Introduction

Critical to the success of an organization is the effective management of its information technology (IT). Today's business environment requires increased quality, system integration, functionality and ease of use, decreased delivery time, and continuously improving service levels, while demanding that costs be controlled.

An effective IT program addresses the following key areas:

a) IT governance;
b) Risk management;
c) IT Strategic planning;
d) Project management;
e) Information security;
f) Electronic banking;
g) IT operations;
h) Vendor risk management;
i) Business continuity planning;
j) Audit coverage; and
k) Management Information Systems (MIS).

The term, "key areas" or "key functions" as used in this document refers to the above list.

IT Governance

IT governance is critical to the performance and success of all business activities since IT is an enabler for the various lines of business to succeed. Ultimately, it is the board of directors' responsibility to ensure a satisfactory governance process is in place.

The board of directors typically charters a separate IT Steering Committee (ITSC) to help provide the oversight of the many key areas that present risks to the organization; but, the board itself maintains the ultimate responsibility to ensure that risks from any IT activities are well controlled. It is not uncommon for organizations to have a number of other IT committees to support each key area according to the needs of the organization.

Due to the complexities of IT, governance processes need to be sufficiently robust to determine the level of day-to-day compliance with established policies, practices and procedures in each of the key areas of IT organization. This is achieved in a number of ways and may include the following:

a) Board approved IT policies.
b) Board Packages with timely and informative key-area information.
c) Written IT departmental policies.
d) Written procedures in each of the key functions.

e) Formal processes for line management to self-identify their level of compliance with any relevant IT policy, practice or procedure pertaining to their function, and
f) Formal process to determine if overall policies, practices and procedures are acceptable, if management complies with them, and if any changes are warranted in them.

Risk Management

The ability to mitigate IT risks is dependent upon sound risk assessments. Senior management needs to identify, measure, monitor and control technology to mitigate risks that threaten the efficient operation and the safety and soundness of an institution. Institutions ***plan*** for use of technology; ***assess*** the risk associated with technology; decide how to ***implement*** the technology; and establish a process to ***measure and monitor*** risk that exists in their organizations. All organizations need:

a) An effective planning process that aligns IT with business objectives;
b) An ongoing risk assessment process that evaluates the environment and potential changes;
c) Technology implementation procedures that include appropriate controls; and
d) Quantifiable measurements identified and implemented to effectively monitor efforts that identify risk exposures.

The board should implement policies that establish a satisfactory program to identify, manage, and report risk levels. The program should identify the institution's tolerance for risk, measure the effectiveness of internal controls, establish management's accountability, and identify processes to manage IT effectively.

Strategic Planning

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

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

a) Member demographics;
b) Organizational growth targets;
c) Technology capabilities;
d) Regulatory requirements such as privacy, security, and disclosures;
e) Cost containment;
f) Process improvement and efficiency gains;

g) Customer service and technology performance quality;
h) Outsourcing vs. in-house expertise;
i) Optimal infrastructure for the future; and
j) Ability to adopt and integrate new technology.

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

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

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

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

IT Related Project Management

An organization's ability to manage projects successfully is dependent on clearly defined expectations, satisfactory project management processes, realistic budgets, effective communications and adequate oversight by the board and executive management. Ineffectively managed projects often result in late deliveries, cost-overruns, or poor quality applications and may expose the organization to data loss, reputation risk and inability to meet business goals.

Financial institutions use various methods to manage technology projects. The systems development life cycle (SDLC) provides a systematic way to control the numerous tasks associated with development projects. Large projects should be well defined both in time, money or impact to the organization and processes often differ from smaller projects that present less risk.

Each large project should have a well documented cost-benefit analysis, clearly identified project management methodologies, and budgetary controls to help meet desired goals in

an acceptable manner. Smaller projects should be itemized in a centralized list and tracked to ensure that controls are effective. The board, or board-designated committee should periodically review the status of all significant projects as well as keep abreast of smaller projects via the centralized list. Proper documentation should be available to support significant deviations from approved procedures, goals, time-frames, or major changes.

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

Information Security

Information security is the process by which an organization protects and secures systems, media, and facilities that process and maintain information vital to its operations. The FHLBanks and their service providers should maintain effective security programs adequate for their operational complexity, and the security programs should have satisfactory board and senior management level support, integration of security responsibilities and controls throughout the organization's business processes, and clear accountability for carrying out security responsibilities.

Institutions protect their information by instituting a security process that identifies risks, forms a strategy to manage the risks, implements the strategy, tests the implementation, and monitors the environment to control the risks. This is accomplished by meeting the following objectives:

a) ***Availability***-addresses the processes, policies, and controls used to ensure authorized users have prompt access to information. This objective protects against intentional or accidental attempts to deny legitimate users access to information and/or systems.

b) ***Confidentiality of data or systems***-addresses the processes, policies, and controls employed to protect information of customers and the institution against unauthorized access or use.

c) ***Integrity of data or systems***-relates to the processes, policies, and controls used to ensure information has not been altered in an unauthorized manner and that systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability.

d) ***Accountability***-involves the processes, policies, and controls necessary to trace actions to their source. Accountability directly supports non-repudiation, deterrence, intrusion prevention, intrusion detection, recovery, and legal admissibility of records.

e) ***Assurance***-addresses the processes, policies, and controls used to develop confidence that technical and operational security measures work as intended. Assurance levels are part of the system design and include availability, integrity, confidentiality, and accountability.

