Federal Financial Institutions Examination Council

FFIEC

Management MGT

JUNE 2004

IT Examination Handbook

TABLE OF CONTENTS

INTRODUCTION

The "Management Booklet" is one of several that comprise the *Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook* (IT Handbook). This booklet rescinds and replaces Chapter 9 "Management" and Chapter 11 "Management Information Systems (MIS) Review" of the *1996 FFIEC Information Systems Examination Handbook*. This booklet provides guidance to examiners and financial institution management.[1] The examination procedures in this booklet assist examiners in evaluating financial institution risk management processes to ensure effective information technology (IT) management.

Effective IT management in financial institutions maximizes the benefits from technology and supports enterprise-wide goals and objectives. The IT department typically leads back-office operations, network administration, and systems development and acquisition efforts. IT management also provides expertise in choosing and operating technology solutions for an institution's lines of business such as commercial credit and asset management, or enterprise-wide activities such as security and business continuity planning. This dual role and the increasing use of technology raise the importance of IT management in effective corporate governance.

Management of IT in financial institutions is critical to the performance and success of an institution. Sound management of technology involves more than containing costs and controlling operational risks. An institution capable of aligning its IT infrastructure to support its business strategy adds value to its organization and positions itself for sustained success. The board of directors and executive management should understand and take responsibility for IT management as a critical component of their overall corporate governance efforts.

The IT Governance Institute defines IT governance as "…an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives."[2] Due to the reliance on technology, effective IT management practices play an integral role in achieving many goals related to corporate governance. The ability to manage technology effectively in isolation no longer exists. Institutions should integrate IT management into the strategic planning function of each line of business within the institution. Financial institutions face many challenges in today's marketplace that increase the importance of IT management.

- Technology is becoming a commodity that is pervasive across all institutions and all business units within an institution.

[1] This booklet uses the terms "institution" and "financial institution" to describe insured banks, thrifts, and credit unions, as well as technology service providers that provide services to such entities.

[2] Board Briefing on IT Governance, 2nd Edition, IT Governance Institute, www.itgi.org, 2003.

- Institution systems connect with customers, business lines, third parties, and the public.
- Technology has created interdependencies among the infrastructure, applications, web content, and the decision-making process necessary to support the delivery of new products and services.
- Timely and accurate information is critical to meeting business requirements throughout the organization.
- The industry continues to experience rapid changes in technologies prompting new investment in infrastructure, systems, and applications.
- New technology requires new expertise, which creates competition for the necessary talent, knowledge, and skill sets.

Effective IT management can leverage opportunities from these challenges while strengthening an institution's ability to manage risk. Advances in technology can result in the ability to offer new products and services to customers, to increase efficiency of operations, to ease the sharing of information between business lines, and to better prepare the institution for future competition. The board of directors and executive management should also understand that new technology and changes in technology could introduce new sources of risk to the institution. External connectivity with non-bank systems, reliance on third parties, involvement in e-commerce, and adoption of new payment systems are some examples that may introduce new or increased operational risk associated with the confidentiality, integrity, and availability of systems and information. Changes in technology may not only introduce new operational risks to manage, but can also introduce an institution to increased risk to its reputation or legal standing. Therefore, IT management is an essential component of effective corporate governance and operational risk management.

This booklet has four parts. First, it provides an overview of how IT management relates to operational and non-operational risks. Second, it describes the structural issues associated with IT oversight. After reviewing the risks and structural issues, the booklet next describes a process for managing technology related risks. The final section provides additional guidance for companies providing technology services to financial institutions.

RISK OVERVIEW

OPERATIONAL / TRANSACTION RISK

Although management needs to be aware of all potential risks, operational risk is the primary risk associated with information technology. Operational risk (also referred to as transaction risk) is the risk of loss resulting from inadequate or failed processes, people, or systems. The root cause can be either internal or external events. Operational risk is present across all business lines.

Operational risk may arise from fraud or error. Management's inability to maintain a competitive position, to manage information, or to deliver products and services can also create and compound operational risk. Weak operational risk management can result in substantial losses from a number of IT threats including business disruptions or improper business practices.

An institution should properly identify, measure, monitor, and control operational risk. Management should distinguish the operational risk component from other risks to enable a stronger focus on operational risk mitigation. The board should ensure a program exists to manage and monitor this risk. The program should address the institution's tolerance for risk, the effectiveness of internal controls, management's accountability in regards to risk mitigation, and the processes needed to manage IT effectively.

Operational risk includes not only back office operations and transaction processing, but also areas such as customer service, systems development and support, internal controls and processes, and capacity planning. Operational risk from IT also affects credit, compliance, strategic, reputation, and market risks. Management should be aware of the implications of operational risk including:

- *Liquidity, interest, and price risks* – Credit and market risks can materialize from external changes in markets, industries, or specific customers. Internal controls that rely heavily on the availability and performance of technology create additional operational risk exposure. For example, a failure to properly implement changes to underwriting, account management, or collection systems can lead to significant losses, and higher loan servicing and collection costs.
- *Reputation risk* – Reputation risk stems from errors, delays, or omissions in information technology that become public knowledge or directly affect business partners, customers and consumers resulting in a loss of confidential information and potential customer withdrawal of funds. Two activities that can lead to reputation risk are the unauthorized disclosure of confidential customer information and the hacking/modifying of an institution's website.
- *Strategic risk* – Strategic risk can stem from inaccurate information or analysis that causes management to make poor strategic decisions. For example, IT management could decide to

save money by delaying an infrastructure upgrade to increase network bandwidth, which could result in a business line losing market share due to an inability to compete.

- *Compliance (legal) risk* – Compliance risk results from the institution's inability to meet the regulatory and legal requirements associated with its IT products and services. Legal risk may lead to civil or criminal liability if, for example, an institution discloses confidential information or provides inaccurate or untimely consumer compliance disclosures.

IT management should have a corporate-wide view of technology. It should maintain an active role in corporate strategic planning to align technology with established business goals and strategies. It also should ensure effective technology controls exist throughout the organization either through direct oversight or by holding business lines accountable for IT-related controls. From a control standpoint, management should assess risks and determine how to control and mitigate the risks. Management should continually compare its risk exposure to the value of its business activities to determine acceptable risk levels.

ROLES AND RESPONSIBILITIES

IT ROLES

Action Summary

Financial institution boards of directors and management should establish IT oversight by ensuring:

- Strong board involvement and awareness of IT activities;
- Circulation and enforcement of sound policies and procedures;
- Implementation and maintenance of an effective risk management process;
- Staff members are competent and sufficient to perform their mission;
- Effective Management Information Systems (MIS) are in place; and
- A sound project management structure is utilized.

BOARD OF DIRECTORS / STEERING COMMITTEE

The board of directors should approve IT plans, policies, and major expenditures. To carry out their responsibilities, board members should be familiar with information technology and data center concepts and activities.

Many boards of directors choose to delegate the responsibility for monitoring IT activities to a senior management committee or IT steering committee. The IT steering committee's mission should be to assist the board in overseeing IT-related activities. The committee should consist of representatives from senior management, the IT department, and major end-user departments. Members do not have to be department heads, but should know IT department policies, practices, and procedures. Each member should have the authority to make decisions within the group for his/her respective areas. Risk management staff should participate in an advisory capacity. See Risk Management Functions on page 9 for more information.

The committee should regularly report to the board on the status of major IT projects or issues. In addition, the committee should ensure the board has adequate information to make informed decisions about IT operations. The board should define the responsibilities of the IT steering committee within a committee charter.

The steering committee should provide general reviews for the board regarding major IT projects. The overview the committee provides enables the board to make decisions without becoming involved in routine operations. The committee helps to ensure business alignment, effective strategic IT planning and oversight of IT performance. The committee may also:

- Oversee the development and maintenance of the IT strategic plan;
- Approve vendors used by the organization and monitors their financial condition;
- Approve and monitor major projects, IT budgets, priorities, standards, procedures, and overall IT performance;
- Coordinate priorities between the IT department and user departments; and
- Review the adequacy and allocation of IT resources in terms of funding, personnel, equipment, and service levels.

The steering committee should receive the appropriate management information from IT departments, user departments, and audit to coordinate and monitor the institutions' IT resources effectively. The committee should monitor performance and institute appropriate action to achieve desired results. The committee should also maintain formal minutes of its meetings to document its decisions and inform the board of directors of its activities.

CHIEF INFORMATION OFFICER / CHIEF TECHNOLOGY OFFICER

Senior management should ensure IT systems meet the needs of the organization. Management should also ensure the institution complies with board policies and the board's strategic plan regarding acquisition or development of IT systems. The senior IT manager or Chief Information Officer (CIO) is responsible for the key IT initiatives of a company. The CIO focuses on strategic issues and the overall effectiveness of the IT organization. This position typically oversees the IT budget and maintains responsibility for performance management, IT acquisition oversight, professional development, and training. In addition, the CIO is responsible for a company's IT architecture and strategic and capital planning. The CIO should be a member of executive management with direct involvement in key decisions for the company and usually reports directly to the CEO. The CIO should play a key role in the strategic technology planning as well as supporting activities of peers in various lines of business. The position often has a leadership role on the IT steering committee.

