which contains guidance on the component ratings.

A supplemental table is included in Appendix A that maps existing provisions in the revised ITRM framework against each component. In this connection, BSFIs are expected to understand the ITRS and give their utmost cooperation in implementing the same.

The ITRS shall be effective for IT examinations starting 01 April 2015.

For information and guidance.


NESTOR A. ESPENILLA, JR.
Deputy Governor

01 April 2015

Att: A/S

THE INFORMATION TECHNOLOGY RATING SYSTEM

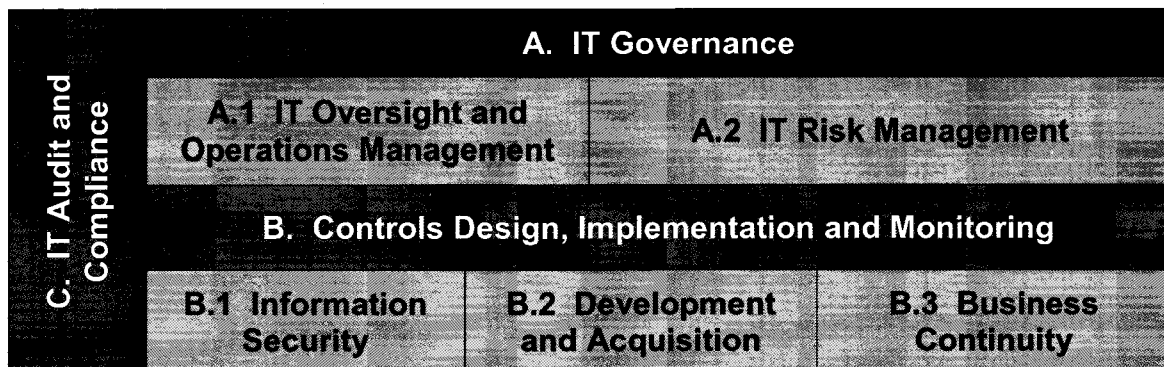
Introduction

In response to the aggressive and widespread adoption of technology in the financial services industry, the Monetary Board, in its Resolution No. 1286 dated 01 August 2013, approved the amendments to Sections X177 and 4177Q/4196S/4193P/4196N of the Manual of Regulations for Banks (MORB) and Manual of Regulations for Non-Bank Financial Institutions (MORNBFI), respectively, to strengthen existing BSP framework for IT risk management. Subject to a risk-based implementation approach, BSP-supervised financial institutions (BSFIs) are expected to comply with the relevant requirements of the above-cited amended regulations commensurate with the size, nature and complexity of their IT operations.

Consequently, as described in Subsections X177.4 and 4177Q.4/4196S.4/4193P.4/4196N.4 of the MORB and the MORNBFI, *“the BSP, in the course of its on-site examination activities, shall evaluate BSFIs’ ITRM system and measure the results based on BSP’s IT rating system (ITRS).”* The ITRS as a tool shall enable BSP to have a comprehensive and consistent approach in the measurement of BSFI’s existing practices against acceptable level given the BSFI’s risk profile.

Overview

The ITRS shall be composed of three major areas with six components as illustrated below:



- A. IT Governance
 - A.1. IT Oversight and Operations Management
 - A.2. IT Risk Management
- B. Controls Design, Implementation and Monitoring
 - B.1. Information Security
 - B.2. Development and Acquisition
 - B.3. Business Continuity
- C. IT Audit and Compliance

Composite and component ratings are assigned based on a 1 to 4 numerical scale. A rating of 4 is the highest, which indicates strong IT risk management practices and no cause

for supervisory concern. A rating of 1 is the lowest, which indicates weak practices and the highest degree of supervisory concern.

Assignment of composite and component ratings shall consider the complexity of BSFI's IT profile with due consideration of risk management policies, practices and impact on the overall safety and soundness of the institution. Composite rating is not an arithmetic average of the component ratings but a qualitative assessment of the different components and their interrelationships.