The security process is the method an organization uses to implement and achieve its security objectives.

a) ***Information Security Risk Assessment-***A process to identify threats, vulnerabilities, attacks, probabilities of occurrence, and outcomes.

b) ***Information Security Strategy-***A plan to mitigate risk that integrates technology, policies, procedures and training. The plan should be reviewed and approved by the board of directors.

c) ***Security Controls Implementation-***The acquisition and operation of technology, the specific assignment of duties and responsibilities to managers and staff, the deployment of risk-appropriate controls, and assurance that management and staff understand their responsibilities and have the knowledge, skills, and motivation necessary to fulfill their duties.

d) ***Security Testing-***The use of various methodologies to gain assurance that risks are appropriately assessed and mitigated. These testing methodologies should verify that significant controls are effective and performing as intended.

e) ***Monitoring and Updating-***The process of continuously gathering and analyzing information regarding new threats and vulnerabilities, actual attacks on the institution or others combined with the effectiveness of the existing security controls. This information is used to update the risk assessment, strategy, and controls. Monitoring and updating makes the process continuous instead of a one-time event.

Information security is the responsibility of everyone at the institution, as well as the institution's service providers and contractors. The board, management, and employees all have different roles in developing and implementing an effective security process. A failure in any one group impacts the entire organization.

The board of directors is responsible for overseeing the development, implementation, and maintenance of the institution's information security program. Oversight requires the board to provide management with adequate guidance and appropriately review security reports on the effectiveness of the overall information security program.

The board needs to approve written information security policies and the information security program at least annually. The board should provide management with its expectations and requirements for:

a) Central oversight and coordination;
b) Areas of responsibility;
c) Risk measurement;
d) Monitoring and testing;
e) Reporting; and
f) Acceptable residual risk.

Security officers are responsible and accountable for security administration. At a minimum, they should directly manage or oversee risk assessment, development of policies, standards, and procedures, testing, and security reporting processes. Security officers are responsible for responding to security events and need to have sufficient authority to order emergency actions to protect the financial institution and its members from an imminent loss of information or value. They need to have sufficient knowledge, background, and training, as well as be in an organizational position which enables them to perform their assigned tasks.

A central authority should be responsible for establishing and monitoring the security program. Preferably, this should be performed within the context of a comprehensive, enterprise-wide compliance program that also includes IT. Security management responsibilities, however, may be distributed throughout the institution from the IT department to various lines of business depending on the institution's size, complexity, culture, nature of operations, and other factors. The distribution of duties should ensure an appropriate segregation of duties between individuals or organizational groups.

Senior management is responsible for ensuring the integration of security controls across the organization. Effectively integrated controls will:

a) Ensure the security process is governed by organizational policies and practices that are consistently applied;
b) Require that data with similar criticality and sensitivity characteristics be protected consistently regardless of where in the organization it resides;
c) Enforce compliance with the security program in a balanced and consistent manner across the organization;
d) Develop an acceptable data classification program;
e) Develop an acceptable document retention program; and
f) Coordinate information security with physical security.

Employees should know, understand, and be held accountable for fulfilling their security responsibilities. Institutions should define these responsibilities in their security policy. Job descriptions or contracts should specify any additional security responsibilities beyond the general policies. Financial institutions can achieve effective employee awareness and understanding through security training, employee certifications of compliance, self-assessments, audits, and monitoring.

Management also should consider the roles and responsibilities of external parties. Technology Service Providers (TSPs), contractors, customers, and others who have access to the institution's systems and data should have their security responsibilities clearly delineated and documented in contracts.

Electronic Banking

Electronic banking (E-Banking) is defined as the automated delivery of banking products and services directly to customers through electronic, interactive communication channels. E-Banking includes the systems that enable financial institution customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the internet. The primary access to the products and services are obtained through informational and transactional websites.

Informational websites provide members access to general information about the financial institution and its products or services. Specific risks to be considered are as follows:

a) Potential liability and violations for inaccurate or incomplete information about products, services, and advance pricing presented on the website;
b) Potential access to confidential financial institution or member information if the website server is not properly isolated from the financial institution's internal network;
c) Potential liability for spreading viruses and other malicious code to computers communicating with the institution's website; and
d) Negative public perception if the institution's on-line services are unavailable during normal business hours, are disrupted for an extended period, or if its website is defaced or otherwise presents inappropriate or offensive material.

Transactional websites provide members with the ability to view and/or conduct transactions through the financial institution's website by initiating banking transactions or buying products and services. Transactions can range from something as basic as viewing a member's demand deposit account to implementing a recurring wire transfer to pre-established beneficiaries, conducting a security purchase and/or sale(s), or submitting an advance request.

