Federal Financial Institutions Examination Council

FFIEC

Audit AUD

April 2012

IT Examination Handbook

Table of Contents

Introduction

This "Audit Booklet" is one of several booklets that comprise the Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook (IT Handbook) and provides guidance to examiners and financial institutions on the characteristics of an effective information technology (IT) audit function. [1] This booklet replaces and rescinds Chapter 8 of the 1996 FFIEC Information Systems Examination Handbook. It should beused by examiners of the FFIEC member agencies [2] as a foundation from which they can assess the quality and effectiveness of an institution's IT audit program. It describes the roles and responsibilities of the board of directors, management, and internal or external auditors; identifies effective practices for IT audit programs; and details examination objectives and procedures. Agency examiners will use the examination procedures in Appendix A to assess the adequacy of IT audit programs at both financial institutions and technology service providers.The examination guidance and procedures in this booklet focus on IT audit and supplement other, more general, internal and external audit guidance provided by the FFIEC agencies. [3]

A well-planned, properly structured audit program is essential to evaluate risk management practices, internal control systems,and compliance with corporate policies concerning IT-related risks at institutions of every size and complexity. Effective audit programs are risk-focused, promote sound IT controls, ensure the timely resolution of audit deficiencies, and inform the board of directors of the effectiveness of risk management practices. An effective IT audit function may also reduce the time examiners spend reviewing areas of the institution during examinations. Ideally, the audit program would consist of a full-time, continuous program of internal audit coupled with a well-planned external auditing program.

The financial industry must plan, manage, and monitor rapidly changing technologies to enable it to deliver and support new products, services, and delivery channels. The rate of these changes and the resulting increased reliance on technology make the inclusion of IT audit coverage essential to an effective over all audit program. The audit program should address IT risk exposures throughout the institution, including the areas of IT management and strategic planning, data center operations, client/server architecture, local and wide-area networks, telecommunications, physical and information security, electronic banking, systems development, and business continuity planning. IT audit should also focus on how management determines the risk exposure from its operations and controls or mitigates that risk.

To determine what risks exist, management should prepare an independent assessment of the institution's risk exposure and the quality of the internal controls associated with the development, acquisition, implementation, and use of information technology. An institution's IT audit function can provide this independent assessment within the context of the overall audit function and can include work performed by both internal and external auditors and by other independent third parties as appropriate for the institution's complexity and level of internal expertise. The FFIEC member agencies believe that a strong internal auditing function combined with a well-planned external auditing function substantially increase the probability that an institution will detect potentially serious technology-related problems. An effective IT audit program should:

- Identify areas of greatest IT risk exposure to the institution in order to focus audit resources;
- Promote the confidentiality, integrity, and availability of information systems;
- Determine the effectiveness of management's planning and oversight of IT activities;
- Evaluate the adequacy of operating processes and internal controls;
- Determine the adequacy of enterprise-wide compliance efforts related to IT policies and internal control procedures; and
- Require appropriate corrective action to address deficient internal controls and follow up to ensure management promptly and effectively implements the required actions.

The examiner is responsible for evaluating the effectiveness of the IT audit function in meeting these objectives. The examiner should also consider the institution's ability to promptly detect and report significant risks to the board of directors and senior management. Examiners should take into account the institution's size, complexity, and overall risk profile when performing this and other evaluations. Examiners should consider the following issues when evaluating the IT audit function:

- Independence of the audit function and its reporting relationship to the board of directors or its audit committee;
- Expertise and size of the audit staff relative to the IT environment;
- Identification of the IT audit universe, risk assessment, scope, and frequency of IT audits;
- Processes in place to ensure timely tracking and resolution of reported weaknesses; and
- Documentation of IT audits, including work papers, audit reports, and follow-up.

IT Audit Roles and Responsibilities

Board of Directors and Senior Management

The board of directors and senior management are responsible for ensuring that the institution's system of internal controls operates effectively. One important element of an effective internal control system is an internal audit function that includes adequate IT coverage.

To meet its responsibility of providing an independent audit function with sufficient resources to ensure adequate IT coverage, the board of directors or its audit committee should:

- Provide an internal audit function capable of evaluating IT controls,
- Engage outside consultants or auditors to perform the internal audit function, or
- Use a combination of both methods to ensure that the institution has received adequate IT audit coverage.

An institution's board of directors may establish an "audit committee" to oversee audit functions and to report on audit matters periodically to the full board of directors. For purposes of this booklet, the term "audit committee" means the committee with audit oversight regardless of the type of financial institution. [4] Audit committee members should have a clear understanding of the importance and necessity of an independent audit function.

To comply with the Sarbanes-Oxley Act of 2002, [5] public stock-issuing institutions are required to appoint outside directors as audit committee members. All members of a stock-issuing institution's audit committee must be members of the board of directors and be independent (i.e., not otherwise compensated by, or affiliated with, the institution). Additionally, 12 CFR 363 (Federal Deposit Insurance Corporation Improvement Act, or FDICIA) requires all depository institutions with total assets greater than $500 million to have independent audit committees. Although not all institutions are subject to these requirements due to their corporate structure (Sarbanes-Oxley) or their size (FDICIA), it is generally considered good practice that they use them as guidelines to ensure the independence of their audit committees.

The board of directors should ensure that written guidelines for conducting IT audits have been adopted. The board of directors or its audit committee should assign responsibility for the internal audit function to a member of management (hereafter referred to as the "internal audit manager") who has sufficient audit expertise and is independent of the operations of the business.

The board should give careful thought to the placement of the audit function in relation to the institution's management structure. The board should have confidence that the internal audit staff members will perform their duties with impartiality and not be unduly influenced by senior management and managers of day-to-day operations. Accordingly, the internal audit manager should report directly to the board of directors or its audit committee.

The board or its audit committee is responsible for reviewing and approving audit strategies (including policies and programs), and monitoring the effectiveness of the audit function. The board or its audit committee should be aware of, and understand, significant risks and control issues associated with the institution's operations, including risks in new products, emerging technologies, information systems, and electronic banking. Control issues and risks associated with reliance on technology can include:

- Inappropriate user access to information systems,
- Unauthorized disclosure of confidential information,
- Unreliable or costly implementation of IT solutions,

- Inadequate alignment between IT systems and business objectives,
- Inadequate systems for monitoring information processing and transactions,
- Ineffective training programs for employees and system users,
- Insufficient due diligence in IT vendor selection,
- Inadequate segregation of duties,
- Incomplete or inadequate audit trails,
- Lack of standards and controls for end-user systems,
- Ineffective or inadequate business continuity plans, and
- Financial losses and loss of reputation related to systems outages.

The board or its audit committee members should seek training to fill any gaps in their knowledge related to IT risks and controls. The board of directors or its audit committee should periodically meet with both internal and external auditors to discuss audit work performed and conclusions reached on IT systems and controls.

Audit Management

The internal audit manager is responsible for implementing board-approved audit directives. The manager oversees the audit function and provides leadership and direction in communicating and monitoring audit policies, practices, programs, and processes. The internal audit manager should establish clear lines of authority and reporting responsibility for all levels of audit personnel and activities. The internal audit manager also should ensure that members of the audit staff possess the necessary independence, experience, education, training, and skills to properly conduct assigned activities.

The internal audit manager should be responsible for internal control risk assessments, audit plans, audit programs, and audit reports associated with IT. Audit management should oversee the staff assigned to perform the internal audit work, should establish policies and procedures to guide the audit staff, and should ensure the staff has the expertise and resources to identify inherent risks and assess the effectiveness of internal controls in the institution's IT operations.

Internal IT Audit Staff

The primary role of the internal IT audit staff is to assess independently and objectively the controls, reliability, and integrity of the institution's IT environment. These assessments can help maintain or improve the efficiency and effectiveness of the institution's IT risk management, internal controls, and corporate governance.

Internal auditors should evaluate IT plans, strategies, policies, and procedures to ensure

adequate management oversight. Additionally, they should assess the day-to-day IT controls to ensure that transactions are recorded and processed in compliance with acceptable accounting methods and standards and are in compliance with policies set forth by the board of directors and senior management. Auditors also perform operational audits, including system development audits, to ensure that internal controls are in place, that policies and procedures are effective, and that employees operate in compliance with approved policies. Auditors should identify weaknesses, review management's plans for addressing those weaknesses, monitor their resolution, and report to the board as necessary on material weaknesses.