Composite Rating

The composite rating reflects the supervisor's overall conclusion on the design and effectiveness of a BSFI's IT risk management system. It is based on a collective evaluation of the different components, including their interrelationships, and encompasses oversight and management, policies, practices and over-all responsiveness to changes in the business environment. The composite ratings are defined and described as follows:

Composite Rating	Definition	Description
4	Strong	BSFIs rated composite "4" exhibit strong performance. Weaknesses noted are minor in nature and can be easily corrected during the normal course of business. BSFI's IT risk management system shows no cause for supervisory concern. Management is proactive in identifying potential weaknesses and promptly takes action. Audit and regulatory concerns were timely, appropriately and substantially addressed. Strategic plans are well defined and aligned with business strategy. Management is able to quickly adapt to changing market, business, technological and security needs of the BSFI. Risk management program, processes and practices are formally approved, enterprise-wide, comprehensive and able to adequately identify, measure, monitor and control BSFI's risk exposures. Organizational information and cyber-security practices are regularly updated with changes in the threat and technology landscape and, at the same time, the BSFI promotes information sharing with partners to improve cyber-security management. Assessment of controls, operating and financial condition of the BSFI's technology service provider is strong. Generally, all or most of its component ratings are 4 with no component rating below 3.
3	Satisfactory	BSFIs rated composite "3" exhibit satisfactory performance with low to moderate weaknesses. While internal control weaknesses may exist, there are no significant concerns. As a result, supervisory action is informal and limited. Management normally identifies weaknesses and takes appropriate corrective actions in the normal course of

Composite Rating	Definition	Description
		business. Strategic plans are defined but may require clarification, better coordination or improved communication throughout the organization. Management anticipates, but responds less quickly to changes in market, business, technological and security needs of the BSFI. Risk management processes adequately identify, measure, control and monitor risks relative to IT risk profile. Organizational information and cyber-security practices are regularly updated with changes in the threat and technology landscape. Assessment of controls, operating and financial condition of the BSFI's technology service provider is acceptable. Generally, all or most of its component ratings are 3 with no component rating below 2.
2	Less than Satisfactory	BSFIs rated composite "2" exhibit less than satisfactory performance due to a combination of weaknesses that may range from moderate to severe. If weaknesses persist, further deterioration in the condition and performance of the BSFI is likely. Increased supervision is necessary and a combination of formal and informal supervisory actions may be necessary to secure corrective action. Repeat concerns may exist, indicating that management lacks the ability or willingness to resolve concerns. Self-assessment practices are weak and are generally reactive to audit and regulatory exceptions. Strategic plans are vaguely defined and may not provide adequate direction for IT initiatives. Management experiences difficulty responding to changes in business, market, technological and security needs of the BSFI. Risk management practices are formally approved but are not implemented or linked to an enterprise-wide policy. Risk management processes and practices do not effectively identify and measure risks and may be inappropriate relative to the BSFI's risk profile. Implemented controls and monitoring activities are not linked to a formal risk assessment process. Organizational information and cyber-security practices are not responsive to changes in the threat and technology landscape. Assessment of controls, operating and financial condition of the BSFI's technology service provider is weak and/or derogatory information is noted from other clients. Generally, all or most of its component ratings are 2.
1	Deficient	BSFIs rated composite "1" indicate a deficient environment that may impair the future viability of the BSFI requiring immediate remedial action. Serious operational problems and weaknesses may exist throughout the organization. Failure of the BSFI is likely unless IT problems are remedied.

Composite Rating	Definition	Description
		Ongoing supervisory attention is necessary and formal enforcement action is warranted. Self-assessment practices are absent and management is unwilling or incapable of correcting audit and regulatory concerns. Strategic plans are poorly defined or non-existent and the Board and Senior Management have little or no direction for IT initiatives. Management is unaware of or inattentive to technological and security needs of the BSFI. Risk management practices are not formalized and risk is managed in an ad hoc and sometimes reactive manner. Risk management processes and practices are absent or inadequate in identifying, measuring, monitoring and controlling BSFI's risk exposures. Maintenance and updating of organizational information and cyber-security practices are non-existent. Assessment of controls, operating and financial condition of the BSFI's technology service provider is poor or not performed. Generally, all or most of its component ratings are 1.

Detailed guidelines for component evaluation are in Appendix A.

Enforcement Action/s

In addition to assigning a composite rating, the BSP shall come up with specific recommendations directed to the underlying causes of supervisory issues or weaknesses noted. Enforcement action/s to be imposed on the institution shall be those provided under existing regulations.