Since transactional websites typically enable the viewing of account balances, or conduct an electronic exchange of confidential member information and the transfer of funds, services provided through these websites expose the FHLBank to higher risk than basic informational websites.

Wholesale E-Banking systems such as wire transfers typically expose FHLBanks to the highest risk per transaction, since commercial transactions usually involve larger dollar amounts. Specific risks to be considered include:

a) Security controls for safeguarding member information;
b) Authentication processes necessary to initially verify the identity of new members and authenticate existing members who access electronic banking services;
c) Liability for unauthorized transactions;
d) Losses from fraud if the institution fails to verify the identity of individuals or businesses applying for new accounts or credit on-line;
e) Possible violations of laws or regulations pertaining to privacy, anti-money laundering, anti-terrorism, or the content, timing, or delivery of required disclosures; and
f) Negative public perception, member dissatisfaction, and potential liability resulting from failure to process third-party payments as directed or within specified time frames, lack of availability of on-line services, or unauthorized access to confidential information during transmission or storage.

IT Operations

One of the primary responsibilities of IT operations management is to ensure the institution's current and planned infrastructure can satisfactorily support the strategic plans of senior management and the board in a safe and sound manner. To accomplish this objective, operations management should ensure the institution has sufficient personnel in knowledge, experience, and number, system capacity and availability, program integration, and storage capacity to achieve strategic objectives. Operations management should select or recommend technology solutions that can meet strategic requirements with reduced resources to control capital expenditures and operating costs.

Management should have an inventory of all of the institution's technology assets, maintain documentation noting all interdependencies of these systems and should understand how these systems support the associated business lines. Additionally, management should understand the flow of data across and between systems. Adequate documentation of infrastructure and data flow facilitates risk identification, application of controls, and ongoing maintenance of information systems. Procedures should be established to identify and remove outdated and/or unsupported hardware and software.

IT operations management should establish procedures to stay abreast of security patches, to test them in a segregated environment, and to install them when appropriate. Change management procedures should require documentation of any patch installations. Procedures should be established to address the version controls of operating and application software to ensure the implementation of the latest releases such as maintaining a record of versions in place, and ongoing monitoring for product enhancements, security issues, patches or upgrades, or other problems with current versions of the software.

Management should implement a cost-effective and risk-focused control environment. The control environment should provide guidance, accountability, and enforceability while mitigating risk. Management should periodically assess the effectiveness of the

control environment, which may be evaluated through self-assessments or other means. Management should also regularly test the results of the assessments through audits or other independent verification. Detailed internal control assessments performed to meet Sarbanes-Oxley (SARBOX) Act requirements are an adjunct to the internal audit process, and not a substitute for internal audits.

To ensure sound recovery operations management should develop a business continuity plan (BCP). IT systems should have robustness, resiliency, redundancy and capacity sufficient to accommodate ordinary interruptions to operations and to facilitate prompt restoration without escalating to more drastic and costly disaster recovery procedures. Operations management staff should recognize any limitations of IT operations staff and be prepared to obtain professional assistance. At times, it may be more efficient and cost effective to acquire outside expertise than to hire and train new employees, especially for functions that do not require full-time personnel.

Operations management should ensure the operating environment is physically and logically secure. Sound IT operations management also includes providing adequate staffing through personnel selection, succession plans, and employee training. Hiring practices that result in an appropriate number of skilled staff promote smooth, continuous, and efficient operations. Ongoing training is vital to maintaining creative, motivated, and knowledgeable employees.

Operations management needs to have a good set of automated tools to help assist in monitoring key performance indicators (KPIs). Essential KPIs include memory capacities, storage capacity, bandwidth, key utilizations by time of day per unit and an enterprise-wide assessment of these factors. KPI monitoring expands as complexities increase.

Vendor Risk Management

Financial institutions increasingly rely on external or third-party TSP service providers for a variety of technology-related services. External service providers can sometimes provide low-cost processing and other IT-related services that are more adaptive to the enterprise than internally provided services. Generally, the term "outsourcing" is used to describe these types of arrangements.

Outsourcing, however, does not reduce the fundamental risks associated with information technology nor does it remove the FHLBank's responsibilities for controlling risk. Risks such as loss of funds, loss of competitive advantage, damaged reputation, improper disclosure of information, and regulatory action remain. When the functions are performed by an organization outside the financial institution, the risks may be realized in a different manner than if the functions were inside the financial institution, resulting in the need for controls designed to monitor such risks.

Financial institutions can outsource many areas of operations, including all or part of any service, process, or system operation. Examples of information technology operations frequently outsourced by institutions include: the origination, processing, and settlement of payments and financial transactions; information processing related to customer account creation and maintenance; information and transaction processing activities that support critical banking functions, such as loan processing, deposit processing, fiduciary and trading activities; payroll; security monitoring and testing; system development and maintenance; network operations; help desk operations; and call centers.