Some institutions hire a Chief Technology Officer (CTO) to more narrowly focus on tactical issues and the efficiency of the IT organization. The CTO should report to the CIO. The CTO is responsible for understanding the evolution of current technology and how to maximize the value of institution investments in technology. Many institutions combine the roles of CIO and CTO due to their complementary roles.

IT LINE MANAGEMENT

IT line managers supervise the resources and activities of a specific IT function, department, or subsidiary. They typically coordinate services between the data processing area and other user departments. They report to senior IT management on the plans, projects, and performance of their specific systems or departments. Some IT functions that often rely on line managers include data center operations, network services, application development, systems administration, telecommunications, and customer support. Front line managers coordinate the daily activities, monitor current production, ensure adherence to established schedules, and enforce corporate policies and controls in their areas.

BUSINESS UNIT MANAGEMENT

Managers in the institution's various business lines also have IT responsibilities. Examples of these responsibilities include:

- Establishing processes for on-going communication of business needs and strategy;
- Determining MIS needs and product development plans and communicating them to IT support or line management;
- Establishing processes to test compliance with IT related control policies within the business unit;
- Ensuring IT development efforts are prioritized/funded and aligned with business continuity planning within the business unit;
- Ensuring that required backup IT resources are available; and
- Ensuring that participation in testing processes is ongoing.

The specific roles of IT and business unit management, with respect to technology, may vary depending upon the institution's approach to risk management and policy enforcement. Institutions can approach technology management from either a centralized or a decentralized strategy.

In a centralized IT environment, IT management typically acquires, installs, and maintains technology for the entire organization. They have a much greater ability to control and monitor the organization's technology investment. A centralized approach promotes greater operational efficiencies. The business line managers retain the responsibility for enforcing internal controls within their area.

In a decentralized IT environment, IT management only has an advisory role in some departments' acquisition, installation, and maintenance of technology. The decentralized approach is most prevalent in complex institutions where it can expedite the availability of IT services by transferring decision-making authority to strategically significant departments. Business line management has a much greater responsibility for ensuring technology investments are consistent with organization-wide strategic plans. Companies

need to ensure system compatibility and the enforcement of organization-wide policies in a decentralized environment. IT management should still have a role in defining the organization's control requirements, but enforcement is more difficult.

IT RESPONSIBILITIES AND FUNCTIONS

Action Summary

Financial institutions should ensure clear and well-defined responsibilities and expectations exist between risk management and IT functional areas. The critical functional areas include:

- Risk management functions including IT audit, information security, business continuity, outsourcing, and regulatory compliance; and
- IT functions including project management, human resources, operations and MIS.

RISK MANAGEMENT FUNCTIONS

A financial institution should ensure an adequate risk management structure exists within the organization. Some institutions have a separate risk management department that is responsible for overseeing the areas of information security, business continuity planning, audit, insurance and compliance. Regardless of the particular structure used, the institution should ensure that lines of authority are established for enforcing and monitoring controls. These risk management functions should play a key role in measuring, monitoring, and controlling risk.

Information Security

The board is responsible for overseeing and approving the development, implementation, and maintenance of a comprehensive, written information security program, as required by the Gramm-Leach-Bliley Act (GLBA). GLBA is discussed in more detail on page 30 of this booklet. The information security program should include appropriate administrative, technical, and physical safeguards based on the size, complexity, nature, and scope of the institution's operations. The board may delegate information security monitoring to an independent audit function and information security management to an independent information security officer. Ideally, the institution should separate information security program management and monitoring from the daily security duties required in IT operations. The senior information security officer should be an organization-wide risk manager rather than a production resource devoted to IT operations. To ensure independence, the information security officer should report directly to the board or senior management rather than through the IT department. The IT department needs personnel with daily responsibility for implementing the corporate security policy, but they should not have the ability to change policy and grant exceptions. The *IT Handbook's* "Information Security Booklet" has additional information on this topic.

Business Continuity

Similar to information security, business continuity planning should be a corporate-wide strategy. Business continuity planners should assess business continuity across all lines of business. The business continuity function often resides in the risk management organizational structure. The IT department should have personnel responsible for developing and maintaining the department's business continuity plans. The *IT Handbook's* "Business Continuity Planning Booklet" has additional information on this topic.

IT Audit

Senior management and the board should ensure cooperation between management and IT audit. It should also ensure timely and accurate response to audit concerns and exceptions. The IT audit area should report directly to the board of directors or a designated committee of the board comprised of outside directors. The board is responsible for overseeing the audit department's performance and compensation. Audit's key role is to review risk within each of the departments. Audit should verify that management has implemented effective control processes. Audit should have no role in implementing controls and should not have primary responsibility for enforcing policy.

Management should have processes in place to monitor and enforce policy compliance. Audit should verify those processes function effectively and report to the board. The board, in turn, should ensure auditors have the necessary expertise and that audit coverage is adequate, timely, and independent. IT audit coverage should include system development and acquisition projects. See the *IT Handbook's* "Audit Booklet" for additional discussion of this topic.

Compliance

Senior management should ensure the involvement of regulatory compliance staff whenever a new system or application affects compliance with regulations. New implementations or application changes can cause noncompliance through inaccurate interest rate calculations, inadequate or inaccurate disclosures, weak security controls over the storage or transmission of customer information, and poor customer verification procedures. The compliance function should review any new system or significant change for regulatory compliance.

PROJECT MANAGEMENT

Project management is the application of knowledge, skills, tools, and techniques to various activities to meet the requirements of organizational projects.[3] IT management typically has two broad responsibilities. They should control the delivery of technology operations and services to the various lines of business. They should also oversee technology-related changes to operational and business processes. Project management addresses the latter responsibility. An effective project management process is a key factor in a well-managed IT operation.

The operational complexity of the financial institution dictates the formality of project management practices. Generally, project management consists of initiating, planning, executing, controlling, and closing projects. Management uses project management techniques to control projects for systems acquisition and development, as well as other activities including systems conversions, product enhancements, infrastructure upgrades, and system maintenance. A financial institution's ability to manage projects drives its ability to adapt to changes in its business requirements and satisfy its strategic objectives.

Project teams should balance resource investments of time, money, and expertise with the project priority, risk, and requirements. Management should monitor projects closely to control costs and assure adherence to standards and specifications. A project management system should employ well-defined and proven techniques for managing projects at all stages. Controlling a large number of projects requires monitoring systems that include the following elements:

- *Target completion dates* – Management should establish target completion dates for each task or phase of the project. Management determines a final project completion date by carefully identifying and assessing all critical tasks. Identification of realistic target dates for tasks or phases results in improved project control.
- *Project status updates* – Management should compare actual completion dates with planned targeted dates. While project managers may have to revise target dates, management should measure progress against original targets to better assess time and potential cost overruns. If development cost overruns become substantial, management may need to re-evaluate the justification for the project or seek additional approval to continue funding it.

Critical success factors for project management include:

- Experienced and skilled project managers;
- Accepted and standardized project management practices;
- Senior management support for a disciplined project management process;

[3] Project Management Institute, A Guide to the Project Management Body of Knowledge, 2000.

- Stakeholders and IT staff collaboration to establish project requirements and share in the responsibilities for each phase of the project;
- Tracking and measuring project performance against requirements;
- Defining and monitoring an organization-wide project risk assessment methodology; and
- Transition in ownership from implementation teams to the operational teams is a well-managed process with sufficient testing and training.

The *IT Handbook's* "Development and Acquisition Booklet" has additional information on this topic.

OTHER IT FUNCTIONS AND SUPPORT ROLES

Human Resources

The goal of human resources is to hire and maintain a competent and motivated workforce. An organization should have an effective IT human resources management plan that meets the requirements for IT and the business lines it supports. IT management should integrate its management of human resources with technology planning to ensure optimum development and availability of IT skills.

Components of an effective IT human resources management process include compensation planning, performance reviews, participation in industry forums, knowledge transfer mechanisms (e.g., rotational assignments), training, and mentoring. The board should define and enforce incentive programs for IT management, similar to those available for other senior management of the organization, to reward managers who meet IT performance goals.

The company should have programs in place to ensure its staff has the expertise necessary to perform its job and achieve company goals and objectives. A company may need to look externally to find necessary expertise for specialized areas.

Management should develop training programs for all new technology standards and products before their deployment in the organization. Institutions may employ a certification program to ensure the staff maintains the necessary expertise to support the business.

The board and senior management should also consider appropriate succession and transition strategies for key managers and personnel. Some strategies include the use of employment contracts, professional development plans, and contingency plans for interim staffing of key management. Management should mitigate the risk by backing up key positions, cross-training additional personnel, and selecting customized insurance products targeting key employees. The ultimate objective is to provide for a smooth transition in the event of turnover in vital IT management or operations functions.

MIS and Reporting

The IT department often provides an important support role for the institution's management information systems. A management information system (MIS) is a process that provides the information necessary to manage an organization effectively. Accurate and timely MIS reports are an essential component of prudent and reasonable business decisions. Many levels of management view and use MIS, which should support the institution's longer-term, strategic goals and objectives. IT management typically sets policies, procedures, and controls to govern database management and report creation to help ensure the effectiveness and usefulness of the organization's MIS.