Auditors should make recommendations to management about procedures that affect IT controls. In this regard, the board and management should involve the audit department in the development process for major new IT applications. The board and management should develop criteria for determining those projects that need audit involvement. Audit's role generally entails reviewing the control aspects of new applications, products, conversions, or services throughout their development and implementation. Early IT audit involvement can help ensure that proper controls are in place from inception. However, the auditors should be careful not to compromise, or even appear to compromise, their independence when involved in these projects.

Operating Management

Operating management should formally and effectively respond to IT audit or examination findings and recommendations. The audit procedures should clearly identify the methods for following up on noted audit or control exceptions or weaknesses. Operating management is responsible for correcting the root causes of the audit or control exceptions, not just treating the exceptions themselves. Response times for correcting noted deficiencies should be reasonable and may vary depending on the complexity of the corrective action and the risk of inaction. Auditors should document, report, and track recommendations and outstanding deficiencies. Additionally, auditors should conduct timely follow-up audits to verify the effectiveness of management's corrective actions for significant deficiencies.

External Auditors

External auditors typically review IT control procedures as part of their overall evaluation of internal controls when providing an opinion on the adequacy of an institution's financial statements. As a rule, external auditors review the general and application controls affecting the recording and safeguarding of assets and the integrity of controls over financial statement preparation and reporting. General controls include the plan of organization and operation, documentation procedures, access to equipment and data files, and other controls affecting overall information systems operations. Application controls relate to specific information systems tasks and provide reasonable assurance that the recording, processing, and reporting of data are properly performed.

External auditors may also review the IT control procedures as part of an outsourcing arrangement in which they are engaged to perform all or part of the duties of the internal audit staff. Such arrangements are discussed in more detail in the "Outsourcing Internal IT Audit" section of this booklet.

The extent of external audit work, including work related to information systems, should be clearly defined in an engagement letter. Such letters should discuss the scope of the audit, the objectives, resource requirements, audit timeframe, and resulting reports. Examiners will typically review the engagement letter, reports, and audit work papers to determine the extent to which they can rely on external audit coverage and reduce their examination scope accordingly.

Independence and Staffing of Internal IT Audit

Independence

The ability of the internal audit function to achieve desired objectives depends largely on the independence of audit personnel. Generally, the position of the auditor within the organizational structure of the institution, the reporting authority for audit results, and the auditor's responsibilities indicate the degree of auditor independence. The board should ensure that the audit department does not participate in activities that may compromise, or appear to compromise, its independence. These activities may include preparing reports or records, developing procedures, or performing other operational duties normally reviewed by auditors.

The auditor's independence is also determined by analyzing the reporting process and verifying that management does not interfere with the candor of the findings and recommendations. For an effective program, the board should give the auditor the authority to:

- Access all records and staff necessary to conduct the audit, and
- Require management to respond formally, and in a timely manner, to significant adverse audit findings by taking appropriate corrective action.

Internal auditors should discuss their findings and recommendations periodically with the audit committee or board of directors.

Ideally, the internal audit manager should report directly to the board of directors or its audit committee regarding both audit issues and administrative matters. [6] Alternatively, an institution may establish a dual reporting relationship where the internal audit manager reports to the audit committee or board for audit matters and to institution executive management for administrative matters. The objectivity and organizational stature of the internal audit function are best served under such a dual arrangement if the internal audit manager reports administratively to the chief executive office (CEO), and not to the chief financial officer (CFO) or a similar officer who has a direct responsibility for systems being audited. The board or its audit committee should determine the internal audit manager's performance evaluations and compensation.

The formality and extent of an institution's internal IT audit function depends on the institution's size, complexity, scope of activities, and risk profile. It is the responsibility of the audit committee and management to carefully consider the extent of auditing that will

effectively monitor the internal control system subject to consideration of the internal audit function's costs and benefits. For larger institutions or institutions with complex operations, the benefits derived from a full time manager of internal audit or an audit staff will likely outweigh the cost. For small institutions with few employees and/or simple operations, these costs may outweigh the benefits. Nevertheless, an institution without an internal auditor can ensure that it maintains an objective and independent internal function by implementing comprehensive internal reviews of significant internal controls. The key characteristic of such reviews is that the person(s) directing or performing the review is (are) not also responsible for managing or operating those controls.

Staffing

Personnel performing IT audits should have information systems knowledge commensurate with the scope and sophistication of the institution's IT environment and possess sufficient analytical skills to determine and report the root cause of deficiencies. If internal expertise is inadequate, the board should consider using qualified external sources such as management consultants, independent auditors, or other professionals to supplement or perform the institution's internal IT audit function. In some institutions, a person or group that has no other responsibilities outside the IT audit function performs IT audits. Generally, institutions using this approach centralize IT audit coverage and assign one or more IT audit specialists to perform end-user application control reviews as well as technical system audits. A centralized IT audit department can ensure sufficient technical expertise, but can also strain technical resources and require multiple audits in a user department. Additionally, IT auditors in this environment may need to have a greater understanding of financial and business line audit concerns.

Other institutions may use an integrated audit approach. Using this method, IT audit specialists perform the technology system and other technical reviews, while generalist auditors perform the end-user application control reviews. Institutions should use auditors with technical knowledge appropriate for the areas reviewed.

An institution's hiring and training practices should ensure that the institution has qualified IT auditors. The auditor's education and experience should be consistent with job responsibilities. Audit management should also provide an effective program of continuing education and development. As the information systems of an institution become more sophisticated or as more complex technologies evolve, the auditor may need additional training.

Internal Audit Program

Action Summary

Management should develop and follow a formal internal audit program consisting of policies and procedures that govern the internal audit function, including IT audit.

An institution's internal audit program consists of the policies and procedures that govern its internal audit functions, including risk-based auditing programs and outsourced internal audit work, if applicable. While smaller institutions' audit programs may not require the formality of those found in larger, more complex institutions, all audit programs should include

- A mission statement or audit charter outlining the purpose, objectives, organization, authorities, and responsibilities of the internal auditor, audit staff, audit management, and the audit committee.
- A risk assessment process to describe and analyze the risks inherent in a given line of business. Auditors should update the risk assessment at least annually, or more frequently if necessary, to reflect changes to internal control or work processes, and to incorporate new lines of business. The level of risk should be one of the most significant factors considered when determining the frequency of audits.
- An audit plan detailing internal audit's budgeting and planning processes. The plan should describe audit goals, schedules, staffing needs, and reporting. The audit plan should cover at least 12 months and should be defined by combining the results of the risk assessment and the resources required to yield the timing and frequency of planned internal audits. The audit committee should formally approve the audit plan annually, or review it annually in the case of multi-year audit plans. The internal auditors should report the status of planned versus actual audits, and any changes to the annual audit plan, to the audit committee for its approval on a periodic basis.
- An audit cycle that identifies the frequency of audits. Auditors usually determine the frequency by performing a risk assessment, as noted above, of areas to be audited. While staff and time availability may influence the audit cycle, they should not be overriding factors in reducing the frequency of audits for high-risk areas.
- Audit work programs that set out for each audit area the required scope and resources, including the selection of audit procedures, the extent of testing, and the basis for conclusions. Well-planned, properly structured audit programs are essential to strong risk management and to the development of comprehensive internal control systems.
- Written audit reports informing the board and management of individual department or division compliance with policies and procedures. These reports should state whether operating processes and internal controls are effective, and describe deficiencies as well as suggested corrective actions. The audit manager should consider implementing an audit rating system (for example, satisfactory, needs improvement, unsatisfactory) approved by the audit committee. The rating system facilitates conveying to the board a consistent and concise assessment of the net risk posed by the area or function audited. All written audit reports should reflect the assigned rating for the areas audited.
- Requirements for audit work paper documentation to ensure clear support for all audit findings and work performed, including work paper retention policies.
- Follow-up processes that require internal auditors to determine the disposition of any agreed-upon actions to correct significant deficiencies.

- Professional development programs to be in place for the institution's audit staff to maintain the necessary technical expertise.

All institutions are encouraged to implement risk-based IT audit procedures based on a formal risk assessment methodology to determine the appropriate frequency and extent of work. See the "Risk Assessment and Risk-Based Auditing" section of this booklet for more detail.