Management may choose to outsource operations for various reasons. These include:

a) Gain operational or financial efficiencies;
b) Increase management focus on core business functions;
c) Refocus limited internal resources on core functions;
d) Obtain specialized expertise;
e) Increase availability of services;
f) Accelerate delivery of products or services through new delivery channels;
g) Increase ability to acquire and support current technology and avoid obsolescence; and
h) Conserve capital for other business ventures.

Before considering the outsourcing of significant functions, an institution's directors and senior management should ensure such actions are consistent with their strategic plans and should evaluate proposals against well-developed acceptance criteria. The degree of oversight and review of outsourced activities will depend on the criticality of the service, process, or system to the institution's operation. Management should consider the following factors in evaluating the quantity of risk at the inception of an outsourcing decision.

Risks pertaining to the function outsourced include:

a) Sensitivity of data accessed, protected, or controlled by the service provider;
b) Volume of transactions; and
c) Criticality to the financial institution's business.

Risks pertaining to the service provider include:

a) Strength of financial condition;
b) Turnover of management and employees;
c) Ability to maintain business continuity;
d) Ability to provide accurate, relevant, and timely applications;
e) Experience with the function outsourced;
f) Reliance on subcontractors;
g) Location, particularly if cross-border or foreign-based third party service providers; and

h) Redundancy and reliability of data lines.

Risks pertaining to the technology utilized include:

a) Reliability;
b) Security; and
c) Scalability to accommodate growth.

Financial institutions should have a comprehensive outsourcing risk management process to govern their TSP relationships. The process should include risk assessment, selection of service providers, contract review and service level agreements, and monitoring of service providers such as SAS 70 reports, evaluation of financial condition, insurance, etc.

Outsourced relationships should be subject to the same risk management, security, privacy, and other policies that would be expected if the financial institution were conducting the activities in-house. Depending on the type of outsourced process, there may be SARBOX compliance implications if the SAS 70 scope is not of the correct type. A "Type 1" controls attestation SAS 70 may not be adequate for a mission-critical or financial type process. A more detailed, control testing "Type 2" SAS 70 would be required for a TSP providing a mission-critical service that affects financial statements.

Business Continuity Planning and Recovery

Section 917.3(b)(3)(v) of the Finance Board's regulations requires each FHLBank's board of directors to set forth standards for the FHLBank's management regarding business risk including contingency plans, where appropriate. The Finance Board's Advisory Bulletin 03-2, Business Continuation Contingency Planning, discusses bilateral agreements to act as surrogates for each other in the event a debilitating event affected one of the FHLBanks.

The following factors are critical aspects of effective business continuity planning:

Distance between the production site and the recovery site should be carefully assessed. A recovery site that is too close may not be available in certain type of circumstances, and a recovery site that is too far may be a hindrance to realize a fast recovery and meet the recovery goals of the FHLBanks and the Office of Finance.

a) Business continuity planning and recovery should be conducted on an enterprise-wide basis at least annually, and more often if the test revealed issues that need to be addressed.
b) A thorough business impact analysis and risk assessment (BIA) is the foundation of an effective BCP and therefore, the BIA should be updated at least annually.
c) Business continuity planning and recovery is more than the recovery of the technology; it is aimed at the recovery of the business. Line management should

ascertain how long they can function without electronic processes and should clearly identify what responsibilities/functions should continue to be done in the absence of electronic processes being available.

d) The effectiveness of a BCP can only be validated through thorough volume testing. Volume testing for this purpose denotes a level of test transactions that affirms the ability of the back up system to accept input, process, and generate output acceptable to conduct the FHLBank's various lines of businesses.
e) The BCP and test results should be subjected to independent audit or assessment.
f) A BCP should be periodically updated to reflect and respond to changes in the institution, and
g) The IT Division should also have a business resumption plan that covers personnel, equipment, and key contracts for the support of IT activities.

IT Audit (Internal, External, and Outsourced)

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. 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.

Examiners should consider the following issues when evaluating the IT audit function:

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

It is important to note that SARBOX control self-assessments are not audits since the self-assessments are usually performed by the business lines and thus are not independent. Internal/External audit should not rely on these self-assessments or substitute them for independent audit work but can utilize them to gain an understanding of the controls in a functional area.

Management Information Systems (MIS)

A management information system (MIS) is a system or process that provides the information necessary to manage the FHLBank effectively and efficiently. MIS and the

information it generates are generally considered essential components of prudent and reasonable business decisions and are designed to:

a) Facilitate the assessment of and management of risks within the institution;
b) Provide management with an adequate decision support system by providing information that is timely, accurate, consistent, complete and relevant;
c) Deliver complex material throughout the institution;
d) Support the organization's strategic goals and objectives;
e) Provide an objective system for recording and aggregating information;
f) Reduce expenses related to labor-intensive manual activities; and
g) Enhance communication with employees and customers.

The importance of maintaining a consistent approach to the development, use and review of MIS systems within the institution should be an ongoing concern of both FHLBank management and the examiners. Every line of business in the FHLBanks is heavily dependent upon technology to be successful, thus MIS should have a clearly defined framework of guidelines, policies or practices, standards, and procedures for the organization. These should be followed throughout the institution in the development, maintenance and use of all MIS.