Management should design its MIS to:

- Facilitate the management of the business;
- Provide management with an adequate decision support system by providing information that is timely, accurate, consistent, complete, and relevant;
- Deliver complex material throughout the institution;
- Support the organization's strategic goals and direction;
- Ensure the integrity and availability of data;
- Provide an objective system for recording and aggregating information;
- Reduce expenses related to labor-intensive manual activities; and
- Enhance communication among employees.

MIS supplies decision makers with facts, supports and enhances the overall decision-making process and enhances job performance throughout an institution. At the most senior levels, MIS provides the data and information to help the board and management make strategic decisions. At other levels, MIS allows management to monitor the institution's activities and distribute information to other employees, customers, and members of management.

Advances in technology have increased the volume of information available to management and directors for planning and decision-making. Technology increases the potential for inaccurate reporting and flawed decision making. Because report generation systems can rely on manual data entry or extract data from many different financial and transaction systems, management should establish appropriate control procedures to ensure information is correct and relevant. Since management information systems can originate from multiple equipment platforms and systems, the controls should ensure all information systems have sufficient and appropriate controls to maintain the integrity of the information and the processing environment.

Sound fundamental principles for MIS review include proper internal controls, operating procedures, safeguards, and audit coverage. These principles are explained throughout this booklet.

To function effectively, as a feedback tool for management and staff, MIS should be useable. The five elements of information technology processing activities that create useable MIS are timeliness, accuracy, consistency, completeness, and relevance. Compromise of any of these elements hinders the usefulness of MIS.

- *Timeliness* - To facilitate prompt decision-making, an institution's MIS should be capable of providing and distributing *current* information to appropriate users. Developers should design IT systems to expedite the availability of reports. The system should support quick data collection, prompt editing and correction, and meaningful summaries of results.
- *Accuracy* - A sound system of automated and manual internal controls should exist. All information should receive appropriate editing, balancing, and internal control checks. The board should ensure a comprehensive internal and external audit program exists to ensure the adequacy of internal controls.
- *Consistency* - To be reliable, data should be processed and compiled consistently and uniformly. Variations in data collection and reporting methods can distort information and trend analysis. In addition, management should establish sound procedures to allow for system changes. These procedures should be well defined, documented, and communicated to appropriate employees. Management should also establish an effective monitoring system.
- *Completeness* - Decision makers need complete information in a summarized form. Management should design reports to eliminate clutter and voluminous detail to avoid information overload.
- *Relevance* –Information that is inappropriate, unnecessary, or too detailed for effective decision-making has no value. MIS should be relevant to support its use to management. The relevance and level of detail provided through MIS directly correlates to what the board, executive management, departmental or area mid-level managers, etc., need to perform their jobs.

IT RISK MANAGEMENT PROCESS

IT controls result from an effective, risk assessment process. Therefore, the ability to mitigate IT risks is dependent upon risk assessments. Senior management should identify, measure, control, and monitor technology to avoid risks that threaten the safety and soundness of an institution. The institution should (1) *plan* for use of technology, (2) *assess* the risk associated with technology, (3) decide how to *implement* the technology, and (4) establish a process to *measure and monitor* risk that is taken on. All organizations should have:

- An effective planning process that aligns IT and business objectives;
- An ongoing risk assessment process that evaluates the environment and potential changes;
- Technology implementation procedures that include appropriate controls; and
- Measurement and monitoring efforts that effectively identify ways to manage risk exposure.

This process will typically require a higher level of formality in more complex institutions with major technology-related initiatives.

The risk identification and management process for technology-related risks is not complete without consideration of the overall IT environment in which the technology resides. Management may need to consider risks associated with IT environments from two different perspectives:

- If the IT department is a centralized function that supports business lines across shared infrastructure, management should centralize their IT risk management efforts.
- If the IT function is decentralized, and business units manage the risk, then management should coordinate risk management efforts through common organization-wide expectations.

PLANNING IT OPERATIONS AND INVESTMENT

Action Summary

Financial institution boards and management should implement an IT planning process that:

- Aligns IT with the corporate wide strategic plan;
- Aligns IT strategically and operationally with business units;
- Maintains an IT infrastructure to support current and planned business operations;
- Integrates IT spending into the budgeting process and weighs direct and indirect benefits against the total cost of ownership of the technology; and
- Ensures the identification and assessment of risk before changes or new investment in technology.

Planning involves preparing for future activities by defining goals and the strategies used to achieve them. Information technology is an integral part of financial institution operations. Therefore, financial institutions should integrate IT resources and investments into the overall business planning process. Major investments in IT resources have long-term implications on both the delivery and performance of the institution's products and services. Independent data centers also should plan effectively, so they can provide quality and cost effective service to client financial institutions. Institution management should monitor any changes in the current strategies and plans of independent data centers that provide services.

Plans may vary significantly depending on the size and structure of the organization. Every organization should strive to achieve a planning process that constantly adjusts for new risks or opportunities and maximizes the value of IT to the organization. Management should always document plans, however a written plan does not guarantee an effective planning process. Management should measure specific plans by whether they meet the organization's business needs. For all plans, the examiner should evaluate the process as well as the written product. A sound plan requires the board of directors, senior management, and user involvement in the planning process. The board of directors should review and approve the plan. Senior management participates in formulating and implementing the plan. The individual departments and functional areas identify specific business needs and, ultimately, implement the plans.

STRATEGIC IT PLANNING

Strategic IT planning focuses on a three to five year horizon and helps ensure the institution's technology plans are consistent or aligned with its business plans. If effective, strategic IT planning can ensure delivery of IT services that balance cost and efficiency while enabling the business units to meet the competitive demands of the marketplace.

Strategic planning should address long-term goals and the allocation of IT resources to achieve them. Tactical plans outline specific steps and timetables to achieve the strategic goals. These should include hardware and software architecture, end-user computing resources, and any processing done by outside vendors. The strategic plan should address the budget, periodic board reporting, and the status of risk management controls.

The board of directors and management should consider a number of factors when planning the institution's use of technology, including:

- Marketplace conditions;
- Customer demographics;
- Organizational growth targets;
- Technology standards;
- Regulatory requirements (e.g., privacy, security, consumer disclosures);
- Cost containment;
- Process improvement and efficiency gains;
- Customer service and technology performance quality;
- Outsourcing vs. in-house expertise;
- Optimal infrastructure for the future; and
- Ability to adopt and integrate new technology.

All of these factors should also align with the organization's business plans. Well-implemented technology plans provide the capability to deliver business value in terms of market share, earnings, and capital growth to the organization. The information technology steering committee's cross-functional membership makes it well suited for balancing or aligning the organization's IT investment with its strategic and operational objectives. In fact, effective steering committees will constantly work to align the organization's information technology, both strategically and operationally with its business units. Typically, institutions that are better at keeping IT aligned with changing business goals and objectives are positioned to compete more effectively.

Some institutions will spend too aggressively on technology that business lines cannot fully utilize. Also, IT departments or business units can over invest in specific technology that provides inadequate enterprise-wide value, introduces new incompatibilities, or produces unnecessary excess capacity.

On the other hand, institutions can spend too conservatively and delay investments in infrastructure or new products that business lines need to compete and maintain market share and profits. In addition, business units without a full understanding of the available technology can fail to update processes and products or to achieve productivity gains or increased revenues. The lack of knowledge may also result in increased security risks. To create the appropriate balance, institutions should link strategic and operational plans between IT and the business units.

The four key factors of IT planning that management should address are:

- *Strong senior management participation* - Executive management should understand and support the IT strategic plan and established priorities.
- *Role of IT* - The institution needs to clarify IT's role and whether the current IT planning process enables personnel to work towards achieving enterprise-wide goals and objectives.
- *Impact of IT* - The steering committee should understand the relationship between the IT infrastructure and applications and the business strategic and operating plans. The IT infrastructure should directly support the goals and objectives of these plans.
- *Accurate scorecard on past performance* - The steering committee should monitor past IT projects and initiatives after implementation to determine if the institution realized the anticipated costs and benefits. The scorecard should be based upon a set of objective measures.

The board should oversee management's efforts to create and maintain an alignment between IT and corporate-wide strategies by:

- Confirming IT strategic plans are aligned with the business strategy;
- Determining that IT performance supports the planned strategy;
- Ensuring the IT department is delivering on time, within budget, and to specification;
- Directing IT strategy to balance investments between systems that support current operations, and systems that transform operations and enable business lines to grow and compete in new areas; and
- Focusing IT resource decisions on specific objectives such as entry into new markets, enhanced competitive position, revenue growth, improved customer satisfaction, or customer retention.[4]

[4] Board Briefing on IT Governance, 2nd Edition, IT Governance Institute, www.itgi.org, 2003.

OPERATIONAL IT PLANNING

Operational plans should flow logically from the strategic plan. Management should review and revise them at least annually. Operational planning focuses on short-term actions and incorporates the annual budget process. Management should reference the strategic plans and adjust operational plans based on changes in the underlying business needs.

Operational planning addresses the near-term support for business operations. Specifically, operational planning focuses on immediate concerns such as adequate IT resources, sufficient budget, and appropriate risk identification.