IT audit procedures will vary depending upon the philosophy and technical expertise of the audit department and the sophistication of the data center and end-user systems. However, to achieve effective coverage, the audit program and expertise of the staff must be consistent with the complexity of data processing activities reviewed. The audit procedures may include manual testing processes or computer-assisted audit programs (discussed later in this section).

The audit department should establish standards for audit work papers, related communications, and retention policies. Auditors should ensure that work papers are well organized, clearly written, and address all areas in the scope of the audit. They should contain sufficient evidence of the tasks performed and support the conclusions reached. Formal procedures should exist to ensure that management and the audit committee receive summarized audit findings that effectively communicate the results of the audit. Full audit reports should be available for review by the audit committee. Policies should establish appropriate work paper retention periods. Institutions should consider conducting their internal audit activities in accordance with professional standards, such as the Standards for the Professional Practice of Internal Auditing issued by the Institute for Internal Auditors (IIA), and those issued by the Standards Board of the Information Systems Audit and Control Association (ISACA). These standards address independence, professional proficiency, scope of work, performance of audit work, management of internal audit, and quality assurance reviews.

IT auditors frequently use computer-assisted audit techniques (CAATs) to improve audit coverage by reducing the cost of testing and sampling procedures that otherwise would be performed manually. CAATs include many types of tools and techniques, such as generalized audit software, utility software, test data, application software tracing and mapping, and audit expert systems. CAATs may be:

- Developed by internal programming staff or by outside programmers with audit department supervision;
- Purchased generalized audit software, e.g., audit packages offered by CPA firms or software vendors;
- Developed by IT auditors; or
- Acquired from equipment manufacturers and software houses to analyze machine, programmer, and operations efficiency.

Whatever the source, audit software programs should remain under the strict control of the audit department. For this reason, all documentation, test material, source listings,

source and object program modules, and all changes to such programs, should be strictly controlled. In installations using advanced software library control systems, audit object programs may be catalogued with password protection. This is acceptable if the auditors retain control over the documentation and the appropriate job control instructions necessary to retrieve and execute the object program from the libraries where it is stored. If internal control procedures within the computer system do not allow for strict audit control, audit programs should not be catalogued. Computer programs intended for audit use should be documented carefully to define their purpose and to ensure their continued usefulness and reliability.

CAATs may be used in performing various audit procedures, including the following:

- Tests of transactions and balances, such as recalculating interest;
- Analytical review procedures, such as identifying inconsistencies or significant fluctuations;
- Compliance tests of general controls, such as testing the set-up or configuration of the operating system or access procedures to the program libraries;
- Sampling programs to extract data for audit testing;
- Compliance tests of application controls such as testing the functioning of a programmed control;
- Recalculating entries performed by the entity's accounting systems; and
- Penetration testing.

These tools and techniques can also be used effectively to check data integrity by testing the logical processing of data "through" the system, rather than by relying only on validations of input and output controls.

Risk Assessment and Risk-Based Auditing

Action Summary

The board of directors should establish an effective risk-based audit function.

An effective risk-based auditing program will cover all of an institution's major activities. The frequency and depth of each area's audit will vary according to the risk assessment of that area. Examiners should determine whether the audit function is appropriate for the size and complexity of the institution.

Program Elements

Properly designed risk-based audit programs increase audit efficiency and effectiveness. The sophistication and formality of risk-based audits may vary depending on the institution's size and complexity. To determine the appropriate level of audit coverage for the organization's IT environment, management should define an effective risk assessment methodology. This assessment methodology should provide the auditor and the board with objective information to prioritize the allocation of audit resources properly. Risk-based IT audit programs should:

- Identify the institution's data, application and operating systems, technology, facilities, and personnel;
- Identify the business activities and processes within each of those categories;
- Include profiles of significant business units, departments, and product lines, or systems, and their associated business risks and control features, resulting in a document describing the structure of risk and controls throughout the institution;
- Use a measurement or scoring system that ranks and evaluates business and control risks for significant business units, departments, and products;
- Include board or audit committee approval of risk assessments and annual risk-based audit plans that establish audit schedules, audit cycles, work program scope, and resource allocation for each area audited;
- Implement the audit plan through planning, execution, reporting, and follow-up; and
- Include a process that regularly monitors the risk assessment and updates it at least annually for all significant business units, departments, and products or systems.

Risk Scoring System

A successful risk-based IT audit program can be based on an effective scoring system. [7] In establishing a scoring system, the board of directors and management should ensure the system is understandable, considers all relevant risk factors, and, to the extent possible, avoids subjectivity. Major risk factors commonly used in scoring systems include the following:

- The adequacy of internal controls;
- The nature of transactions (for example, the number and dollar volumes and the complexity);
- The age of the system or application;
- The nature of the operating environment (for example, changes in volume, degree of system and reporting centralization, sensitivity of resident or processed data, the

impact on critical business processes, potential financial impact, planned conversions, and economic and regulatory environment);

- The physical and logical security of information, equipment, and premises;
- The adequacy of operating management oversight and monitoring;
- Previous regulatory and audit results and management's responsiveness in addressing issues;
- Human resources, including the experience of management and staff, turnover, technical competence, management's succession plan, and the degree of delegation; and
- Senior management oversight.

Auditors should develop written guidelines on the use of risk assessment tools and risk factors and review these guidelines with the audit committee or the board of directors. The sophistication and formality of guidelines will vary for individual institutions depending on their size, complexity, scope of activities, geographic diversity, and various technologies used. The institution can rely on standard industry practice or on its own experiences to define risk scoring. Auditors should use the guidelines to grade or assess major risk areas and to define the range of scores or assessments (e.g., groupings such as low, medium, and high risk or a numerical sequence such as 1 through 5).

The written risk assessment guidelines should specify the following elements:

- A maximum length for audit cycles based on the risk scores. (For example, some institutions set audit cycles at 12 months or less for high-risk areas, 24 months or less for medium-risk areas, and up to 36 months for low-risk areas. Audit cycles should not be open-ended.);
- The timing of risk assessments for each department or activity. (Normally risks are assessed annually, but more frequent assessments may be needed if the institution experiences rapid growth or significant change in operation or activities.);
- Documentation requirements to support scoring decisions; and
- Guidelines for overriding risk assessments in special cases and the circumstances under which they can be overridden. (For example, the guidelines should define who can override assessments, and how the override is approved, reported and documented.)

Numerous industry groups offer resources where institutions can obtain matrices, models, or additional information on risk assessments. Among these groups are: ISACA, American Bankers Association (ABA), American Institute of Certified Public Accountants (AICPA), and IIA. Day-to-day management of the risk-based audit program rests with the internal audit manager, who monitors the audit scope and risk assessments to ensure that audit coverage remains adequate. The internal audit manager also prepares reports showing the risk rating, planned scope, and audit cycle for each area. The audit manager

should confirm the risk assessment system's reliability at least annually or whenever significant changes occur within a department or function. Operating department managers and auditors should work together in evaluating the risk in all departments and functions by reviewing risk assessments to determine their reasonableness.

Auditors should periodically review the results of internal control processes and analyze financial or operational data for any impact on a risk assessment or scoring. Accordingly, operating management should be required to keep auditors up to date on all major changes in departments or functions, such as the introduction of a new product, implementation of a new system, application conversions, or significant changes in organization or staff.

Audit Participation in Application Development, Acquisition, Conversions, and Testing

Action Summary

Senior management should involve IT audit in major application development, acquisition, conversion, and testing.

The development, acquisition, or conversion of an automated application is a lengthy and complex process requiring a significant degree of interaction among the programming staff, user departments, and internal audit. This process, known as the system development life cycle or system development methodology, requires detailed developmental stages to ensure that applications meet the needs of the institution. As each stage of the life cycle is reached, the auditor should review the internal controls, testing, and audit trails included in the application. The incorporation of internal controls within a completed application already in production is usually more difficult and expensive. Guidelines should be developed to facilitate the review of new applications during the design phase so that controls can be identified during independent audit review early in the development process.

The institution's audit policy, as approved by the board of directors, should include guidelines detailing what involvement internal audit will have in the development, acquisition, conversion, and testing of major applications. This includes describing the monitoring, reporting, and escalation processes (when internal controls are found to be insufficient or when testing is found to be inadequate). For acquisitions, this includes describing the phases of the system development life cycle in which IT audit will be involved. For acquisitions with significant IT impacts, participation of IT audit may be necessary early in the due diligence stage.