Regulatory Environment

The primary authorities governing, or relevant to, information technology of the FHLBanks are set forth below. The discussion does not address the application of authorities other than the FHLBank Act and the regulations, interpretations and issuances of the Finance Board to the FHLBanks. The examiner should ensure that the application of such authorities to an FHLBank has been considered by the FHLBank and its legal counsel.

1) Rules and Regulations of the Federal Housing Finance Board, which include the following parts and sections relevant to information technology:

Part 917 of the Finance Board regulations addresses powers and responsibilities of FHLBank boards of directors and senior management. In particular, Section 917.3, Risk Management, Section 917.4 Bank Member Products Policy, and Section 917.6, Internal Control System, are pertinent.

Section 917.5 requiring the FHLBank's board of directors to have a strategic business plan that describes how the business activities of the FHLBank will achieve its mission consistent with Part 940 (Core mission activities).

Section 917.7, addresses the powers, duties and responsibilities of the audit committees and oversight of the internal audit function. These responsibilities should be detailed in a charter and approved by the board of directors. The charter should be re-approved at least every three years.

Section 917.8, requires the board of directors to be responsible for the adoption of the FHLBank's annual operating expense budget and capital expenditures, and with the FHLBank's responsibility to protect both its members and the public interest by keeping its costs to an efficient and effective minimum.

Section 989.3, addresses the preparation and completion of the FHLBank's financial statements, and the distribution of financial information and other information to the Finance Board and the Office of Finance.

2) Advisory Bulletins of the Federal Housing Finance Board that provide supervisory guidance relating to the topic of information technology activities are:

Advisory Bulletin 02-02 dated February 13, 2002, which provides guidance on the annual reporting of the FHLBank's strategic plan to the Finance Board.

Advisory Bulletin 03-02 dated February 10, 2003 and Advisory Bulletin 02-3 dated February 13, 2002, which provides guidance on specific attributes to be considered by FHLBanks in the formulation of their business continuity plans, and the establishment of bilateral agreements with other FHLBanks.

Advisory Bulletin 04-01 dated March 10, 2004, which provides guidance on the evaluation of a service organization providing services to an FHLBank whose activities could affect the FHLBank's financial condition. This includes the performance of an assessment of the service organization's internal controls, such as the procurement of a service auditor's report in accordance with Statement of Auditing Standards No. 70 (SAS 70) or the performance of alternative methods.

Advisory Bulletin 05-05 dated May 18, 2005, which provides guidance on the risk management responsibilities of the board, senior management and risk management function.

3) United States Code Title 18 Section 1030-Fraud and related activity in connection with computers provides for fines and/or imprisonment for the unauthorized access or exceeding authorized access to a computer and thus obtaining protected information, including nonpublic financial information.

4) Issuances of the Federal Financial Institutions Examination Council (FFIEC) that address specific guidance, controls and procedures applicable to information technology examinations. Specific FFIEC examination booklets are available covering such topics as:

a) IT Audit;
b) Business Continuity Planning;
c) Development and Acquisition;
d) E-Banking;

e) Information Security;
f) Management;
g) Operations;
h) Outsourcing Technology Services;
i) Retail Payment Systems;
j) Supervision of Technology Service Providers; and
k) Wholesale Payment Systems.

5) Federal Reserve Bank Operating Circulars and Appendices that set forth the terms for maintaining accounts with and obtaining other services from the Federal Reserve Banks. Specifically:

a) Operating Circular No. 1-Account Relationships, Agreements and Forms;
b) Operating Circular No. 5-Electronic Access, Certification Practice Statement, and Password Practice Statement;
c) Operating Circular No. 6-Funds Transfers Through the Fedwire Funds Service; and
d) Operating Circular No. 12-Multilateral Settlement.

6) Issuances of the Board of Governors of the Federal Reserve System (Board) and Federal Financial Institutions Examination Council that address specific controls and procedures as to Fedwire and privately operated payment systems. Specifically:

a) Board of Governors System FedLine Advantage References;
b) FFIEC Information Technology Handbooks, such as Information Security, Business Continuity Planning and Wholesale Payment Systems; and
c) FFIEC Guidance-Authentication in an Internet Banking Environment.

FHLBank Environment

Information technology environments vary due to various factors such as corporate governance, business strategies, risk management/assessment, products, services, personnel, hardware/software, and processing methodologies. In addition, due to staffing limitations and required technical expertise, specific processes and independent testing may be outsourced.

When evaluating the adequacy and effectiveness of information technology activities, examiners should review the FHLBank's policies and procedures against actual practices. If the review of actual practices discloses significant internal control deficiencies, the examiners should be alert to overall weaknesses with corporate governance and independent testing.

Risks Associated with Information Technology

An FHLBank's primary risks relating to the information technology are set forth below.