IT Resources

Management should ensure that IT resources are adequate to meet the current operational needs of the organization. Operational planning should consider the adequacy of IT resources and the impact of any changes on critical business processes. Business processes are the integration of people, technology, and procedures used to accomplish a task or complete a transaction. Changes in business processes require coordination or alignment with the available IT resources. IT resources that require management coordination include:

- *Infrastructure* - power, telecommunications capacity, network architecture, and facilities.
- *Applications software* - includes changes in software used to provide financial services and products, because of competition, market forces, and changing regulations. These changes may require enhancements to, or replacements of, application software for mainframe, midrange, servers and end-user computing systems.
- *Operating software* - operating systems, compilers, and utilities designed to enable the equipment and applications software to function effectively. Changes in this area can have a major impact on hardware and software specifications.
- *Hardware* - includes mainframes, network servers, personal computers, communications networks, storage devices, and peripherals. Planning should ensure the mainframe, midrange servers and end-user computing equipment have sufficient capacity to meet current needs and future growth. For example, planning may indicate that economically it is impractical to add new mainframe equipment. Rather, it may be appropriate to allow a department to purchase a midrange system to operate independently of the main data center.
- *Personnel* - includes issues associated with staff changes, scheduling requirements, training, and compensation. For example, management should consider whether inadequate salaries could

cause high employee turnover and create a lack of adequate expertise or, if excessive, salaries could suppress earnings.

Budgeting

Budgeting is another step in the operational planning process. The board should assess management's plans and its success in defining and meeting budgetary goals as one means of evaluating the performance of the data processing and operations management. The budget is a coordinated financial plan used to estimate and control the organization's activities. By assessing future economic developments and conditions, management creates an action plan and records changes in the balance sheet accounts and profitability (predicated on implementation of the plan). The budget not only projects expected results, but also serves as an important check on management.

Management, when considering new technology projects, should look at the entry costs of the technology and the post implementation support costs. Increasingly institutions are demanding, and vendors are providing, information regarding the total cost of ownership (TCO) beyond the initial entry costs. Technology projects often have undocumented costs including the resources required to configure, maintain, repair, support, upgrade, and manage the technology over its lifetime. Readily available TCO models, as well as historical data, provide management with tools to incorporate these hidden costs into the selection and budgeting process.

Some financial institutions budget IT as a separate department of the institution. A financial analysis of an IT department should include a comparison of the cost-effectiveness of the in-house operation versus contracting with an outside servicer. It may also include a peer group comparison of operating costs and ratios with a peer group of institutions. Depending upon its size and complexity, the institution may or may not allocate costs to the user departments. Where cost allocation exists, management should ensure equitable assignment of the costs to each user department. This is often accomplished by use of a chargeback system that records usage of resources based upon a performance metric such as Central Processing Unit cycles. In some instances, a separate subsidiary of the holding company manages the IT function. Ideally, an IT subsidiary of a holding company should have a positive affect on consolidated earnings performance. It can provide essential services at costs below external providers or individual financial institutions. However, some relationships may not result in a cost savings. To avoid a preferential arrangement with an affiliate, the contracts between the holding company or its subsidiary and the serviced financial institutions should ensure "arms-length" transactions. Institution management should assess these relationships to ensure they are fair and equitable to all parties. *The IT Handbook's* "Outsourcing Technology Services Booklet" has additional information on contract considerations.

RISK IDENTIFICATION AND ASSESSMENT

Action Summary

Financial institutions should maintain a risk assessment process that drives technology selection and controls implementation. The risk assessment process should incorporate specific assessments conducted for functional responsibilities such as security, business continuity, and vendor management. Risk assessment involves four critical steps:

- Ongoing data collection from new initiatives or monitoring of existing activities;
- Risk analysis regarding the potential impact of the risks;
- Prioritization of controls and mitigating actions; and
- Ongoing monitoring of risk mitigation activities.

Operational IT planning should identify and assess risk exposure to ensure policies, procedures, and controls remain effective. Information security risk assessments are required under the GLBA.[5] The assessments should identify the location of all confidential customer and corporate information, any foreseeable internal and external threats to the information, the likelihood of the threats, and the sufficiency of policies and procedures to mitigate the threats. Management needs to consider the results of these assessments when overseeing IT operations.

GLBA risk assessments should cover all IT risk management functions including security, outsourcing, and business continuity. Senior management should ensure IT-related risk identification and assessment efforts at the enterprise-wide level are coordinated and consistent throughout the organization. A strong, high-level, risk assessment process provides the foundation for more detailed assessments within the functional risk management areas. An effective IT risk assessment process will improve policy and internal controls decisions across the organization.

Senior management can use risk assessment data to make informed risk management decisions based on a full understanding of the operational risks. Small institutions with less complex systems may have a more simplified risk assessment process. Regardless of the complexity, the process should be formal and should adapt to changes in the IT environment. Examiners should measure the effectiveness of the process by evaluating management's understanding and awareness of risk, the adequacy of formal risk assessments, and the effectiveness of the resulting policies and internal controls.

[5] Federally insured credit unions must comply with 12 CFR 748. Appendix A of 12 CFR 748 contains guidelines specifically relating to information security risk assessments to assist credit unions in complying with the requirements of 12 CFR 748.

Ongoing Data Collection

Understanding the institution's environment is the first step in any risk assessment process. Senior management should incorporate information on IT issues such as resource limitations, threats, priorities, and key controls from several sources. In developing a formal risk assessment, management should collect and compile information regarding the organization's information technology environment from several locations including:

- IT systems inventories are critical to understanding and monitoring the tactical operations of the institution's information technology as well as to identifying the access and storage points for confidential customer and corporate information.
- IT strategic plans provide insight into the organization's planning process. Review and analysis of the strategic plans as part of the risk assessment process may spotlight developing risk exposures or other deficiencies that limit the institution's ability to implement strategic priorities.
- Business recovery and continuity plans prioritize the availability of various business lines to the institution and often encompass restoration and provision of control, customer service, and support. The plans can offer insight into the organization's critical operating systems and the control environment.
- Due diligence and monitoring of service providers can present valuable information on the servicer control environment. The information is necessary for a complete risk assessment of institution's information technology environment.
- Call center issue tracking reports can often indicate potential performance or control issues if the problem reports are aggregated and analyzed for repetitive or common issues.
- Department self-assessments on IT-related controls can provide early identification of policy noncompliance or weaknesses in controls.
- IT audit findings provide insight into the veracity and responsiveness of the institution's staff and management, commitment to policy compliance and internal controls.

Risk Analysis

Management should use the data collected on IT assets and risks to analyze the potential impact of the risks on the institution. The analysis should identify various events or threats that could negatively affect the institution strategically or operationally. Management should evaluate the likelihood of various events and rank the possible impact. Some examples of events that could affect the institution include the following:

- Security breaches - Security breaches that can affect the institution include external and internal security breaches, programming fraud, computer viruses, or denial of service attacks.
- System failures - Common causes of system failures include network failure, interdependency risk, interface failure, hardware failure, software failure, or internal telecommunication failure.
- External events - Institutions are also exposed to external threats including weather-related events, earthquakes, terrorism, cyber attacks, cut utility lines or wide spread power outages that bring about system or facility failures.
- Technology investment mistakes - Mistakes in technology investment including strategic platform or supplier risk, inappropriate definition of business requirements, incompatibility with existing systems, or obsolescence of software may constrain profitability or growth.
- Systems development and implementation problems - Common system development and implementation problems include inadequate project management, cost/time overruns, programming errors (internal/external), failure to integrate and/or migrate successfully from existing systems, or failure of system to meet business requirements.
- Capacity shortages - Shortages in capacity result from lack of adequate capacity planning, including the lack of accurate forecasts of growth.

Once the institution has identified the universe of risks, management should estimate the probability of occurrence as well as the financial, reputation, or other impact to the organization. Organizational impacts are highly variable and not always easy to quantify, but include such considerations as lost revenue, flawed business decisions, data recovery and reconstruction expense, costs of litigation and potential judgments, loss of market share, and increases to premiums or denials of insurance coverage. Typically, risk analysis ranks the results based on the relationship between cost and probability.

Prioritization

Once management understands the institution's technology environment and analyzes the risk, it should rank the risks and prioritize its response. The probability of occurrence and the magnitude of impact provide the foundation for reducing risk exposures or establishing mitigating controls for safe, sound, and efficient IT operations appropriate to the complexity of the organization. The overall risk assessment results should be a major factor in decision making in most IT management responsibility areas including:

- Technology budgeting, investment, and deployment decisions;
- Contingency planning;
- Policies and procedures;

- Internal controls;
- Staffing and expertise;
- Insurance;
- IT performance benchmarks;
- Service levels for internal and outsourced IT services; and
- Policy enforcement and compliance.

Monitoring

Management and the board should monitor risk mitigation activities to ensure identified objectives are complete or in process. Monitoring should be ongoing, and departments should provide progress reports to management on a periodic basis. Ongoing monitoring further ensures that the risk assessment process is continuous instead of a one-time or annual event. Key elements of an effective monitoring program include:

- Mitigation or corrective action plans;
- Clear assignment of responsibilities and accountability; and
- Management reporting.