It is necessary that audit's participation in the development process be independent and objective. Auditors can determine and should recommend appropriate controls to project management. However, such recommendations do not necessarily "pre-approve" the controls, but instead guide the developers in considering appropriate control standards and structures throughout their project. The auditors are more than just "consultants" on internal controls. While they should not have any direct involvement in management decisions, they should raise objections if they believe the control environment to be

inadequate.

Once a new application system, conversion, or major revision to an existing system is accepted for production processing, the IT auditor should conduct a post-implementation review. This review should occur shortly after the implementation of the new or revised system and should include extensive testing of program logic, calculations, error conditions, edits, and controls. Such testing helps to validate that the software operates as expected. By performing the review soon after migration to the production environment, the auditors can quickly identify processing errors or other unsatisfactory conditions. A prompt post-implementation review should minimize potential losses from processing errors or ineffective software operation or controls and loss of reputation caused by inaccurate information provided to customers.

In larger IT facilities, formal quality assurance or change management groups may have primary responsibility for post-implementation reviews. In such cases, the IT auditor may choose not to perform a separate review but instead to participate in establishing the test criteria and evaluating results of any other independent reviews.

Outsourcing Internal IT Audit

Action Summary

The board of directors of an institution that outsources its internal IT audit function should ensure that the structure, scope, and management of the outsourcing arrangement provides for an adequate evaluation of the system of internal controls.

In addressing quality and resource issues, many institutions engage independent public accounting firms and other outside professionals to perform work that has been traditionally carried out by internal auditors. These arrangements are often called "internal audit outsourcing," "internal audit assistance," "audit co-sourcing," or "extended audit services."

Outsourcing such audit services may be beneficial to an institution if it is properly structured, carefully conducted, and prudently managed. To do this, management should ensure that there are no conflicts of interest and that the use of these services does not compromise independence. Potential conflicts of interest may arise if the outsourced auditing firm performs IT audit functions in addition to other audit services, such as providing the independent financial statement, or serving in an IT or management consulting capacity. The board of directors of an institution remains responsible for ensuring that the outsourced internal audit function operates effectively and complies with all regulations governing such arrangements.

Examiners should assess whether the structure, scope, and management of an internal audit outsourcing arrangement adequately evaluate the institution's system of internal controls. They should also determine whether or not directors and senior managers have fulfilled their responsibilities for maintaining an effective system of internal controls and for overseeing the internal audit function in an outsourced internal audit environment.

Additional detailed guidance on the structure, independence, and sound practices

concerning the use of outsourcing audit providers is available in the "Interagency Policy Statement on the Internal Audit Function and Its Outsourcing."

Independence of the External Auditor Providing Internal Audit Services

It is important that examiners ensure that management has designed any outsourcing arrangements in order to maintain the independence of the audit provider. An accounting firm hired to perform internal audit services for an institution risks compromising its independence when it also performs the external audit for the institution. Concerns arise because, rather than having an independent review, the responsibility of performing outsourced internal audits places the accounting firm in the position of auditing its own work. For example, in designing procedures to audit an institution's financial statements, the accounting firm considers the extent to which it may rely on the institution's internal control system, including the internal audit function.

The Sarbanes-Oxley Act of 2002 specifically prohibits a registered public accounting firm from performing certain non-audit services for a public company client for whom it performs financial statement audits. Among those prohibited non-audit services are internal audit outsourcing services and financial information system design and implementation. Under rules adopted by the Securities and Exchange Commission, this prohibition generally became effective on May 6, 2003, although a one-year transition period was provided for contractual arrangements in place as of that date. Under Section 36 of the Federal Deposit Insurance Act and its implementing regulation and guidelines, FDIC-insured depository institutions with total assets of $500 million or more are required to be audited annually. The guidelines require these institutions, whether or not they are public companies, and their external auditors to comply with the SEC's auditor independence requirements. Other non-public institutions are encouraged to have their financial statements audited and to follow the Sarbanes-Oxley Act's prohibition on outsourcing internal audit to their external auditor. However, there are circumstances in which these institutions can use the same accounting firm for both external and internal audit work.

Examples of Arrangements

An outsourcing arrangement is a contract between the institution and an audit services firm to provide internal audit services. Outsourcing arrangements take many forms and are used by institutions of all sizes. The services under contract can be as limited as assisting internal audit staff with an assignment in which they lack expertise. This type of arrangement would typically fall under the control of the institution's internal audit manager, to whom the audit provider would typically report.

Other outsourcing arrangements may call for an audit provider to perform all or several parts of the internal audit work. Under these types of arrangements, the institution should maintain an internal audit manager and, as appropriate, internal audit staff sufficient to oversee vendor activities. The audit provider usually assists the internal audit function in determining the institution's areas of risk and the levels of risk to be reviewed, and recommends and performs audit procedures approved by the institution's internal audit manager. In addition, the outsourced audit provider should work jointly with the internal audit manager in reporting significant findings to the board or its audit committee.

Before entering into an outsourcing arrangement, the institution should perform due diligence to ensure that the audit provider has a sufficient number of qualified staff members to perform the contracted work. Because the outsourcing arrangement is a professional or personnel services contract, the institution's internal audit manager should have confidence in the competence of the staff assigned by the audit provider and receive timely notice from the vendor of any key staffing changes. Throughout the outsourcing arrangement, management should ensure that the audit provider maintains sufficient expertise to perform effectively and fulfill its contractual obligations.

When an institution enters into an outsourcing arrangement, or significantly changes the mix of internal and external resources used by internal audit, operational risk may increase. Because the arrangement could be terminated suddenly, the institution should have a contingency plan to mitigate any significant gap in audit coverage, particularly for high-risk areas. In its planning, an institution should consider possible alternatives and determine what it will do if an auditor with specialized knowledge or skills is unable to complete reviews of high risk areas, or if an outsourcing arrangement is terminated. For example, management could maintain information about the services offered and areas of expertise, as well as contact names and phone numbers, of other firms in their geographic area that could provide internal audit assistance in specific areas or a broader range of outsourcing services.

When negotiating the outsourcing arrangement with a vendor, an institution should carefully consider its current and anticipated business risks in setting each party's internal audit responsibilities. To clearly define the institution's duties and those of the outsourcing vendor, the institution should have a written contract, often referred to as an engagement letter. [8] The contract should:

- Define the expectations and responsibilities for both parties;
- Set the scope, frequency, and cost of work to be performed by the vendor;
- Set responsibilities for providing and receiving information, such as the manner and frequency of reporting to senior management and the board about the status of contract work;
- Establish the protocol for changing the terms of the service contract, especially for expansion of audit work if significant issues are found, and stipulations for default and termination of the contract;
- State that any information pertaining to the institution must be kept confidential;
- Specify the locations of internal audit reports and the related work papers;
- Specify the period of time that vendors must maintain the work papers; [9]
- State that outsourced internal audit services provided by the vendor are subject to regulatory review and that examiners will be granted full and timely access to the internal audit reports and related work papers prepared by the outsourcing vendor; [10]
- State that internal audit reports are the property of the institution, that the institution will be provided with any copies of the related work papers it deems necessary, and that employees authorized by the institution will have reasonable and timely access

to the work papers prepared by the audit provider;

- Prescribe a process (arbitration, mediation, or other means) for resolving problems and for determining who bears the cost of consequential damages arising from errors, omissions, and negligence; and
- State that audit providers will not perform management functions, make management decisions, or act or appear to act in a capacity equivalent to that of an employee or a member of management of the institution, and will comply with professional and regulatory independence guidance.

Directors and senior management should ensure that the outsourced internal audit function is competently managed. For example, larger institutions should employ sufficient competent staff members in the internal audit department to assist the internal audit manager in overseeing the outsourcing vendor. Smaller institutions that do not employ a full-time audit manager should appoint a competent institution employee to oversee the outsourcing vendor's performance under the contract. This person should report directly to the audit committee for purposes of communicating audit issues and ideally should have no managerial responsibility for the area being audited.

Communication among the internal audit function, the audit committee, and senior management should not diminish because the institution engages an outsourcing vendor. The institution's audit manager should be involved with the audit provider in defining the audit universe and setting a risk-based IT audit schedule. The audit provider should appropriately document all work and promptly report all control weaknesses found during the audit to the institution's internal audit manager.