1) Lack of Sound Corporate Governance (Board of Directors and Senior Management Oversight)

a) Information technology is not aligned with the bank's goals and strategies.
b) Key risks and controls are not adequately identified, assessed, and monitored.
c) The FHLBank's financial performance and compliance with established risk tolerances, goals, policies, procedures, accounting and regulatory requirements are not properly reviewed and monitored due to inadequate, inaccurate and/or untimely reporting to the board of directors and senior/line management. Original establishment of risk tolerances, threshold guidelines, etc., are not well documented on how they were determined.
d) A lack of establishment of an acceptable IT Compliance Program that provides ongoing process to identify missing controls, or controls that are not meeting expectations.
e) Weak architecture design which may not support current operations as well as future operations that meet the corporate goals of growth, capacity needs, etc.
f) Lack of a robust firewall architecture to implement a satisfactory physical dual-layered firewall architecture with sufficient redundancy at the primary (network facing) firewall layer as well as at the perimeter (internet facing) firewall layer.
g) Lack of satisfactory separation of duties for the security administration function. Maintaining insufficient security tools, lack of security policy monitoring, and lack of self-identification.
h) Security is built and monitored by the same individuals versus separating the security functions into at least two major areas - the policy and testing function from that of the day-to-day build, add, modify and or delete functions.
i) Internal control weaknesses potentially affecting financial reporting have not been adequately identified, assessed and disclosed, or evaluated for the determination of the risk imposed as a result of control weaknesses.
j) Duties, responsibilities, and staff expertise, including segregation of operational and control functions, are not adequately defined.
k) Background credit and criminal investigations are not performed on personnel prior to their retention. Periodic credit investigations are not performed and mandatory leave policies have not been established or enforced.
l) Duties, responsibilities, and liabilities are not adequately addressed with outside service providers and vendors.
m) Losses due to errors and fraud are not effectively mitigated through insurance or other means.
n) Regulatory requirements are not complied with due to errors and/or deficiencies affecting the vendor software.
o) Independent audit coverage and testing is limited. Staff is inexperienced or lacks the technical expertise to test the control environment.

p) Lack of data classification policies and document retention policies and supporting processes to provide guidance how to store, protect, and, archive data in a sound manner.
q) Lack of End User Computing (EUC) policies and supporting processes to ensure adequate controls are in place to safeguard data, maintain proper documentation and ensure all IT policies, standards and guidelines are satisfactory met.

2) Operational Risk

a) Management information systems do not adequately meet the needs of the FHLBank's lines of business resulting in various manual processes such as user developed applications and workarounds which can result in errors and misstated financial results.
b) IT key performance standards (KPIs) are not identified or not based on historical information and business goals. IT KPIs are not being measured and reported to line management.
c) Inside and/or an outside threat gains unauthorized access to system information, or an internal or external user inadvertently damages the integrity of critical information resulting in the following:
    i) Possible financial loss due to an unauthorized transaction;
    ii) Loss of data integrity due to an unauthorized modification, deletion or input of erroneous transactions;
    iii) Loss of availability due to use of malicious software, software with viruses, etc. that make the systems unavailable;
    iv) Loss of confidentiality; and
    v) Loss of public confidence and credibility due to compromise of the external website and/or internal bank systems.
d) Viruses, worms and/or other malware infiltrate the FHLBank's systems resulting in corrupt files, loss or stolen data, system unavailability, slow response times, etc.
e) Unauthorized purchase of new applications or modifications/changes to existing systems which may be incompatible with the operating system.
f) Patches and updates to existing applications are not being monitored, reviewed and tested for compatibility to the operating system.
g) Systems are impacted by hurricane, flood, bomb, fire, etc. Power issues such as a long term outage or spike surge could cause the FHLBank and customers to lose availability of critical systems and data.
h) Technology inventory such as hardware, software, network components, media storage, etc. is not accurate, updated or completed on an on-going basis.
i) SAS 70 reviews are not obtained, nor alternative methods performed to obtain assurances on the outside service provider's internal control environment.
j) Insurance coverage had not been evaluated and obtained to mitigate the FHLBank's risks and exposure.
k) Procedures that pertain to the destruction and retention of records have not been established.

l) A lack of pre-planning capacity estimation processes, or omission of key capacity monitoring such as memory, telecommunication channels, central processing units, etc.
m) Maintaining inadequate separation between production process environment and development and/or testing environments.
n) End User Computing lacks adequate processes to ensure that all lines of business adequately control EUC processes, that a complete inventory is maintained and that sufficient controls are in place for each EUC application to ensure safe, accurate and timely outputs is achieved.
o) Not establishing sufficient controls to prevent unauthorized software from being introduced into the FHLBank's or the Office of Finance's processing environments. Not establishing sufficient controls to detect unauthorized software.

Specific Risk Controls Related to Information Technology

An FHLBank's controls relating to information technology are set forth below.

1) Corporate Governance

The board of directors and senior management have the ultimate responsibility for the design, implementation, and monitoring of the FHLBank's internal control environment. The internal controls should address the FHLBank's tolerance for risk, the effectiveness of internal controls, management's accountability in regards to risk mitigation, and the processes needed to manage information technology effectively and efficiently.