IT CONTROLS IMPLEMENTATION

Action Summary

Financial institution management should implement satisfactory control practices as part of its overall IT risk mitigation strategy. These practices should include:

- Internal controls that effectively mitigate the identified risks associated with IT processes such as system and security administration, systems development, IT operations, outsourced functions, vendor management, and other IT risk areas;
- Ensuring controls over MIS to provide management with accurate and timely information to make informed decisions;
- Adoption and enforcement of IT policies and standards;
- Standards for hiring, changing duties, and terminating IT personnel, including internal staff, consultants, temporary employees, and other external parties;
- Training and assessment programs to maintain IT expertise levels;
- Annual review of IT insurance coverage and needs;
- Formal business continuity plans for each critical area of operations; and
- Oversight and management of third-party relationships.

This section provides guidelines for controls that will reduce risk when effectively implemented. These guidelines are applicable to both in-house and external provider situations. The financial institution should review and assess external provider practices for consistency with these guidelines. Identified gaps represent increased risk, which management should mitigate before establishing a formal relationship.

POLICIES, STANDARDS, AND PROCEDURES

Management should adopt and enforce appropriate policies and procedures to manage technology risk. The effectiveness of these policies and procedures depends largely on whether they are used by internal staff and vendors. Testing compliance with these policies and procedures often helps to identify and correct problems before they become serious. Clearly written and frequently communicated policies can establish clear assignments of duties, help employees to coordinate and perform their tasks effectively and consistently, and aid in the training of new employees. Senior management should ensure policies, procedures, and systems are current and well documented.

In general, a policy is a governing principle that provides the basis for standards, and carries the highest authority in the organization. It is an overall statement of corporate philosophy or intent that reflects the best market practice. Standards are mandatory

criteria that ensure corporate conformity with policy, government regulations, and acceptable levels of control. Procedures are typically documents that describe, in detail, the behavior or processes used to adhere to the criteria mandated by standards.

Financial institutions should create, document, maintain, and adhere to policies and standards to manage and control their IT environment. Documented procedures are one of the evidentiary elements that can demonstrate compliance to those policies and standards. The level of detail required is dependent upon the complexity of the IT environment, but should enable management to monitor the identified risk posture.

INTERNAL CONTROLS

The institution should adopt adequate controls based on the degree of exposure and the potential risk of loss arising from the use of technology. Controls should include clear and measurable performance goals, the allocation of specific responsibilities for key project implementation, and independent mechanisms that will both measure risks and minimize excessive risk-taking. Management should re-evaluate these controls periodically.

Management should establish an effective system of internal controls. Internal controls for an IT environment generally should address the overall integrity of that environment. Typically, internal controls span management and multiple technical disciplines. The scope and quality of internal controls are key components of the risk assessment process. Senior management is responsible for the oversight and monitoring of internal controls.

Management should identify the specific requirements for internal controls in the financial institution's policies, standards, and practices in order to establish an auditable baseline. The established baseline provides a general picture of the control environment. The detail aspects for each area or discipline are used to measure compliance against the established requirements (standards).

Management practices associated with general controls include:

- Reporting effectiveness to the Board of Directors;
- Periodic review and updating of policies, standards, and practices;
- Regular review of internal and third party audit results;
- Review of service level agreements; and
- Review of control metrics including issues and corrective action plans.

Adequate internal controls should be structured to assure senior management that:

- Personnel create, transmit, and store records and transactions in a safe and sound manner;
- Adequate segregation of duties exists;
- MIS data are reliable and the reporting cycle is adequate;

- Operating procedures are efficient and effective;
- Procedures are in effect to assure continuity of business;
- The institution identifies and monitors high-risk conditions, functions, and activities; and
- There is proper adherence to management standards and policies, applicable laws and regulations, regulatory statements of policy, and other guidelines.

Independent audits can verify that these controls exist and are functioning effectively.

PERSONNEL

Financial institutions should mitigate the risks posed by IT staff by performing appropriate background checks and screening of new employees. In addition to staff, the controls in this section are relevant for vendor personnel, consultants, and temporary staff that support the IT function. Typically, the minimum verification considerations include:

- Character references;
- Background checks including confirmations of prior experience, academic credentials, professional qualifications, or criminal records; and
- Confirmation of identity from government issued identification.

Financial institutions should protect the confidentiality of information about their customers and organization by obtaining agreements covering confidentiality, nondisclosure, and authorized use. Management should obtain signed confidentiality and nondisclosure agreements before granting new employees, contractors, and temporary staff access to information technology systems. In addition, management should require periodic acknowledgement of acceptable use policies for the network, software applications, Internet, e-mail, and institution data.

Financial institutions should use job descriptions, employment agreements (usually higher level positions), training, and awareness programs to promote understanding and increase individual accountability. Management should routinely update the institution's written job descriptions. The job descriptions should confirm and promote user access rights. Employment agreements set both the expectations and limits associated with the employee's functions. Information security awareness and training programs help support these and other management policies.

Financial institutions should establish a timely process to remove or change access rights associated with any party when appropriate. The lack of such a process may result in unauthorized or inappropriate activity. The failure to remove access rights, particularly for those individuals with high levels of privilege, represents significant risk.

INSURANCE

In establishing an insurance program, management should recognize its exposure to loss, the extent to which insurance is available to cover potential losses, and the cost of such insurance. Insurance programs should be commensurate with the complexity and risk of each institution. Management should weigh these factors to determine how much risk the organization will assume directly. In assessing the extent of that risk, institutions should analyze the effect of an uninsured loss on themselves and any affiliates or parent companies. Management should also review a company's financial condition and/or credit rating reviews when deciding on an insurance company. Once management has acquired appropriate insurance coverage, it should establish procedures to review and ensure its adequacy. These procedures should include, at a minimum, an annual program review by the board of directors.

Insurance complements, but does not replace, an effective system of controls. Thus, an overall appraisal of the control environment becomes significant in assessing the adequacy of the insurance program. Effective controls and audits may result in lower premiums. Before purchasing insurance, management should assess the costs of insuring:

- IT equipment and facilities;
- Media reconstruction;
- Business interruption;
- Loss of items in transit;
- Employee fidelity;
- Extra expense;
- E-banking activities;
- Errors and omissions; and
- Liability to customers resulting from electronic fund transfer system (EFTS) activities.

Estimates of these costs will enable management to choose the types and amounts of insurance to carry. They also allow management to determine to what extent the institution should self-insure against certain losses.

An institution or data center can insure against risks covered in standard insurance policies. Insurance that covers physical disasters often specifically excludes computer equipment. Those policies usually cover replacement of the physical magnetic media, but omit the cost of reconstructing the recorded information found in the media. Management should clearly understand what is covered and document any gaps in coverage that may exist.

Insurance policies provide a variety of IT-related coverage. They are constructed so that they can be adapted to the particular institution's IT environment. Some examples of specific coverage and guidelines for evaluating them include:

- *IT Equipment and Facilities* – Management should obtain coverage of physical damage to the data center and automation equipment throughout the institution. Coverage should include leased equipment if the lessee is responsible for hazard coverage.
- *Media Reconstruction* – An institution should obtain insurance for damage to IT media, such as magnetic tape and disks, if it is the institution's property and the institution has liability for the media. Insurance is available for on-premises, off-premises, or in-transit situations. It should cover the actual reproduction cost of the property or, if not replaced or reproduced, the blank value of the media. Additional considerations to determine the amount of coverage include programming costs, physical replacement, and backup expense.
- *Extra Expense* – Insurance coverage should include the extra costs of continuing operations following damage or destruction at the data processing center or other work areas.
- *E-banking Activities* – Insurance coverage should include loss or liability arising from electronic banking activities such as Internet banking and bill payment services.
- *Business Interruption* - Data centers and institutions offering outside services should obtain coverage that reimburses them for monetary losses resulting from suspension of operations, because of physical loss of equipment or media.
- *Valuable Papers and Records* – Coverage should include the actual cash value of papers and records (not defined as media) against direct physical loss or damage.
- *Errors and Omissions* – Management should obtain insurance that provides protection against claims arising from negligent acts, errors, or omissions that occur in performing IT services for others. These policies commonly contain the following exclusions:
  - Employee dishonesty;
  - Libel, slander, or defamation of character;
  - Liability of others assumed by the insured under contract or agreement;
  - Liability of loss or damage to property of others;
  - Personal or bodily injury or sickness;
  - Liability arising out of advice from third parties on methods, procedures, practices, etc.;
  - Liability for preparation of income tax returns; and
  - Loss caused intentionally by, or at the direction of, the insured.

INFORMATION SECURITY

The board of directors is responsible for overseeing the development, implementation, and maintenance of the institution's information security program. The board should provide management with guidance and review the effectiveness of management's actions. The board should approve written information security policies and the information security program at least annually. The board should provide management with its expectations and requirements for:

- Central oversight and coordination;
- Areas of responsibility;
- Risk measurement;
- Monitoring and testing;
- Reporting; and
- Acceptable residual risk.[6]

Information is one of a financial institution's most important assets. Management and the board of directors should protect information assets to establish and maintain trust between the financial institution and its customers. The unauthorized loss, destruction, or disclosure of confidential information can adversely affect a financial institution's earnings and capital.