The outsourcing vendor should work with the internal audit manager to mutually determine what audit findings are significant and should be emphasized when reported to the board and its audit committee. The concept of materiality as the term is used in financial statement audits is not necessarily a good indicator of which control weaknesses to report. For example, reportable weaknesses could affect the institution's reputation or compliance with laws and regulations without a direct impact on the financial statements.

Third-Party Reviews of Technology Service Providers

A technology service provider (TSP) that processes work for financial institutions often is subject to separate audits by internal auditors from each of the serviced institutions. These audits may duplicate each other, creating a hardship on the provider's management and resources. The TSP can reduce that burden by arranging for its own third-party audit to determine the status and reliability of internal controls and by sharing the results of that audit with its client financial institutions.

A third-party audit or review is performed by independent auditors who are not employees of either the TSP or the serviced institution(s). The TSP, its auditors, or its serviced institutions may engage the third-party auditor. The serviced institutions' auditors may use this third-party review to determine the scope of any additional audit coverage they require to evaluate the system and controls at the TSP. Examiners can

also use the third-party review to help scope their supervisory activities.

Financial institutions are required to effectively manage their relationships with key TSPs. Institution management meets this requirement related to audit controls by:

- Directly auditing the TSP's operations and controls
- Employing the services of external auditors to evaluate the TSP's operations and controls; or
- Receiving from, and reviewing sufficiently detailed independent audit reports on, the TSP.

Financial institutions using such audits to complement their own coverage should ensure that the independent auditor is qualified to perform the review, that the scope satisfies their own audit objectives, and that any significant deficiencies reported are corrected. It is critically important that the examiner and the institution understand the nature and scope of the engagement and the level of assurance accruing from the work product of the reviewing firm.

There are two common types of independent third-party reviews: attestation reviews and non-attestation reviews. Attestation reviews [11] are generally conducted by Certified Public Accountants (CPAs) and are based upon Attestation Standards issued by the American Institute of Certified Public Accounts (AICPA). Non-attestation reviews include those performed by IT consultants or others; they may be based upon external standards [12] or industry developed criteria. [13]

The type of independent third-party review chosen should be based upon the size and complexity of the servicer, the products and services it offers, and its risk profile because the level of assurance provided varies with each type of review.

Users of audit reports or reviews should not rely solely on the information contained in the report to verify the internal control environment of the TSP. They should use additional verification and monitoring procedures as discussed more fully in the Outsourcing Technology Services Booklet of the FFIEC IT Examination Handbook. Refer to that booklet for additional information on vendor management and to supplement the examination coverage in this booklet.

Endnotes

[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 of Governors of the Federal Reserve System (Federal Reserve Board), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), and Office of Thrift Supervision (OTS).
[3]	These include the "Interagency Policy Statement on the Internal Audit Function and Its Outsourcing," March 17, 2003; "Interagency Policy Statement on External Auditing Programs of Banks and Savings Associations," September 22, 1999; and "Interagency Policy Statement on Coordination and Communication Between External Auditors and Examiners," July 23, 1992.
[4]	A federal credit union board of directors is required to establish a "supervisory committee" with oversight responsibility for audit. A supervisory committee consists of not less than three members, nor more than five members, one of whom may be a director other than the compensated officer of the board.
[5]	Sarbanes-Oxley Act of 2002 (Public Law 107-204) puts into place significant new requirements that provide for auditor independence of registered companies that will apply, through FDIC guidelines, (1) to any financial institution that is required under banking laws to have an annual independent audit or (2) to its holding company if the bank satisfies this requirement at the holding company level. All insured depository institutions with $500 million or more in total assets are required under banking laws to have an annual audit by an independent public accountant. If the institution is a subsidiary of a holding company, it can satisfy this requirement by an independent audit of the holding company. Further, the Federal Reserve Board may apply the auditor independence requirements in the Act to all bank holding companies that are required by the Federal Reserve Board to have an annual audit by an independent public accountant even if no subsidiary institution is subject to the requirements.
[6]	Administrative matters in this context include routine personnel matters such as leave and attendance reporting, expense account management, and other departmental matters such as furniture, equipment and supplies.
[7]	Scoring refers to any consistent means of quantifying and then comparing distinct items based on elements that they have in common. All risk-based systems require some means to rank greater or lesser risk, or risk factors. Consequently, many risk-based systems rely on some means of scoring in their implementation.
[8]	In general, the contract between the institution and the audit provider may or may not be the same as the engagement letter.
[9]	If work papers are in electronic format, contracts often call for the vendor to maintain the software that allows the institution and examiners access to electronic work papers during a specified period of time.

[10]	FDICIA Section 112 (12 USC Section 1831m(g)(3)) provides that all auditors are required to make their work papers available to bank examiners. 12 CFR 715.9(c) requires credit unions to obtain a signed audit engagement letter that includes a certification of unconditional access to the complete set of original working papers by credit union examiners.
[11]	For example, AICPA's SSAE-16 Type I and Type II, SOC 2 Type I and Type II, SOC 3 (Web Trust). See http://www.aicpa.org/_catalogs/masterpage/Search.aspx?S=soc+1
[12]	ISACA, NIST, IAA, & etc.
[13]	Shared Assessments Program; see http://www.sharedassessments.org/

Appendix A: Examination Procedures

Examination objectives allow the examiner to determine the quality and effectiveness of the audit function related to IT controls. These procedures will disclose the adequacy of audit coverage and to what extent, if any, the examiner may rely upon the procedures performed by the auditors in determining the scope of the IT examination.

- Tier I objectives and procedures relate to the institution's implementation of an effective audit function that may be relied upon to identify and manage risks.
- Tier II objectives and procedures provide additional validation as warranted by risk to verify the effectiveness of the institution's audit function. Tier II questions correspond to the Uniform Rating System for Information Technology (URSIT) rating areas and can be used to determine where the examiner may rely upon audit work in determining the scope of the IT examination for those areas.

TIER I OBJECTIVES AND PROCEDURES

Objective 1: Determine the scope and objectives of the examination of the IT audit function and coordinate with examiners reviewing other programs.

1. Review past reports for outstanding issues, previous problems, or high-risk areas with insufficient coverage related to IT. Consider:

- Regulatory reports of examination;
- Internal and external audit reports, including correspondence/communication between the institution and auditors;
- Regulatory, audit, and security reports from key service providers;
- Audit information and summary packages submitted to the board or its audit committee;
- Audit plans and scopes, including any external audit or internal audit outsourcing engagement letters; and
- Institution's overall risk assessment.

2. Review the most recent IT internal and external audit reports in order to determine:

- Management's role in IT audit activities;

- Any significant changes in business strategy, activities, or technology that could affect the audit function;
- Any material changes in the audit program, scope, schedule, or staffing related to internal and external audit activities; and
- Any other internal or external factors that could affect the audit function.

3. Review management's response to issues raised since the last examination. Consider:

- Adequacy and timing of corrective action;
- Resolution of root causes rather than just specific issues; and
- Existence of any outstanding issues.

4. Assess the quality of the IT audit function. Consider:

- Audit staff and IT qualifications, and
- IT audit policies, procedures, and processes.

Using the results from the preceding procedures and discussions with the EIC, select from the following examination procedures those necessary to meet the examination objectives. Note: examinations do not necessarily require all steps.

Objective 2: Determine the quality of the oversight and support of the IT audit function provided by the board of directors and senior management.

1. Review board resolutions and audit charter to determine the authority and mission of the IT audit function.

2. Review and summarize the minutes of the board or audit committee for member attendance and supervision of IT audit activities.

3. Determine if the board reviews and approves IT policies, procedures, and processes.

4. Determine if the board approves audit plans and schedules, reviews actual performance of plans and schedules, and approves major deviations to the plan.

5. Determine if the content and timeliness of audit reports and issues presented to and reviewed by the board of directors or audit committee are appropriate.

6. Determine whether the internal audit manager and the external auditor report directly to the board or to an appropriate audit committee and, if warranted, has the opportunity to escalate issues to the board both through the normal audit committee process and through the more direct communication with outside directors.

Objective 3: Determine the credentials of the board of directors or its audit committee related to their ability to oversee the IT audit function.

1. Review credentials of board members related to abilities to provide adequate oversight. Examiners should:

- Determine if directors responsible for audit oversight have appropriate level of experience and knowledge of IT and related risks; and
- If directors are not qualified in relation to IT risks, determine if they bring in outside independent consultants to support their oversight efforts through education and training.