INFORMATION TECHNOLOGY RATING SYSTEM COMPONENT RATINGS

Area A - IT Governance

As defined in the MORB/MORNBF, IT Governance *"is an integral part of BSFIs' governance framework and consists of the leadership and organizational structures and processes that ensure the alignment of IT strategic plan with BSFIs' business strategy, optimization of resources management, IT value delivery, performance measurement and the effective and efficient use of IT to achieve business objectives and effective IT risk management implementation."*

To enable a more effective assessment of this area, it was further divided into two components, consistent with what it intends to achieve, as follows:

Objective	Component
Achieve business objectives	A.1 IT Oversight and Operations Management
Effective IT risk management implementation	A.2 IT Risk Management

Component A.1 - IT Oversight and Operations Management

The IT oversight and operations management component is the core of IT governance as it captures how IT is being managed throughout the organization. It reflects the capability and effectiveness of the Board of Directors and Senior Management in the discharge of their duties and responsibilities as prescribed under existing BSP guidelines.

This component also includes existing controls and processes to ensure that the Board and Senior Management remain apprised of significant IT activities to enable them to make balanced and well-informed decisions about the BSFI's IT Operations. Operations management further includes activities and other measures undertaken by the BSFI to ensure that IT is capable of supporting existing and prospective business and operational requirements.

This component includes the following factors:

1. Oversight and organization of IT functions
2. IT policies, procedures and standards
3. Staff competence and training
4. Management information systems (MIS)

In addition to what is prescribed under Subsection X177.7 and 4177Q.7/4196S.7/4193P.7/4196N.7 of the MORB and MORNBF, respectively, this component also includes relevant provisions under Appendix 75d/Q-59d IT Operations, Appendix 75e/Q-59e IT Outsourcing/Vendor Management and Appendix 75f/Q-59f

Electronic Banking, Electronic Payment, Electronic Money and Other Electronic Products and Services of the MORB/MORNBFI. An overview of related provisions is as follows:

MORB/MORNBFI Appendix	Relevant Provisions
75d/Q-59d IT Operations	Technology Inventory, Preventive Maintenance, Event/Problem Management, User Support/Help Desk, Scheduling, Service Level Agreements, Performance Monitoring, Capacity Planning
75e/Q-59e IT Outsourcing/Vendor Management	All
75f/Q-59f Electronic Banking, Electronic Payment, Electronic Money and Other Electronic Products and Services	Infrastructure and Security Monitoring, Incident Response and Management, Outsourcing Management, Cross Border E-banking Activities

Below is the rating scale for the component “IT Oversight and Operations Management”:

Component Rating	Definition	Description
4	Strong	A component rating of “4” indicates strong support structure, processes and practices for IT oversight and operations management. Organizational structure is well-defined and formally adopted allowing the Board to be regularly informed of IT performance and set appropriate direction for IT activities. MIS provides the Board and Senior Management accurate, timely and comprehensive information to enable prudent and reasonable business decisions. MIS supports monitoring of the institution’s activities as well as a means for information dissemination at various levels of the organization. Adequate internal controls, operating procedures, safeguards, and audit coverage of MIS-related activities are in place. Formally adopted IT strategic plan, policies, procedures, and standards are thorough and reflective of the complexity of the IT environment. These are communicated and enforced throughout the organization. Staff level and competency are sufficient. Adequate resources are allocated to hire and train employees to achieve a level of expertise necessary to meet business objectives. Succession and transition strategies are formally adopted, well-defined, and readily implementable. Relevant controls on IT Operations, Vendor Management and Electronic Banking fully conform to BSP’s requirements. Consistent application of said controls is also evident.
3	Satisfactory	A component rating of “3” indicates satisfactory support structure, processes and practices for IT oversight and operations management. Organizational structure is defined

Component Rating	Definition	Description
		<p>and formally adopted allowing the Board to remain informed of IT performance and set direction for major IT activities. MIS provides the Board and Senior Management accurate and timely information to support key business decisions. MIS also provides means for monitoring major activities as well as information dissemination. Internal controls, operating procedures, safeguards, and audit coverage of MIS-related activities are in place but may exhibit modest weaknesses. Formally adopted IT strategic plan, policies, procedures, and standards are adequate. However, minor weaknesses may exist in management's ability to communicate and enforce them throughout the organization. Staff level and competency generally meet business needs. Minor gaps are noted in employee hiring and training process. Succession and transition strategies are formally adopted but may not be readily implementable. Relevant controls on IT Operations, Vendor Management and Electronic Banking generally conform to BSP's requirements.</p>
2	Less than Satisfactory	<p>A component rating of "2" indicates less than satisfactory support structure, processes and practices for IT oversight and operations management. Organizational structure is informal. The Board is occasionally informed of IT performance. MIS provides the Board and Senior Management information as basis for decision making but reports may be incomplete, delayed or contain significant inaccuracies. IT strategic plan, policies and procedures exist, but may be incomplete. The plan may not be formally adopted, effectively communicated, or enforced throughout the organization. Staff level and competency are less than what is needed to meet business requirements. Significant gaps are noted in employee hiring and training process. Succession and transition strategies are informal. Relevant controls on IT Operations, Vendor Management and Electronic Banking are inadequate to conform to BSP's requirements.</p>
1	Deficient	<p>A component rating of "1" indicates deficient support structure, processes and practices for IT oversight and operations management. Organizational structure and oversight of IT is deficient or lacking. MIS is lacking or is grossly inaccurate which may mislead the Board and Senior Management when making decisions and setting direction. IT strategic plan, policies, procedures, and standards have not been formally adopted or are deficient. These are not effectively communicated and enforced throughout the</p>