Specific internal control environment include the identification of the key risks, implementation of controls, organizational structure, departmental policies and procedures, managerial review and exception reporting, hiring practices and business contingency planning, and retention of staff possessing the necessary technical expertise. Ideally, information technology should be included in an enterprise-wide compliance program to ensure that policies and procedures are complied with and functioning as intended.

2) Business Continuity and Recovery

Business continuity planning is the process whereby the FHLBank ensures the maintenance or recovery of operations, including services to members, when confronted with adverse events such as natural disasters, technological failures, human error, or terrorism. The objectives of a business continuity plan are to minimize financial loss to the institution, continue to serve members and financial market participants; and mitigate the negative effects disruptions can have on an FHLBank's strategic plans, reputation, operations, liquidity, credit quality, market position and ability to remain in compliance with applicable laws and regulations.

Information technology personnel have a leadership role in the FHLBank's business continuity plan. This includes prioritizing critical business functions, and identifying the necessary resources to creating, maintaining and testing the plan.

For example, the FHLBank should have written procedures for operations at its designated hot-site. Back-up tapes should be stored off-site and be easily retrievable. Bilateral agreements with one or more FHLBanks may need to be used to effectuate the FHLBank's activities. Each FHLBank should have at least one back-up system and should test it periodically to ascertain its reliability.

3) Insurance

The potential for liability to an FHLBank arising from its information technology activities and its system of control should be reflected in the FHLBank's annual risk assessment. The FHLBank may mitigate its risks and liability with the purchase of specific insurance and bond coverage such as directors and officers' liability, errors and omissions, computer cyber crime policies and fidelity bond coverage. Where an FHLBank mitigates its operational risk through the maintenance of insurance coverage, the adequacy of such coverage relative to actual loss experience should be periodically assessed.

In addition, the specific limitations, exclusions, notifications, and other clauses of each policy should be reviewed to determine their effects upon the availability of coverage under specific circumstances. Claims may be rejected if the FHLBank has weak controls or fails to follow its internal procedures.

Examination Guidance

A work program for Information Technology accompanies this narrative. What follows below are illustrative examples of attributes that should be considered by the examiner in completing the analyses required in that work program. In determining the extent of review and testing to be conducted in completing each analysis, the examiner should take into account his or her assessment of the quality and effectiveness of corporate governance, risk management, internal controls and audit coverage relating to the institution's information technology activities.

1) Organizational Structure

a) Evaluate the organizational chart and determine if there is sufficient separation of duties at the functional level to achieve the desired IT goals of the enterprise;
b) Functional organization and reporting structure;
c) Identification of key personnel;
d) Primary duties, responsibilities and technical expertise of personnel;
e) Segregation of duties;
f) Cross-training of personnel;

g) Coordination with other departments such as risk management, business lines, executive management, and human resources; and
h) Significant changes in the foregoing since the last examination.

2) Establishment of risk tolerances and development of key policies and oversight by the board of directors. Evaluate the adequacy of senior management oversight and the risk management function for information technology, which may include the following:

a) Determine if the organization has adopted sufficient board approved policies that support all key areas of the IT function;
b) Determine if senior management has appropriately complemented board policies with departmental policies, procedures, guidelines, standards and practices;
c) Determine if any key policy, procedure, or standards have not been formalized and implemented;
d) Determine if the organization has established sufficient oversight. Consider all committees, management groups, etc., to effectively monitor IT activities, establish adequate controls, monitor projects, identify risks and provide proper oversight to all key areas of IT operations;
e) Evaluate the information provided to the board of directors and/or committees and evaluate the completeness of IT information provided;
f) Determine the effectiveness of how the organization aligns business needs with IT activities;
g) Determine if the organization has implemented an effective IT Compliance Program to ensure a satisfactory compliance with key policies, procedures, guidelines and thresholds desired;
h) Determine how management identifies, updates and maintains a satisfactory level of compliance with applicable federal and state regulations;
i) Determine if the FHLBank has formally implemented a process to maintain an effective and updated IT Standards Manual(s);
j) Determine if management information systems (MIS) are adequate to measure the performance based on clearly defined goals and objectives; and
k) Interview management and determine if any significant changes have been implemented and/or are under consideration with respect to information technology activities. Consider systems, processes, staffing, and utilization of outside consultants that may affect the processing, telecommunications or recovery environments.

3) Key FHLBank policies and procedures, which may include those relating to the following:

a) Enterprise-wide IT policy;
b) Risk management policy;
c) Information security policy;
d) Business resumption policy;

e) Systems programming and development policy (System Development Life Cycle);
f) Change management policy;
g) Document retention policy;
h) Data classification policy;
i) Vendor management policy;
j) Fraud prevention policy;
k) Whistleblower provisions of SARBOX;
l) End-user computing;
m) Database management;
n) Evaluate the work flow and processes used to implement an effective network architecture and maintain related documentation and work flow diagram current; and
o) Identify changes from the prior examination and determine if management has complied with acceptable change management practices.