2. Determine if the composition of the audit committee is appropriate considering entity type and complies with all applicable laws and regulations. Note - If the institution is a publicly traded company, this is a requirement of Sarbanes-Oxley. Additionally, this is a requirement of FDICIA for institutions with total assets greater than $500 million.

Objective 4: Determine the qualifications of the IT audit staff and its continued development through training and continuing education.

1. Determine if the IT audit staff is adequate in number and is technically competent to accomplish its mission. Consider:

- IT audit personnel qualifications and compare them to the job descriptions;
- Whether staff competency is commensurate with the technology in use at the institution; and
- Trends in IT audit staffing to identify any negative trends in the adequacy of staffing.

Objective 5: Determine the level of audit independence.

1. Determine if the reporting process for the IT audit is independent in fact and in appearance by reviewing the degree of control persons outside of the audit function have on what is reported to the board or audit committee.

2. Review the internal audit organization structure for independence and clarity of the reporting process. Determine whether independence is compromised by:

- The internal audit manager reporting functionally to a senior management official (i.e., CFO, controller, or similar officer);
- The internal audit manager's compensation and performance appraisal being done by someone other than the board or audit committee; or
- Auditors responsible for operating a system of internal controls or actually performing operational duties or activities.

  Note that it is recommended that the internal audit manager report directly to the audit committee functionally on audit issues and may also report to senior management for administrative matters.

Objective 6: Determine the existence of timely and formal follow-up and reporting on management's resolution of identified IT problems or weaknesses.

1. Determine whether management takes appropriate and timely action on IT audit findings and recommendations and whether audit or management reports the action to the board of directors or its audit committee. Also, determine if IT audit reviews or tests management's statements regarding the resolution of findings and recommendations.

2. Obtain a list of outstanding IT audit items and compare the list with audit reports to ascertain completeness.

3. Determine whether management sufficiently corrects the root causes of all significant deficiencies noted in the audit reports and, if not, determine why corrective action is not sufficient.

Objective 7: Determine the adequacy of the overall audit plan in providing appropriate coverage of IT risks.

1. Interview management and review examination information to identify changes to the institution's risk profile that would affect the scope of the audit function. Consider:

- Institution's risk assessment,

- Products or services delivered to either internal or external users,
- Loss or addition of key personnel, and
- Technology service providers and software vendor listings.

2. Review the institution's IT audit standards manual and/or IT-related sections of the institution's general audit manual. Assess the adequacy of policies, practices, and procedures covering the format and content of reports, distribution of reports, resolution of audit findings, format and contents of work papers, and security over audit materials.

Objective 8: Determine the adequacy of audit's risk analysis methodology in prioritizing the allocation of audit resources and formulating the IT audit schedule.

1. Evaluate audit planning and scheduling criteria, including risk analysis, for selection, scope, and frequency of audits. Determine if:

- The audit universe is well defined; and
- Audit schedules and audit cycles support the entire audit universe, are reasonable, and are being met.

2. Determine whether the institution has appropriate standards and processes for risk-based auditing and internal risk assessments that:

- Include risk profiles identifying and defining the risk and control factors to assess and the risk management and control structures for each IT product, service, or function; and
- Describe the process for assessing and documenting risk and control factors and its application in the formulation of audit plans, resource allocations, audit scopes, and audit cycle frequency

Objective 9: Determine the adequacy of the scope, frequency, accuracy, and timeliness of IT-related audit reports.

1. Review a sample of the institution's IT-related audit reports and work papers for specific audit ratings, completeness, and compliance with board and audit committee-approved standards.

2. Analyze the internal auditor's evaluation of IT controls and compare it with any evaluations done by examiners.

3. Evaluate the scope of the auditor's work as it relates to the institution's size, the nature and extent of its activities, and the institution's risk profile.

4. Determine if the work papers disclose that specific program steps, calculations, or other evidence support the procedures and conclusions set forth in the reports.

5. Determine through review of the audit reports and work papers if the auditors accurately identify and consistently report weaknesses and risks.

6. Determine if audit report content is:

- Timely
- Constructive
- Accurate
- Complete

Objective 10: Determine the extent of audit's participation in application development, acquisition, and testing, as part of the organization's process to ensure the effectiveness of internal controls.

1. Discuss with audit management and review audit policies related to audit participation in application development, acquisition, and testing.

2. Review the methodology management employs to notify the IT auditor of proposed new applications, major changes to existing applications, modifications/additions to the operating system, and other changes to the data processing environment.

3. Determine the adequacy and independence of audit in:

- Participating in the systems development life cycle;

- Reviewing major changes to applications or the operating system;
- Updating audit procedures, software, and documentation for changes in the systems or environment; and
- Recommending changes to new proposals or to existing applications and systems to address audit and control issues.

Objective 11: If the IT internal audit function, or any portion of it, is outsourced to external vendors, determine its effectiveness and whether the institution can appropriately rely on it.

1. Obtain copies of:

- Outsourcing contracts and engagement letters,
- Outsourced internal audit reports, and
- Policies on outsourced audit.

2. Review the outsourcing contracts/engagement letters and policies to determine whether they adequately:

- Define the expectations and responsibilities under the contract for both parties.
- Set the scope, frequency, and cost of work to be performed by the vendor.
- Set responsibilities for providing and receiving information, such as the manner and frequency of reporting to senior management and directors about the status of contract work.
- Establish the protocol for changing the terms of the service contract, especially for expansion of audit work if significant issues are found, and stipulations for default and termination of the contract.
- State that internal audit reports are the property of the institution, that the institution will be provided with any copies of the related work papers it deems necessary, and that employees authorized by the institution will have reasonable and timely access to the work papers prepared by the outsourcing vendor.
- State that any information pertaining to the institution must be kept confidential.
- Specify the locations of internal audit reports and the related work papers.
- Specify the period of time that vendors must maintain the work papers. If work papers are in electronic format, contracts often call for vendors to maintain

proprietary software that allows the institution and examiners access to electronic work papers during a specified period.

- State that outsourced internal audit services provided by the vendor are subject to regulatory review and that examiners will be granted full and timely access to the internal audit reports and related work papers and other materials prepared by the outsourcing vendor.
- Prescribe a process (arbitration, mediation, or other means) for resolving problems and for determining who bears the cost of consequential damages arising from errors, omissions and negligence.
- State that outsourcing vendors will not perform management functions, make management decisions, or act or appear to act in a capacity equivalent to that of a member of institution management or an employee and, if applicable, they are subject to professional or regulatory independence guidance.

3. Consider arranging a meeting with the IT audit vendor to discuss the vendor's outsourcing internal audit program and determine the auditor's qualifications.

4. Determine whether the outsourcing arrangement maintains or improves the quality of the internal audit function and the institution's internal controls. The examiner should:

- Review the performance and contractual criteria for the audit vendor and any internal evaluations of the audit vendor;
- Review outsourced internal audit reports and a sample of audit work papers. Determine whether they are adequate and prepared in accordance with the audit program and the outsourcing agreement;
- Determine whether work papers disclose that specific program steps, calculations, or other evidence support the procedures and conclusions set forth in the outsourced reports; and
- Determine whether the scope of the outsourced internal audit procedures is adequate.

5. Determine whether key employees of the institution and the audit vendor clearly understand the lines of communication and how any internal control problems or other matters noted by the audit vendor during internal audits are to be addressed.

6. Determine whether management or the audit vendor revises the scope of outsourced audit work appropriately when the institution's environment, activities, risk exposures, or systems change significantly.

7. Determine whether the directors ensure that the institution effectively manages any outsourced internal audit function.

8. Determine whether the directors perform sufficient due diligence to satisfy themselves of the audit vendor's competence and objectivity before entering the outsourcing arrangement.

9. If the audit vendor also performs the institution's external audit or other consulting services, determine whether the institution and the vendor have discussed, determined, and documented that applicable statutory and regulatory independence standards are being met. Note - If the institution is a publicly traded company, this is a requirement of Sarbanes-Oxley. Additionally, this is a requirement of FDICIA for institutions with total assets greater than $500 million.

10. Determine whether an adequate contingency plan exists to reduce any lapse in audit coverage, particularly coverage of high-risk areas, in the event the outsourced audit relationship is terminated suddenly.

Objective 12: Determine the extent of external audit work related to IT controls.

1. Review engagement letters and discuss with senior management the external auditor's involvement in assessing IT controls.