Component Rating	Definition	Description
		organization. Staff level and competency do not meet business needs. Hiring and training processes are absent or deficient. Succession and transition strategies are non-existent or trivial. There are few or no controls in place for IT Operations, Vendor Management and Electronic Banking. Implementation of the required controls as prescribed in the BSP guidelines is very minimal.

Component A.2 - IT Risk Management

Risk management is a significant component of IT governance. BSFIs shall have well-defined technology risk management practices that will drive response selection and controls implementation. There shall be processes and tools to enable management to identify, understand and continually compare its risk exposure against acceptable risk levels.

This component includes the IT Risk Management function and processes for risk identification, assessment, measurement and monitoring as described in relevant subsections of the MORB and MORNBF. Appropriate guidance on the risk assessment process is also provided for IT audit, information security, IT operations and IT outsourcing/vendor management in related appendices.

Below is the rating scale for the component "IT Risk Management":

Component Rating	Definition	Description
4	Strong	IT risk management practices, processes and tools exceed what is considered necessary given the BSFI's risk profile. The Board considers IT risk in a holistic manner and requires active involvement of the designated IT risk leader in the design, and implementation of risk management activities. Comprehensive inventory of identified IT-related risks and controls supports an enterprise-wide view of the IT risk profile. Information assets are appropriately mapped to business processes and are classified according to their criticality. Risk response satisfactorily addresses key IT risks identified and are based on a comprehensive assessment in the context of the design and operational effectiveness of existing controls. Cost-benefit discussions for risk response are regularly conducted. Strategies and plans for responding to identified IT risks are continuously being updated and communicated throughout the institution. Strategic objectives take into account IT-related business threats, risk scenarios and competitive opportunities.
3	Satisfactory	IT risk management practices, processes and tools meet what is considered necessary given the BSFI's risk profile.

Component Rating	Definition	Description
		The Board understands the value of IT risk management and designates an enterprise-wide IT risk leader to handle regular risk identification, measurement, monitoring and control activities. Inventory of identified IT-related risks and controls provide an adequate understanding of the IT risk profile. Key information assets are identified and classified according to their criticality. Risk response adequately addresses key IT risks identified. Cost-benefit discussions for risk response are evident but may not be consistently performed. Strategies and plans for responding to identified IT risks are adequately documented and communicated.
2	Less than Satisfactory	IT risk management practices, processes and tools do not meet what is considered necessary given the BSFI's risk profile. The Board recognizes the need for IT risk management and issues general guidance. However, responsibility and accountability is informal or unclear. Periodic risk assessment activities have significant scope limitations. Inventory of identified IT-related risks and controls provides limited view of the IT risk profile as it may be inconsistently prepared and/or not consolidated. Key information assets are identified but are not adequately classified based on their criticality. Risk response is inadequate as it does not appropriately manage IT risk to an acceptable level. There is very little or no cost-benefit discussions for risk response. Strategies and plans for responding to IT risk have significant weaknesses and/or inadequately documented.
1	Deficient	IT risk management practices, processes and tools are deficient, in a material way, to meet what is considered necessary given the BSFI's risk profile. The Board does not recognize the need for IT risk management and existing IT risk management function is ineffective. Risk assessment activities are lacking or performed only on an ad hoc basis. Inventory of IT-related risks and information assets does not exist or is deficient and does not support the maintenance of the IT risk profile. Risk response is absent or does little to manage IT risk to an acceptable level.