The GLBA, section 501(b), requires management to develop and the board to approve an information security program to protect the security and confidentiality of customer information. The institution should protect customer information from any anticipated threats to security or integrity. It should also protect customer information from unauthorized access or use that would result in substantial harm or inconvenience to any customer. GLBA also requires that the Board oversee the development, implementation and maintenance of the bank's security program and that it assigns specific responsibility for its implementation. The Board should also review an annual report, prepared by management, regarding the bank's actions toward GLBA compliance. The *IT Handbook's* "Information Security Booklet" has additional information on this topic.

BUSINESS CONTINUITY

The board of directors and senior management are responsible for establishing policies, procedures, and responsibilities for organization-wide business continuity planning. At a minimum, the board of directors should annually update and approve the institution's business continuity plans. Management should document, maintain, and test the organization's business continuity plan and back-up systems on a periodic basis to mitigate the risk of system failures and unauthorized intrusions. Management should also report the tests of the plan and back-up systems to the board of directors on an annual

[6] FFIEC IT Examination Handbook, Information Security Booklet

basis. Detailed information on this topic is available in the *IT Handbook's* "Business Continuity Planning (BCP) Booklet."

SOFTWARE DEVELOPMENT AND ACQUISITION

Senior management should assess and mitigate the operational/transactional risks associated with the development or acquisition of software. Management should develop applicable policies and standards, which specify risk management controls for the development and acquisition of systems. Uncontrolled software development or acquisition may introduce unacceptable levels of risk.

Management should guide the development or acquisition of software by using a system development life cycle (SDLC) or similar methodology that is appropriate for the specific IT environment. A SDLC methodology will also help to identify the risks when acquiring software, however financial institutions should consider the vendor's control environment, reputation, and capabilities.

Each phase of the SDLC should have procedures that verify the maintenance and integrity of controls before the start of the next phase. An institution should review information security aspects in each phase to identify those requirements. Audit should be involved to ensure proper security is incorporated during development. Depending upon the size and complexity of the institution, management should analyze the operational impact early in the process to identify any additional cost and support issues.

Management should test new technology, systems, and products thoroughly before deployment. Testing validates that equipment and systems function properly and produce the desired results. As part of the testing process, management should verify whether new technology systems operate effectively with other technology components including vendor-supplied technology. Pilot programs or prototypes can be helpful in developing new technology applications before management accepts them for use on a broad scale. Management should conduct retesting periodically to help manage risk exposure on an ongoing basis.

Refer to the *IT Handbook's* "Development and Acquisition Booklet" for additional detailed information on this topic.

OPERATIONS

Senior management should be aware of and mitigate the operational/transactional risks associated with IT operations. Financial institutions and their service providers may have one or more IT operations groups. The number and types will vary from organization to organization. Common examples are data center or computer operations, network services, distributed computing, personal or desktop computing, change management, security, resource management, and contingency planning.

Many operations functions have significant risk factors that need effective management and control. For example, system and security administrators have powerful levels of

control over the systems they operate or manage. Institutions should record and review audit trails and logs of system and security administrator activities to control the risk exposure. Additional information on this topic is available in the *IT Handbook's* "Operation's Booklet."

OUTSOURCING RISK MANAGEMENT

Financial institutions increasingly rely on service providers, software vendors, and other third parties. Complex institutions often have an institution-wide vendor management program that encompasses all of these relationships. IT departments can contract with third parties for a large number of services including data processing, software development, equipment maintenance, business continuity, data storage, Internet access, and security management.

The board of directors and senior management are responsible for ensuring appropriate oversight of outsourced relationships. Technology needed to support business objectives is often a critical factor in deciding to outsource. Managing such relationships is not just a technology issue; it is an enterprise-wide corporate governance issue. An effective outsourcing oversight program should provide the framework for management to understand, monitor, measure, and control the risks associated with outsourcing. The board and senior management should develop and implement enterprise-wide policies and procedures to govern the outsourcing process including establishing objectives and strategies, selecting a provider, negotiating the contract, and monitoring the outsourced relationship.

Some factors institutions should consider or address include:

- Ensuring each outsourcing relationship supports the institution's overall objectives and strategic plans;
- Evaluating prospective providers based on the scope and criticality of outsourced services; and
- Tailoring the enterprise-wide service provider monitoring program based on an initial and ongoing risk assessment of outsourced services.

The time and resources devoted to effectively manage outsourcing relationships will depend on several factors, such as the criticality of outsourced processes, staff knowledge, and complexity of systems.

Detailed information on this topic is available in the *IT Handbook's* "Outsourcing Technology Services Booklet."

MEASURE AND MONITOR

Action Summary

Financial institution management should ensure satisfactory monitoring and reporting of IT activities and risk. These practices should include:

- Routine review of business plan goals and strategies relative to information technology;
- Developing benchmarks for reviewing performance;
- Establishing and reviewing service level agreements with critical vendors and third parties; and
- Implementing a quality control or quality assurance program to monitor and test products and practices.

Financial institutions should continuously measure and monitor the risk profile of their IT functions. Metrics, as part of the monitoring process, will aid management in its ability to assess the overall program. The specific metrics reported, and the frequency, will depend upon the IT environment of the institution. Some common examples are:

- The current number of risk issues identified for each IT discipline (updated regularly to reflect new or mitigated issues);
- The current number of risk acceptance issues approved by senior management (a database or other repository of the descriptions, mitigation options, and evidence of management acceptance should be maintained);
- Current and historical counts of events or issues (external and internal events that deviate from the control standards); and
- Current counts of internal audit, external audit, or regulator identified issues.

PLAN-TO-ACTUAL OUTCOME MEASURES (OUTCOME-BASED MEASUREMENT)

Financial institutions should periodically review their IT function and determine if their plan, goals, and expectations are on target. Given the cost of, and business reliance upon, IT functions, failure to perform such measurements could put the institution at risk. Management should measure outsourced relationships by the penalties and incentive clauses in the service contracts.

PERFORMANCE BENCHMARKS

Financial institutions should establish performance benchmarks or standards for IT functions and monitor them on a regular basis. Such monitoring can identify potential problem areas and provide assurance that IT functions are meeting the objectives. Areas

to consider include mainframe and network availability, data center availability, system reruns, out of balance conditions, response time, error rates, data entry volumes, special requests, and problem reports.

SERVICE LEVELS

Financial institutions should establish formal service level agreements with their IT provider, for both in-house and outsourced functions. Service level agreements (SLAs) establish mutual expectations and provide a baseline to measure IT performance. Management can also tie SLAs to incentive and penalty actions. SLAs should broadly cover the IT environment to provide the institution the greatest level of assurance. Performance benchmarks and outcome-based measurements (see above) are examples of SLA issues.

QUALITY ASSURANCE/QUALITY CONTROL

Management should establish quality assurance procedures and update future planning with the quality assurance results. These procedures may include internal performance measures, focus groups, and customer surveys. Management should conduct quality assurance reviews for all significant activities both internally and with another organization.

The traditional goal of Quality Assurance (QA) activities is to ensure the product conforms to specifications, and is fit to use. QA asks three fundamental questions: Does it work? Does it do what it is designed to do? Is it fit for use? The purpose of quality Control (QC) activities is to identify weaknesses in work products and to avoid the resource drain and expense of redoing a task. While financial institutions will benefit from that perspective, they also have additional incentives to incorporate QA functions into their IT environment. QA functions can be effective in preventing internal fraud. For example, management can conduct quality assurance testing on a new system before implementation. The testing should be independent of any programming function (if developed in-house) and incorporate user acceptance testing programs (if off-the-shelf). The thorough testing of a new system can identify malicious code or poor functionality. QA reports are a valuable tool for management and help document the control process for the production environment.

POLICY COMPLIANCE

Financial institutions should develop, implement, and monitor a process to measure IT compliance with their established policies, standards, and practices. In addition to the traditional reliance upon internal and third party audit functions, financial institutions should perform self-assessments on a periodic basis. The scope and frequency of self-assessments will depend upon the scale and historical performance of the IT function. Self-assessment activities broaden management's perspective by involving a varied audience and by requiring acknowledgement of the results by those involved. The self-assessment process can help identify the need for policy changes and updates.

MANAGEMENT CONSIDERATIONS FOR TECHNOLOGY SERVICE PROVIDERS

Action Summary

Technology service providers (TSPs) should support customer institutions by:

- Providing audited financial statements at least annually;
- Negotiating clear contracts with appropriate language;
- Implementing independent audit programs governing TSP controls and reporting findings to customers; and
- Providing responsive customer service including user group support.

Financial institutions should oversee the quality of service, financial condition, and control environment of the companies providing them with critical IT services. The *IT Handbook's*, "Outsourcing Technology Services Booklet" provides detailed guidance for institutions to follow. The booklet addresses the risk management concerns from the perspective of the service recipient. TSPs include financial institutions, affiliates, and independent third parties. TSPs have an obligation to support their customers' oversight responsibilities. Financial institutions should expect TSP support at a level consistent with the criticality of the services provided to the institution. Unlike the institutions' risk management efforts, the TSP's size and complexity have little impact on its risk management expectations. This section provides additional management considerations TSPs should address to support financial institutions in meeting their safety and soundness and consumer compliance obligations.

FINANCIAL INFORMATION

Financial institutions should receive sufficient current information from TSPs to perform due diligence and, at least annually, ongoing monitoring. Publicly held TSPs have mandatory financial reporting obligations, which facilitate obtaining financial information. Where mandatory reporting requirements do not exist, such as in the case of privately held TSPs, institutions should obtain contractual assurances that the TSP will provide financial statements (preferably independently audited) at least annually.