2. If examiners rely on external audit work to limit examination procedures, they should ensure audit work is adequate through discussions with external auditors and reviewing work papers if necessary.

Objective 13: Determine whether management effectively oversees and monitors any significant data processing services provided by technology service providers:

1. Determine whether management directly audits the service provider's operations and controls, employs the services of external auditors to evaluate the servicer's controls, or receives sufficiently detailed copies of audit reports from the technology service provider.

2. Determine whether management requests applicable regulatory agency IT examination reports.

3. Determine whether management adequately reviews all reports to ensure the audit scope was sufficient and that all deficiencies are appropriately addressed.

CONCLUSIONS

Objective 14: Discuss corrective actions and communicate findings.

1. Determine the need to perform Tier II procedures for additional validation to support conclusions related to any of the Tier I objectives.

2. Using results from the above objectives and/or audit's internally assigned audit rating or audit coverage, determine the need for additional validation of specific audited areas and, if appropriate:

- Forward audit reports to examiners working on related work programs, and
- Suggest either the examiners or the institution perform additional verification procedures where warranted.

3. Using results from the review of the IT audit function, including any necessary Tier II procedures:

- Document conclusions on the quality and effectiveness of the audit function as related to IT controls; and
- Determine and document to what extent, if any, examiners may rely upon the internal and external auditors' findings in order to determine the scope of the IT examination.

4. Review preliminary examination conclusions with the examiner-in-charge (EIC) regarding:

- Violations of law, rulings, and regulations;
- Significant issues warranting inclusion as matters requiring board attention or recommendations in the report of examination; and
- Potential effect of your conclusions on URSIT composite and component ratings.

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

6. Document examination conclusions, including a proposed audit component rating, in a memorandum to the EIC that provides report-ready comments for all relevant sections of the report of examination.

7. Document any guidance to future examiners of the IT audit area.

8. Organize examination work papers to ensure clear support for significant findings and conclusions.

TIER II OBJECTIVES AND PROCEDURES

The Tier II examination procedures for the IT audit process provide additional verification procedures to evaluate the effectiveness of the IT audit function. These procedures are designed to assist in achieving examination objectives and scope and may be used entirely or selectively.

Tier II questions correspond to URSIT rating areas and can be used to determine where the examiner may rely upon audit work in determining the scope of the IT examination for those areas.

Examiners should coordinate this coverage with other examiners to avoid duplication of effort with the examination procedures found in other IT Handbook booklets.

A. MANAGEMENT

1. Determine whether audit procedures for management adequately consider:

- The ability of management to plan for and initiate new activities or products in response to information needs and to address risks that may arise from changing business conditions;
- The ability of management to provide reports necessary for informed planning and decision making in an effective and efficient manner;
- The adequacy of, and conformance with, internal policies and controls addressing the IT operations and risks of significant business activities;
- The effectiveness of risk monitoring systems;

- The level of awareness of, and compliance with, laws and regulations;
- The level of planning for management succession;
- The ability of management to monitor the services delivered and to measure the institution's progress toward identified goals in an effective and efficient manner;
- The adequacy of contracts and management's ability to monitor relationships with technology service providers;
- The adequacy of strategic planning and risk management practices to identify, measure, monitor, and control risks, including management's ability to perform self-assessments; and
- The ability of management to identify, measure, monitor, and control risks and to address emerging IT needs and solutions.

B. SYSTEMS DEVELOPMENT AND ACQUISITION

1. Determine whether audit procedures for systems development and acquisition and related risk management adequately consider:

- The level and quality of oversight and support of systems development and acquisition activities by senior management and the board of directors;
- The adequacy of the institutional and management structures to establish accountability and responsibility for IT systems and technology initiatives;
- The volume, nature, and extent of risk exposure to the institution in the area of systems development and acquisition;
- The adequacy of the institution's systems development methodology and programming standards;
- The quality of project management programs and practices that are followed by developers, operators, executive management/owners, independent vendors or affiliated servicers, and end-users;
- The independence of the quality assurance function and the adequacy of controls over program changes including the:

  - parity of source and object programming code,

  - independent review of program changes,

  - comprehensive review of testing results,

  - management's approval before migration into production, and

  - timely and accurate update of documentation;

- The quality and thoroughness of system documentation;
- The integrity and security of the network, system, and application software used in the systems development process;
- The development of IT solutions that meet the needs of end-users; and
- The extent of end-user involvement in the systems development process.

C. OPERATIONS

1. Determine whether audit procedures for operations consider:

- The adequacy of security policies, procedures, and practices in all units and at all levels of the financial institution and service providers.
- The adequacy of data controls over preparation, input, processing, and output.
- The adequacy of corporate contingency planning and business resumption for data centers, networks, service providers, and business units. Consider the adequacy of offsite data and program backup and the adequacy of business resumption testing.
- The quality of processes or programs that monitor capacity and performance.
- The adequacy of contracts and the ability to monitor relationships with service providers.
- The quality of assistance provided to users, including the ability to handle problems.
- The adequacy of operating policies, procedures, and manuals.
- The quality of physical and logical security, including the privacy of data.
- The adequacy of firewall architectures and the security of connections with public networks.

D. INFORMATION SECURITY

1. Determine whether audit procedures for information security adequately consider the risks in information security and e-banking. Evaluate whether:

- A written and adequate data security policy is in effect covering all major operating systems, databases, and applications;
- Existing controls comply with the data security policy, best practices, or regulatory

guidance;

- Data security activities are independent from systems and programming, computer operations, data input/output, and audit;
- Some authentication process, such as user names and passwords, that restricts access to systems;
- Access codes used by the authentication process are protected properly and changed with reasonable frequency;
- Transaction files are maintained for all operating and application system messages, including commands entered by users and operators at terminals, or at PCs;
- Unauthorized attempts to gain access to the operating and application systems are recorded, monitored, and responded to by independent parties;
- User manuals and help files adequately describe processing requirements and program usage;
- Controls are maintained over telecommunication(s), including remote access by users, programmers and vendors; and over firewalls and routers to control and monitor access to platforms, systems and applications;
- Access to buildings, computer rooms, and sensitive equipment is controlled adequately;
- Written procedures govern the activities of personnel responsible for maintaining the network and systems;
- The network is fully documented, including remote and public access, with documentation available only to authorized persons;
- Logical controls limit access by authorized persons only to network software, including operating systems, firewalls, and routers;
- Adequate network updating and testing procedures are in place, including configuring, controlling, and monitoring routers and firewalls;
- Adequate approvals are required before deployment of remote, Internet, or VPN access for employees, vendors, and others;
- Alternate network communications procedures are incorporated into the disaster recovery plans;
- Access to networks is restricted using appropriate authentication controls; and
- Unauthorized attempts to gain access to the networks are monitored.

2. Determine whether audit procedures for information security adequately consider compliance with the "Interagency Guidelines Establishing Standards for Safeguarding Customer Information," as mandated by Section 501(b) of the Gramm-Leach-Bliley Act of 1999. Consider evaluating whether management has:

- Identified and assessed risks to customer information;
- Designed and implemented a program to control risks;
- Tested key controls (at least annually);
- Trained personnel; and
- Adjusted the compliance plan on a continuing basis to account for changes in technology, the sensitivity of customer information, and internal/external threats to information security.

E. PAYMENT SYSTEMS

1. Determine whether audit procedures for payment systems risk adequately consider the risks in wholesale electronic funds transfer (EFT). Evaluate whether:

Adequate operating policies and procedures govern all activities, both in the wire transfer department and in the originating department, including authorization, authentication, and notification requirements;

- Formal contracts with each wire servicer exist (i.e., Federal Reserve Bank (FRB), correspondent financial institutions, and others);
- Separation of duties is sufficient to prevent any one person from initiating, verifying, and executing a transfer of funds;
- Personnel policies and practices are in effect;
- Adequate security policies protect wire transfer equipment, software, communications lines, incoming and outgoing payment orders, test keys, etc.;
- Credit policies and appropriate management approvals have been established to cover overdrafts;
- Activity reporting, monitoring, and reconcilement are conducted daily, or more frequently based upon activity;
- Appropriate insurance riders cover activity;
- Contingency plans are appropriate for the size and complexity of the wire transfer function; and
- Funds transfer terminals are protected by adequate password security.