Area B – Controls Design, Implementation and Monitoring

Management is required to establish and implement an adequate and effective system of internal controls to maintain the overall integrity of BSFI's environment. Internal controls, comprised of policies, practices and supporting organization structure, shall be embedded in BSFI's culture and processes to provide reasonable assurance that business

objectives will be achieved. For monitoring purposes, measurable performance goals, self-assessment tools and other indicators may be used by the BSFI.

In Circular No. 808 dated 22 August 2013, there were five areas highlighted wherein satisfactory control practices need to be designed, implemented and monitored as part of the overall IT risk mitigation strategy, namely: (a) information security, (b) project management/development and acquisition and change management, (c) IT operations, (d) IT outsourcing/vendor management and (e) electronic banking, electronic payments, electronic money and other electronic products and services. Supervisory expectations and guidelines for each area have been included as appendices in the said Circular.

However, for the IT Rating System, “Controls Design, Implementation and Monitoring” shall focus on three components: information security, development and acquisition and business continuity. Mapping of related appendices for each component is as follows:

Component	Related Appendices (MORB/MONBFI)
B.1 Information Security	<ul style="list-style-type: none"> • 75b/Q-59b Information Security • 75d/Q-59d IT Operations (i.e., Environmental Controls, Patch Management, Network Management, Disposal of Media) • 75f/Q-59f Electronic Banking, Electronic Payment, Electronic Money and Other Electronic Products and Services (i.e., Non-Repudiation, Authentication Control and Access Privileges, Confidentiality and Integrity of Information, Transactions and Records, Application Security)
B.2 Development and Acquisition	<ul style="list-style-type: none"> • 75c/Q-59c Project Management/Development, Acquisition and Change Management • 75d/Q-59d IT Operations (i.e., Change Management and Control, Conversions)
B.3 Business Continuity	<ul style="list-style-type: none"> • 75d/Q-59d IT Operations (i.e., Systems and Data Back-up, Systems Reliability, Availability and Recoverability) • 75f/Q-59f Electronic Banking, Electronic Payment, Electronic Money and Other Electronic Products and Services (i.e., Service Availability and Business Continuity)

Component B.1 – Information Security

As defined, information security refers to *“the protection of information assets from unauthorized access, use, disclosure, disruption modification or destruction in order to provide confidentiality, integrity and availability.”* To meet this objective, controls shall be designed and implemented as prescribed in the relevant appendices as summarized in Area B.

Factors to be considered in the assessment include:

1. Level of security oversight and adequacy of supporting structure
2. Cooperation and involvement in cyber-security initiatives within the industry
3. Security controls design and implementation
4. Security technologies
5. Information security awareness activities
6. Activity monitoring

Below is the rating scale for the component **“Information Security”**:

Component Rating	Definition	Description
4	Strong	Information security oversight, supporting structure, practices and controls exceed what is considered necessary given the BSFI’s risk profile. Organization is able to adapt to changes in the security landscape as continuous improvement is embedded in the process. The BSFI promotes information sharing and collaboration with partners to manage industry-wide and cyber-security risks. Existing controls and practices fully conform to BSP guidelines and are consistently implemented. Participation from all employees is evident in ensuring information security risks are proactively managed.
3	Satisfactory	Information security oversight, supporting structure, practices and controls meet what is considered necessary given the BSFI’s risk profile. Organization is regularly updated of changes in the technology and threat landscape. BSFI understands its dependencies with partners to enable collaboration on certain industry-wide and cyber-security risks. Existing controls and practices generally conform to BSP guidelines. Employees understand their roles and responsibilities and are kept abreast of developments on information security.
2	Less than Satisfactory	Information security oversight, supporting structure, practices and controls do not meet what is considered necessary given the BSFI’s risk profile. Organization is aware of the risks but an enterprise-wide approach is not established. BSFI is aware of its role in the industry but has not formalized its capabilities to interact and share information to its partners to manage certain industry-wide and cyber-security risks. Existing controls and practices are generally not compliant with BSP guidelines. Roles and responsibilities in managing security risks within the organization are defined but are not known among its employees. Employees have limited awareness of information security risks.

Component Rating	Definition	Description
1	Deficient	Information security oversight, supporting structure, practices and controls are deficient, in a material way, to meet what is considered necessary given the BSFI's risk profile. Approach to managing security risks is not formalized and may be done only in an ad hoc or reactive manner. BSFI is not capable to participate in information sharing with partners in the industry. Roles and responsibilities in managing security risks within the organization are not defined. Employees are not aware of information security risks.