Bankruptcy of a TSP can have a devastating impact on a serviced institution. Under such circumstances, the TSP may not be able to provide a 60- to 120-day notification of service termination. In this situation, the serviced institution, not the TSP, would need to find an alternate processing site. Although the user institutions retain ownership to data

and should be able to obtain current data files from their TSP, the TSP typically owns the programs and documentation required to process those files. Without specific contract provisions, the TSP may not be willing to make the programs available to the users. These programs are often one of the TSP's significant assets. Therefore, a creditor, in an attempt to recover outstanding debts, might attach a lien to those assets that will limit the availability of the programs to the users. At this point, the serviced institutions could: (1) pay off the creditor and hire outside specialists to operate the center, (2) convert data files to another servicer, or (3) purchase equipment, license software and begin processing in-house. All of these options are costly and can cause unacceptable processing delays.

TSPs suffering financial deterioration should communicate with customers, seek additional sources of capital, or develop capital plans to alleviate customer concerns as quickly as possible. If a TSP fails to provide proper financial data, the institution should evaluate the significance of the services to the institution and determine whether a lack of information about the financial stability of the company should stop it from entering into a contract or from continuing a contractual relationship.

CONTRACTS

TSPs and customer financial institutions should negotiate contracts that incorporate the recommended items contained in the *IT Handbook's* "Outsourcing Technology Services Booklet". Financial institutions should negotiate clear, written contracts with sufficient detail to provide assurances for performance, reliability, security, confidentiality, and reporting. A poorly written or inadequately reviewed contract can increase the risk to both the serviced financial institution and the TSP. To avoid or minimize problems in such a contractual arrangement, legal counsel familiar with the terminology and specific requirements of a data processing contract should review it to protect each party's interests. Since the contract sets the terms of a multi-year understanding between the parties, all items agreed upon during negotiations should be included in the final signed contract.

Contracts establish baseline performance standards for information processing services. In addition, the contract defines each party's responsibilities and liabilities. Institutions may encounter situations where service providers cannot or will not agree to terms that the institution requests to manage the risk effectively. Under these circumstances, institutions should either not contract with that provider or supplement the service provider's commitments with additional controls to mitigate the risk. If an institution experiences problems obtaining regulatory required revisions to existing contracts, it should notify user groups and its primary regulator for additional support.

AUDIT REPORTS

A TSP should provide its customer financial institutions' auditors with sufficient access to its data center to meet the clients' oversight responsibilities. An alternative is for the TSP to make audit reports, control reviews, and other independent reviews directly

available to its customer financial institutions. The *IT Handbook's* "Audit Booklet" provides additional information on various third-party audit options available to TSPs.

CUSTOMER SERVICE

TSPs should have customer service programs that monitor performance, track customer problems or concerns, and resolve issues on a timely basis. The formality of a customer service program depends on the size of the servicer's customer base. A large TSP may require a customer call center with formal problem tracking software to ensure responsive customer service. Smaller TSPs may be able to handle call volumes less formally. Some actions TSPs can take include:

- Create a customer service policy that directs employees on how to act, outlines types of appropriate responses, establishes minimum response times, and authorizes escalation to more senior employees;
- Track problems through resolution (by the use of logs) to evaluate response times and to identify any commonality among user problems;
- Provide regular reports monitoring contractual or agreed upon service levels; and
- Obtain customer feedback through user groups or customer surveys.

TSPs should encourage customer institutions to form a user group if sufficient numbers of customers will support it. User groups offer advantages to both the TSP and the serviced institution by allowing customers to discuss and prioritize their concerns.

APPENDIX A: EXAMINATION PROCEDURES

EXAMINATION OBJECTIVE: Determine the quality and effectiveness of the organization's management of information technology. Examiners should use these procedures to measure the adequacy of the institution's IT risk management process, including management awareness and participation, risk assessment, policies and procedures, reporting, ongoing monitoring, and follow-up.

This workprogram is intended to assist examiners in determining the effectiveness of a financial institution's IT management process. However, examiners may choose to use only particular components of the workprogram based upon the size, complexity, and nature of the institution's business.

Objective 1: Determine the appropriate scope and objectives for the examination.

1. Review past reports for outstanding issues or previous problems. Consider:
   - Regulatory reports of examination,
   - Internal and external audit reports,
   - Independent security tests, and
   - Regulatory and audit reports on service providers.
2. Review management's response to issues raised at, or since the last examination. Consider:
   - Adequacy and timing of corrective action,
   - Resolution of root causes rather than just specific issues,
   - Existence of any outstanding issues, and
   - If management has taken positive action toward correcting exceptions reported in audit and examination reports,
3. Interview management and review the response to pre-examination information requests to identify changes to the technology infrastructure or new products and services that might increase the institution's risk. Consider:
   - Products or services delivered to either internal or external users,
   - Network topology including changes to configuration or components,
   - Hardware and software listings,
   - Loss or addition of key personnel,
   - Technology service providers and software vendor listings,

- Communication lines with other control functions (e.g., loan review, credit risk management, line of business quality assurance, and internal audit),
- Credit or operating losses primarily attributable (or thought to be attributable) to IT (e.g., system problems, fraud occurring due to poor controls, improperly implemented changes to systems),
- Changes to internal business processes, and
- Internal reorganizations.

Objective 2: Determine whether board of directors and senior management appropriately consider IT in the corporate governance process including the process to enforce compliance with IT policies, procedures, and controls.

1. Review the corporate and Information Technology (IT) departmental organization charts to determine if:
   - The organizational structure provides for effective IT support throughout the organization,
   - IT management reports directly to senior level management,
   - The IT department's responsibilities are appropriately segregated from business processing activities, and
   - Appropriate segregation of duties exists.
   - Review biographical data of key personnel and the established staff positions to determine the adequacy of:
   - Qualifications,
   - Staffing levels, and
   - Provisions for management succession.
   - Review and evaluate written job descriptions to ensure:
   - Authority, responsibility, and technical skills required are clearly defined, and
   - They are maintained in writing and are updated promptly.
   - Identify key positions and determine whether:
   - Job descriptions are reasonable and represent actual practice,
   - Back-up personnel are identified and trained, and
   - Succession plans provide for an acceptable transition in the event of loss of a key manager or employee.
     - Determine the effectiveness of management's communication and monitoring of IT policy compliance across the organization.

- Consult with the examiner reviewing audit or IT audit to determine the adequacy of coverage and management's responsiveness to identified weaknesses.

Objective 3: Determine the adequacy of the IT planning and risk assessment.

1. Review the membership list of board, IT steering, or relevant management committees established to review IT related matters. Determine if board, senior management, business lines, audit, and IT personnel are represented appropriately and regular meetings are held.
2. Review the minutes of the board of directors and relevant committee meetings for evidence of senior management support and supervision of IT activities.
3. Determine if committees review, approve, and report to the board of directors on:
   - Information security risk assessment,
   - Short and long-term IT strategic plans,
   - IT operating standards and policies,
   - Resource allocation (e.g., major hardware/software acquisition and project priorities),
   - Status of major projects,
   - IT budgets and current operating cost,
   - Research and development studies, and
   - Corrective actions on significant audit and examination deficiencies.
4. Determine if the board of directors or senior management gives adequate consideration to the following IT matters when formulating the institution's overall business strategy:
   - Risk assessment,
   - IT strategic plans,
   - Current status of the major projects in process or planned,
   - Staffing levels (sufficient to complete tasks as scheduled),
   - IT operating costs, and
   - IT contingency planning and business recovery.

5. Review the strategic plans for IT activities. Determine if the goals and objectives are consistent with the institution's overall business strategy. Document significant changes made since the last examination or planned that affect the institution's organizational structure, hardware/software configuration, and overall data processing goals. Determine:

   - If business needs are realistic,
   - If IT has the ability to meet business needs,
   - If the strategic plan defines the IT environment,
   - If the plan lists strategic initiatives,
   - If the plan explains trends and issues of potential impact, and
   - If there are clearly defined goals and metrics.

6. Review turnover rates in IT staff and discuss staffing and retention issues with IT management. Identify root causes of any staffing or expertise shortages including compensation plans or other retention practices.

7. If IT employees have duties in other departments, determine if:

   - Management is aware of the potential conflicts such duties may cause, and
   - Conflicting duties are subject to appropriate supervision and compensating controls.

8. Review the adequacy of insurance coverage (if applicable) for:

   - Employee fidelity,
   - IT equipment and facilities,
   - Media reconstruction,
   - E-banking,
   - EFT,
   - Loss resulting from business interruptions,
   - Errors and omissions,
   - Extra expenses, including backup site expenses,
   - Items in transit, and
   - Other probable risks (unique or specific risks for a particular institution).

Objective 4: Evaluate management's establishment and oversight of IT control processes including business continuity planning, information security, outsourcing, software development and acquisition, and operations.