2. Determine whether audit procedures for payment systems risk adequately consider

the risks in retail EFT (automatic teller machines, point-of-sale, debit cards, home banking, and other card-based systems including VISA/Master Charge compliance). Evaluate whether:

- Written procedures are complete and address each EFT activity;
- All EFT functions are documented appropriately;
- Physical controls protect plastic cards, personal identification number (PIN) information, EFT equipment, and communication systems;
- Separation of duties and logical controls protect EFT-related software, customer account, and PIN information;
- All transactions are properly recorded, including exception items, and constitute an acceptable audit trail for each activity;
- Reconcilements and proofs are performed daily by persons with no conflicting duties;
- Contingency planning is adequate;
- Vendor and customer contracts are in effect and detail the responsibilities of all parties to the agreement;
- Insurance coverage is adequate; and
- All EFT activity conforms to applicable provisions of Regulation E.

3. Determine whether audit procedures for payment systems risk adequately consider the risks in automated clearing house (ACH). Evaluate whether:

- Policies and procedures govern all ACH activity;
- Incoming debit and credit totals are verified adequately and items counted prior to posting to customer accounts;
- Controls over rejects, charge backs, unposted and other suspense items are adequate;
- Controls prevent the altering of data between receipt of data and posting to accounts;
- Adequate controls exist over any origination functions, including separation of data preparation, input, transmission, and reconcilement;
- Security and control exist over ACH capture and transmission equipment; and
- Compliance with NACHA, local clearinghouse, and FRB rules and regulations.

F. OUTSOURCING

1. Determine whether audit procedures for outsourcing activities adequately cover the risks when IT service is provided to external users. Evaluate whether:

- Formal procedures are in effect and staff is assigned to provide interface with users/ customers to control data center-related issues (i.e., program change requests, record differences, service quality);
- There are contracts with all customers (affiliated and nonaffiliated) and whether the institution's legal staff has approved them;
- Controls exist over billing and income collection;
- Disaster recovery plans interface between the data center, customers, and users;
- Controls exist over on-line terminals employed by users and customers;
- Comprehensive user manuals exist and are distributed; and
- There are procedures for communicating incidents to clients.

2. Determine whether audit procedures for outsourced activities are adequate. Evaluate whether:

- There are contracts in place that have been approved by the institution's legal staff,
- Management monitors vendor performance of contracted services and the financial condition of the vendor,
- Applicable emergency and disaster recovery plans are in place,
- Controls exist over the terminal used by the financial institution to access files at an external servicer's location,
- Internal controls for each significant user application are consistent with those required for in-house systems,
- Management has assessed the impact of external and internal trends and other factors on the ability of the vendor to support continued servicing of client financial institutions,
- The vendor can provide and maintain service level performance that meets the requirements of the client, and
- Management monitors the quality of vendor software releases, documentation, and training provided to clients.

Appendix B: Glossary

Application controls - Controls related to transactions and data within application systems. Application controls ensure the completeness and accuracy of the records and the validity of the entries made resulting from both programmed processing and manual data entry. Examples of application controls include data input validation, agreement of batch totals and encryption of data transmitted.

Application system - An integrated set of computer programs designed to serve a well-defined function and having specific input, processing, and output activities (e.g., general ledger, manufacturing resource planning, human resource management).

Audit charter - A document approved by the board of directors that defines the IT audit function's responsibility, authority to review records, and accountability.

Audit plan - A description and schedule of audits to be performed in a certain period of time (ordinarily a year). It includes the areas to be audited, the type of work planned, the high-level objectives and scope of the work and includes other items such as budget, resource allocation, schedule dates, and type of report issued.

Audit program - The audit policies, procedures, and strategies that govern the audit function, including IT audit.

Exposure - The potential loss to an area due to the occurrence of an adverse event.

General controls - Controls, other than application controls, that relate to the environment within which application systems are developed, maintained, and operated, and that are therefore applicable to all the applications at an institution. The objectives of general controls are to ensure the proper development and implementation of systems, and the integrity of program and data files and of computer operations. Like application controls, general controls may be either manual or programmed. Examples of general controls include the development and implementation of an IT strategy and an IT security policy, the organization of IT staff to separate conflicting duties and planning for disaster prevention and recovery.

Independence - Self-governance, freedom from conflict of interest and undue influence. The IT auditor should be free to make his or her own decisions, not influenced by the organization being audited, or by its managers and employees.

Outsourcing - The practice of contracting with another entity to perform services that might otherwise be conducted in-house. Contracted relationship with a third party to provide services, systems, or support.

Risk - The potential that events, expected or unanticipated, may have an adverse effect on a financial institution's earnings, capital, or reputation.

Risk assessment - A prioritization of potential business disruptions based on severity and likelihood of occurrence. The risk assessment includes an analysis of threats based on the impact to the institution, its customers, and financial markets, rather than the nature of the threat.

Systems Development Life Cycle (SDLC) - An approach used to plan, design, develop, test, and implement an application system or a major modification to an application

system.

Work program - A series of specific, detailed steps to achieve an audit objective.

Appendix C: Laws, Regulations, and Guidance

Laws

- 12 USC 1761 & 1761d: Supervisory Committee (N/A)
- Public Law 107-204: Sarbanes-Oxley Act of 2002, Pub (N/A)

Federal Financial Institutions Examination Council

- Interagency Policy Statement on the Internal Audit Function and Its Outsourcing (March 2003)
- Interagency Policy Statement on External Auditing Programs of Banks and Savings Associations (September 1999)
- Interagency Policy Statement on Coordination and Communication Between External Auditors and Examiners (July 1992)

Federal Reserve Board

- 12 CFR Part 208, Appendix D-1: Interagency Guidelines Establishing Standards for Safety and Soundness (N/A)
- SR Letter 03-8; Statement on Application of Recent Corporate Governance Initiatives to Non-Public Banking Organizations (May 5, 2003)
- SR Letter 03-5: Amended Interagency Guidance on the Internal Audit Function and its Outsourcing (April 22, 2003)
- SR Letter 02-20: The Sarbanes-Oxley Act of 2002 (October 29, 2002)

Federal Deposit Insurance Corporation

- 12 CFR Part 363: Annual Independent Audits and Reporting Requirements (N/A)
- FIL 21-2003: Interagency Policy Statement on the Internal Audit Function and Its Outsourcing (March 7, 2003)
- FIL 96-99: Interagency Policy Statement On External Auditing Programs of Banks

and Savings Associations (October 25, 1999)

National Credit Union Administration

- 12 CFR Part 715: Supervisory Committee Audits and Verifications (N/A)
- NCUA Letter to Credit Unions 02-CU-17: E-Commerce Guide for Credit Unions (December 2002)
- NCUA Letter to Credit Unions 01-CU-11: Electronic Data Security Overview (August 2001)
- NCUA Letter to Credit Unions 97-CU-5: Interagency Statement on Retail On-Line PC Banking (April 1997)

Office of the Comptroller of the Currency

- 12 CFR Part 30: Safety and Soundness Standards (N/A)
- OCC Bulletin 2003-12: Interagency Policy Statement on Internet Audit and Internal Audit Outsourcing (March 17, 2003)
- OCC Bulletin 99-37: Interagency Policy Statement on External Auditing Programs (July 9, 2003)
- Comptroller's Handbook: Community Bank Supervision, Booklet (August 2001)
- Comptroller's Handbook: Community Bank Supervision, Appendix (August 2001)
- Comptroller's Handbook: Internal and External Audits, Introduction (April 2003)
- Comptroller's Handbook: Internal and External Audits, Appendixes (April 2003)
- Comptroller's Handbook: Large Bank Supervision (May 2001)
- Comptroller's Handbook: Internal and External Audits, Supplemental Examination Procedures (April 2003)
- The Director's Book: The Role of a National Bank Director (March 1997)

Office of Thrift Supervision

- 12 CFR Part 562.4: Audit of Savings Associations and Savings Association Holding Companies (N/A)

- 12 CFR Part 570, Appendix A: Interagency Guidelines Establishing Standards for Safety and Soundness (N/A)
- Thrift Bulletin 81: Interagency Policy Statement on the Internal Audit Function and Its Outsourcing (March17, 2003)
- CEO LTR 113: Internal Controls (July 14, 1999)
- Thrift Activities Handbook Section 341: Technology Risk Controls (January 2002)
- Thrift Activities Handbook Section 350: External Audit (July 2002)
- Thrift Activities Handbook Section 355: Internal Audit (February 2002)