Component B.2 – Development and Acquisition

BSFIs should carefully manage IT-related projects to ensure organizational needs and requirements are met on time and within budget. Thus, controls shall be put in place to appropriately manage acquisition, installation, maintenance and retirement of technologies. Management needs to exhibit ability to identify, acquire, install and maintain technology solutions. Framework shall be able to cover installation, use and maintenance up to retirement. Controls and activities to manage deployment of a change from test to production environment shall also be included in the scope. Controls and supervisory expectations are further discussed in related appendices as summarized in Area B.

Factors to be considered in the assessment include:

1. Level of oversight and adequacy of supporting structure
2. Project management standards and methodology
3. Systems migration
4. Quality assurance
5. Change management controls

Below is the rating scale for the component “Development and Acquisition”:

Component Rating	Definition	Description
4	Strong	BSFI's project management methodology, controls and related risk management practices exceed what is considered necessary given the BSFI's risk profile. Management regularly exhibits ability to identify and implement IT solutions in a controlled environment. Projects undertaken consistently meet end-user needs. Techniques and practices are effective and formalized. Project controls are evident and consistently result in timely, efficient and effective project completion. Independent quality control/quality assurance procedures for all significant IT-related activities ensure cost-effective value delivery and

Component Rating	Definition	Description
		continuous improvement through on-going monitoring. No significant weaknesses or problems exist.
3	Satisfactory	BSFI's project management methodology, controls and related risk management practices meet what is considered necessary given the BSFI's risk profile. Management exhibits ability to identify and implement IT solutions in a controlled environment. Projects undertaken meet end-user needs though minor enhancements may be necessary to meet original user expectations. Project controls, techniques and practices are generally effective but with weaknesses that may result in minor project delays or cost overruns. Independent quality control/quality assurance procedures for key IT activities are regularly conducted to support value delivery and improvement efforts. Weaknesses may exist but they are easily corrected in the normal course of business.
2	Less than Satisfactory	BSFI's project management methodology, controls and related risk management practices do not meet what is considered necessary given the BSFI's risk profile. Management is not consistently able to identify and implement IT solutions, which may result in unwarranted risk exposure. Projects undertaken generally meet end-user needs though often require changes and workarounds prior to or after implementation. Frequent project delays or cost overruns exist as a result of weak project management controls, techniques and practices. Independent quality control/quality assurance procedures are limited in scope and may not adequately support value delivery and improvement efforts. Moderate to severe weaknesses are present that may result in significant problems or losses in the future.
1	Deficient	BSFI's project management methodology, controls and related risk management practices are deficient, in a material way, to meet what is considered necessary given the BSFI's risk profile. Management is not able to identify and implement IT solutions and maintain project controls to manage risk. Projects do not meet requirements and needs of the BSFI, which result in underused, unsecured or unreliable systems. Severe project delays and cost overruns are experienced by the BSFI due to poor or absence of project management controls, techniques and practices. Independent quality control/quality assurance procedures are deficient or lacking. Significant weaknesses exist that require immediate action.

Component B.3 – Business Continuity

The increasing dependency on IT of BSFIs highlights the importance of effective support and delivery processes within the organization. Thus, this component is focused on controls and activities taken by the BSFI to ensure availability and continuity of operations. BSFIs shall be able to design and implement back-up and recovery strategies based on the periodic business impact analysis and risk assessment. Controls and supervisory expectations are further discussed in related appendices as summarized in Area B.

Factors to be considered in the assessment include:

1. Level of oversight
2. Soundness of back-up strategy against BSFI's risk profile
3. Business impact analysis/risk assessment
4. Infrastructure, including existence and effectiveness of technologies deployed
5. Test and actual results on disaster recovery

Below is the rating scale for the component “**Business Continuity**”:

Component Rating	Definition	Description
4	Strong	Business continuity strategy and practices exceed what is considered necessary given the BSFI's risk profile. Board and Senior Management proactively monitor and are actively involved in ensuring resiliency of BSFI operations. BSFI is able to exhibit capability to recover within business requirements. Tests are regularly performed covering various scenarios including component failure up to total shutdown or inaccessibility of the primary data center. Back-up and recovery strategies, recovery time objective, recovery point objective, technology recovery plans and other related documents are regularly reviewed and updated to align with changes in the business environment. Participation from all employees is evident in ensuring risks are proactively managed.
3	Satisfactory	Business continuity strategy and practices meet what is considered necessary given the BSFI's risk profile. Board and Senior Management are actively involved in ensuring resiliency of BSFI operations. BSFI is able to exhibit capability to recover within business requirements. Tests are periodically performed covering various scenarios including component failure up to total shutdown or inaccessibility of the primary data center with minor problems encountered during systems or applications recovery. Review and update of back-up and recovery strategies, recovery time objective, recovery point objective, technology recovery plans and