1. Review the board of directors and Management IT oversight program. Determine if the Board:
   - Is directly involved in setting or managing IT oversight,
   - Established a steering committee,
   - Implemented processes and procedures that meet objectives of governing IT policies,
   - Approved appropriate oversight policies for Information Security,
   - Has current policies, processes and procedures that result in compliance with applicable regulatory requirements, e.g., GLBA,
   - Addressed risks regarding system development and acquisition, and
   - Has a process in place for business continuity planning.
2. Review the IT governance (i.e., steering committee) practices established by management.
3. Review major acquisitions of hardware and software to determine if they are within the limits approved by the board of directors.
4. Review the IT management organizational structure to determine if the Board established:
   - A defined and functioning role for either the CIO/CTO;
   - Integration of business line manager(s) into the IT oversight process; and
   - Involvement of front line management in the IT oversight process.

Objective 5: Determine whether Board of Directors and management effectively report and monitor IT-related risks.

1. Determine if management and the Board of Directors:
   - Annually review and approve a formal, written, information security program,
   - Approve and monitor the risk assessment process,
   - Approve and monitor major IT projects,
   - Approve standards and procedures,
   - Monitor overall IT performance,
   - Maintain an ongoing relationship between IT and business lines,

- Review and approve infrastructure, vendor, or other major IT capital expenditures based upon board set limits,
- Review and monitor the status of annual IT plans and budgets,
- Review management reports, measure actual performance of selected major projects against established plans. Determine the reasons for the shortfalls, if any, and
- Review the adequacy and allocation of IT resources, including staff and technology.

2. Review the risk assessment to determine whether the institution has characterized their system properly and assessed the risks to information assets. Consider whether the institution has:

   - Identified and ranked information assets according to a rigorous and consistent methodology that considers the risks to customer and non-public information as well as risks to the institution,
   - Identified all reasonable threats to financial institution assets, and
   - Analyzed its technical and organizational vulnerabilities.

3. Identify whether the institution effectively updates the risk assessment before making system changes, implementing new products or services, or confronting new external conditions.

4. Determine the effectiveness of the reports used by senior management or relevant management committees to supervise and monitor the following IT activities:

   - Management reports that provide the status of software development/maintenance activities,
   - Performance and problem reports prepared by internal user groups,
   - System use and planning reports prepared by operating managers, and
   - Internal and external audit reports of IT activities.

Objective 6: Determine the appropriateness of IT policies, procedures, and controls based on the nature and complexity of the institution's operations.

1. Determine if IT management has adequate standards and procedures governing the following items through examination or by discussing the issues with other examiners performing reviews in these areas:

   - Risk assessment,
   - Personnel administration,
   - Development and acquisition,

- Computer operations,
- Outsourcing risk management,
- Computer and information security,
- Business continuity planning, and
- Audit.

Objective 7: If the institution provides IT services to other financial institutions, determine the quality of customer service and support.

1. If the TSP is not a bank, credit union, thrift, or holding company, analyze the TSP's financial condition and note any potential strengths and weaknesses.
2. Determine whether the service provider provides adequate customer access to financial information. Consider:
   - Method of communication with customer financial institutions,
   - Timeliness of reporting, and
   - Quality of financial information as determined by internal or external auditor reports.
3. Determine the adequacy of service provider audit reports in terms of scope, independence, expertise, frequency, and corrective actions taken on identified issues.
4. Determine the quality of customer service and support provided to customer institutions by:
   - Reviewing management reports used to monitor customer service or reported problems,
   - Reviewing complaint files and methods used to handle complaints,
   - Evaluating the extent of user group activity and minutes from meetings, and
   - Interviewing a sample of existing customers for satisfaction (if deemed appropriate).
5. Determine the quality of management's follow up and resolution of customer concerns and problems through analysis of the information above.

Objective 8: IF MIS is included in the scope of the review, complete the following procedures.

1. Review previous IT MIS review-related examination findings. Review management's response to those findings and:

- Discuss with examiners the usefulness and applicability of MIS systems that have been reviewed or are pending review,
- Request copies of any reports that discuss either MIS deficiencies or strengths, and
- Determine the significance of deficiencies and set priorities for follow-up investigations.
- Request and review copies of recent reports prepared by internal or external auditors of targeted IT MIS area(s) and determine:
- The significance of IT MIS problems disclosed,
- Recommendations provided for resolving IT MIS deficiencies,
- Management's responses and if corrective actions have been initiated and/or completed, and
- Audit follow-up activities.

2. Review reports for any MIS target area (i.e., business line selected for MIS review). Determine any material changes involving the usefulness of information and the five MIS elements of:

   - Timeliness,
   - Accuracy,
   - Consistency,
   - Completeness, and
   - Relevance.

Objective 9: Discuss corrective action and communicate findings.

1. Review preliminary conclusions with the EIC regarding:

   - Violations of laws, rulings, regulations,
   - Significant issues warranting inclusion as matters requiring attention or recommendations in the Report of Examination,
   - Proposed URSIT management component rating and the potential impact of your conclusion on other composite or component IT ratings, and
   - Potential impact of your conclusions on the institution's risk assessment.

2. Discuss findings with management and obtain proposed corrective action for significant deficiencies.

3. Document conclusions in a memo to the EIC that provides report ready comments for all relevant sections of the Report of Examination and guidance to future examiners.

4. Organize work papers to ensure clear support for significant findings by examination objective.

APPENDIX B: LAWS, REGULATIONS, AND GUIDANCE

EXTERNAL REFERENCES

- Basel Committee on Banking Supervision: Sound Practices for the Management and Supervision of Operational Risk (February 2003)
  http://www.bis.org/publ/bcbs91.htm
- IT Governance Institute: COBIT®; 3rd Edition; Management Guidelines (July 2000)
  http://www.itgi.org
- ISACA Control Objectives for Enterprise IT Governance
  http://www.isaca.org

LAWS

- 12 USC 1464(d): Home Owners' Loan Act
- 12 USC 1867(c): Bank Service Company Act
- 12 USC 1882: Bank Protection Act
- 15 USC 6801 and 6805(b): Gramm–Leach–Bliley Act
- 18 USC 1030: Fraud and Related Activity in Connection with Computers

FEDERAL RESERVE BOARD

REGULATIONS

- 12 CFR Part 208, Appendix D-2: Interagency Guidelines Establishing Standards for Safeguarding Customer Information
- 12 CFR Parts 211.9 and 211.24 (i): Protection of customer information
- 12 CFR Part 225, Appendix F: Interagency Guidelines Establishing Standards for Safeguarding Customer Information

GUIDANCE

- SR Letter 01-15: Standards for Safeguarding Customer Information (May 31, 2001)
- SR Letter 00-4: Outsourcing Information and Transaction Processing (February 29, 2000)
- SR Letter 98-9: Assessment of Information Technology in the Risk-Focused Frameworks for the Supervision of Community Banks and Large Complex Banking Organizations (April 20, 1998)

FEDERAL DEPOSIT INSURANCE CORPORATION

REGULATIONS

- 12 CFR Part 364, Appendix A: Interagency Guidelines Establishing Standards for Safety and Soundness
- 12 CFR Part 364, Appendix B: Interagency Guidelines Establishing Standards for Safeguarding Customer Information

GUIDANCE

- FIL-50-2001: Bank Technology Bulletin on Outsourcing (June 4, 2001)
- FIL-49-99: Required Notification for Compliance with the Bank Service Company Act (June 3, 1999)
- FIL-43-2003: Computer Software Patch Management (May 29, 2003)

NATIONAL CREDIT UNION ADMINISTRATION

REGULATIONS

- 12 CFR Part 721: Federal Credit Union Incidental Powers Activities
- 12 CFR Part 748: Security Program, Report of Crime and Catastrophic Act, Bank Secrecy Act Compliance, and Appendix A – Guidelines for Safeguarding Member Information
- 12 CFR Part 716: Privacy of Consumer Financial Information
- 12 CFR Part 741: Requirements for Insurance
- 12 CFR Part 740: Advertising

GUIDANCE

- NCUA Letter to Credit Unions 02–CU–17: E-Commerce Guide for Credit Unions (December 2002)
- NCUA Letter to Credit Unions 01–CU–20: Due Diligence Over Third–Party Service Providers (November 2001)

OFFICE OF THE COMPTROLLER OF THE CURRENCY

REGULATIONS

- 12 CFR Part 30, Appendix A: [Interagency] Guidelines Establishing Standards for Safety and Soundness
- 12 CFR Part 30, Appendix B: [Interagency] Guidelines Establishing Standards for Safeguarding Customer Information

GUIDANCE

- OCC Bulletin 2001–47: Third-Party Relationships (November 1, 2001)
- OCC Advisory Letter 2000-9: Third Party Risk (August 29, 2000)
- OCC Bulletin 98–3: Technology Risk Management (February 4, 1998)

OFFICE OF THRIFT SUPERVISION

REGULATIONS

- 12 CFR Part 570, Appendix A: Interagency Guidelines Establishing Standards for Safety and Soundness
- 12 CFR Part 570, Appendix B: Interagency Guidelines Establishing Standards for Safeguarding Customer Information

GUIDANCE

- Thrift Bulletin 82: Third Party Arrangements (March 19, 2003)
- Regulatory Bulletin 32-21: Technology Risk Controls (January 17, 2002)
- Thrift Activities Handbook Section 300, Management
- Thrift Activities Handbook Section 341, Technology Risk Controls