4) Risk assessment under Part 917 and internal control evaluation under SARBOX

a) Evaluate the effectiveness of the annual risk assessment under Part 917 that identifies the key risks arising from technology use.
b) Evaluate controls established by the institution concerning technology use and determine if management has an acceptable process in place to verify the effectiveness of those controls. Note, this is a management driven task and audits do not eliminate the need for management to self-assess;
c) Evaluate the effectiveness of evaluations conducted pursuant to SARBOX that identify the key risks and controls pertaining to financial reporting and evaluate potential fraud, and procedures implemented to periodically attest to the adequacy of the control environment.

5) Testing performed by external and internal audit and outside consultants

a) Evaluate the effectiveness of internal audit activities; consider audit staff participation in key IT meetings such as project discussions, strategic planning, and security planning.
b) Evaluate the effectiveness of audits completed by selecting audit reports and audit work papers.
c) Evaluate the effectiveness of audit reporting by reviewing audit reports to the board of directors and/or committees of the board.
d) Evaluate the effectiveness of scope and testing performed by outside consultants specific to technology.

6) Information Security Administration

a) Evaluate the enterprise-wide data security program. Specific attributes include, but are not limited to the following:

(1) Security automated tools;
(2) Intrusion detection tools;
(3) Staff skill set(s);
(4) Data classification policies;
(5) Network architecture, including demilitarized zones;
(6) Firewall rules;
(7) Intrusion detection systems and alert reporting;
(8) Incident response strategies;
(9) Database protection schemes;
(10) Data encryption;
(11) Segmentation of production, test, and development environments;
(12) Separation of duties at the IT level as well as the line of business level;
(13) User education;
(14) Vulnerability assessments;
(15) Penetration tests;
(16) Reporting to senior management as well as to committees and the board;
(17) Post mortems assessments;
(18) Consultants, technical service providers, temporary employees; and
(19) End-user computing.

b) Evaluate the effectiveness of board oversight concerning security related events.
c) Identify changes from the prior examination and determine if management has complied with acceptable change management practices.

7) Identification and evaluation of controls and significant changes to the activity or function

a) Evaluate workflow and processes as well as controls, including the level and direction of risk and the quality of risk management; and
b) Evaluate any significant changes that have been implemented since the last examination or are being considered that may affect the FHLBank's operational risk profile.

8) Testing

Conduct testing as appropriate taking testing performed by other examiners into consideration. The scope of testing should be based on the preliminary review of governance, risk management, internal controls and audit coverage. Specific examples include, but are not limited to, the following:

a) Obtain and evaluate management information system reports used by management to determine their level of compliance with established policies, procedures, guidelines, thresholds and determine if management takes appropriate action when weaknesses are identified.
b) Review the documentation used to develop the risk assessment and determine if sufficient quantifiable data was used to make informed decisions.

c) Review minutes of any strategic planning done between the IT division and executive management for the purpose of aligning IT Strategic Plans and determine if appropriate documentation evident an effective process.
d) Select a major project either recently completed, in-process or in early stages of planning and review documentation to determine if the organization is in compliance with satisfactory policies, practices or procedures concerning that project. Determine how management determines they are in satisfactory compliance. Consider if major projects have control points before releasing additional funding.
e) Select a key element of information provided to the board and determine how the information was gathered, how management determined its accuracy and if it properly reflects what it reports.
f) Obtain a list of all information security reports that are completed on a frequency basis, and evaluate the effectiveness of the information and management's action(s) to address risks identified.
g) Interview security officers and evaluate their ability to prevent, detect and report and take corrective action when warranted.
h) Obtain copies of network diagrams that detail servers, routers, firewalls, and supporting system components. Determine if these diagrams are current and if any risks are evident as a result of work flows or lack of security points.
i) Obtain and review management asset inventories. Evaluate the process used to maintain the inventories current.
j) Review documentation supporting Systems Development and Programming.
k) Evaluate the effectiveness of monitoring system reliabilities, capacities, and response times. Consider if the organization does adequate assessments for these key performance indicators as well as being able to identify trends.
l) Select a recent outsource project and evaluate if management has implemented sufficient controls to ensure data protection.
m) Evaluate the effectiveness of the organization's data classification policy.
n) Evaluate the effectiveness of the organization's document retention policy.
o) Evaluate the effectiveness of user-acceptance processes; consider how scripts are developed as well as how achievements are defined.
p) Select a recent change to an application and evaluate the effectiveness of change control procedures; considering the organization's Change Control Policy. Identify any weakness in the Policy or in the process.
q) Evaluate the effectiveness of the organization's database processes; consider the level of database use, separation of duties, sensitivity of information, access controls and platforms used to support databases.

9) Assessment of Risks

Summarize the results of the activity or function examined in a separate memorandum. The memorandum must articulate the risks and the management of those risks. It should also clearly and specifically describe the basis and analysis for the assessment. The memorandum should discuss the type(s) of risk (market, credit,

operational); the level of risk (low, moderate, high); the direction of risk (stable, decreasing, increasing); and the quality of risk management (strong, adequate, weak). A memorandum must be prepared irrespective of whether the examiner's assessment is positive or negative.

10) Items requiring follow-up at the next on-site visitation

Identify key issues that have been communicated to management (written or oral) that require follow-up during the next on-site visitation.