Component Rating	Definition	Description
		other related documents are done periodically. Employees understand their roles and responsibilities and are kept abreast of developments on business continuity.
2	Less than Satisfactory	Business continuity strategy and practices do not meet what is considered necessary given the BSFI's risk profile. Board and Senior Management are regularly updated on the status of different initiatives but are not actively involved in ensuring resiliency of BSFI operations. BSFI is not able to adequately exhibit capability to recover within business requirements due to inadequate tests performed. Periodic tests are performed but may be limited in scope or that recovery of critical systems and applications is frequently unsuccessful. Review and update of back-up and recovery strategies, recovery time objective, recovery point objective, technology recovery plans and other related documents are done as needed or not updated. Roles and responsibilities in managing business continuity risks within the organization are defined but are not known among its employees.
1	Deficient	Business continuity strategy and practices are deficient, in a material way to meet what is considered necessary given the BSFI's risk profile. Board and Senior Management are not informed of activities and not involved in ensuring resiliency of BSFI operations. Recovery and back-up strategies are not tied up with business requirements or there are none in place. Tests are not performed or typically unable to recover critical systems and applications. Back-up and recovery strategies, recovery time objective, recovery point objective, technology recovery plans and other related documents are non-existent or no longer updated. Roles and responsibilities in ensuring availability and continuity of operations within the organization are not defined. Employees are not aware of business continuity risks.

Area/Component C – IT Audit and Compliance

Audit plays a key role in assisting the Board in the discharge of its corporate governance responsibilities by performing an independent assessment of technology risk management processes and IT controls of a BSFI. Controls and supervisory expectations are further discussed in Appendix 75a/Q-59a IT Audit of the MORB/MONBFI. Compliance, on the other hand, is more focused on measuring compliance against established policies and standards and regulatory requirements. As the BSP continues to issue regulations on IT matters and electronic products, the BSFI should remain up to date and ensure that necessary actions are taken to address governing requirements.

Factors to be considered in the assessment include:

1. IT audit organizational structure
2. Qualification and experience of auditors
3. Internal IT audit program
4. Audit participation in development, acquisition, conversion, testing and review of technology service providers
5. Post-closing/monitoring activities
6. Policy compliance process (i.e., measuring and monitoring of compliance with established policies and standards and regulatory requirements)

Below is the rating scale for the component “IT Audit and Compliance”:

Component Rating	Definition	Description
4	Strong	IT audit and compliance processes and activities are strong. Risks and weaknesses are independently identified and reported to the Board and Audit Committee in a timely manner. Outstanding issues are monitored until resolved. Policy compliance process is well-defined. It provides timely and comprehensive information to the Board and Senior Management on new issuances and emerging risks that may necessitate appropriate action or corresponding policy change/update.
3	Satisfactory	IT audit and compliance processes and activities are satisfactory. Risks and weaknesses are independently identified and reported to the Board and Audit Committee but reports may be less timely. Major issues are monitored until resolved. Policy compliance process is defined and provides adequate information to the Board and Senior Management on new issuances and emerging risks that may necessitate appropriate action or corresponding policy change/update.
2	Less than Satisfactory	IT audit and compliance processes and activities are less than satisfactory. Audit independence may be compromised. Reports presented to the Board and Audit Committee are less than satisfactory in content and timeliness. Audit plan does not provide sufficient scope/frequency for key IT areas. Monitoring of outstanding audit issues is inadequate. Policy compliance process is informal and provides limited information to the Board and Senior Management on new issuances and emerging risks that may necessitate appropriate action or corresponding policy change/update.
1	Deficient	IT audit and compliance processes and activities are deficient. Audit lacks independence. Risks and weaknesses

Component Rating	Definition	Description
		are not reported to the Board and Audit Committee. Audit plan is ineffective due to inappropriate audit scope/frequency. Monitoring of outstanding audit issues is lacking. Policy compliance process is deficient or absent.