Introduction

Management of information and the supporting technology is critical to the performance and success of each regulated entity and the Office of Finance. Sound management of information and technology requires the same framework utilized for all risk management – identify, measure, monitor, control, and report on information technology (IT) risks. This module is applicable to the examinations of the Enterprises (Fannie Mae and Freddie Mac), the Federal Home Loan Banks (FHLBanks), and the Office of Finance (OF).

Some aspects of IT risks will be addressed through other FHFA Examination Manual modules. For example, IT governance concepts will be included in the Operational Risk Management module, and business continuity planning (including disaster recovery planning) concepts will be included in the Business Continuity Planning module. The scope of this module addresses:

1) IT Governance;
2) IT Operations;
3) Information Security Management;
4) IT Development, Acquisition, and Maintenance;
5) Outsourcing Management;
6) IT Audits;
7) Management Information Systems (MIS); and,
8) Electronic Banking.

Although these topics will be discussed independently, examiners should assess each institution's ability to manage the unique risks posed by each topic, as well as the institution's ability to manage the collective risks posed by the use of technology.

IT Governance

IT governance is critical to the performance and success of all business activities since IT enables the various lines of business to succeed. Ultimately, the board of directors has responsibility to ensure a satisfactory governance process is in place. The board should establish a corporate-wide risk culture for assessing IT demands and providing processes to meet those demands. Establishing a corporate-wide policy for IT that addresses critical aspects of governance and risk management is an essential element to establishing an effective corporate governance culture. Management can then establish a more detailed framework of supporting policies, standards, and procedures that demonstrates how they will operate within the broader risk parameters established by the board.

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 ultimate responsibility for ensuring that risks from any IT activities

are well-controlled. Organizations commonly have a number of other IT committees to support each key area according to the needs of the organization. Examiners should document the committee structures that support IT in the regulated entity under examination. Knowing the goal(s) of each committee helps evaluate if the board and management are appropriately governing all critical aspects of IT activities.

Governance processes need to be sufficiently robust to determine the level of day-to-day compliance with established policies, practices, and procedures in the key areas of entity's IT infrastructure. Ongoing IT compliance monitoring needs to occur in order to keep the board and senior management informed of adherence to approved policies and procedures. Management can achieve an effective compliance monitoring process through various organizational structures but ultimately the process should be independent from IT as well as separate from internal audit. The compliance function should be subject to audit coverage and audit staff should leverage off compliance reviews to the extent practical to avoid unnecessary duplication of efforts.

Management can achieve effective governance in a number of ways including 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 for each 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 processes to determine if overall policies, practices, and procedures are acceptable; if management complies with them; and if any changes are warranted. This is best achieved through a formal IT Compliance Program (ITCP).

IT Operations

IT operations involve the institution's ability to process and store information in a timely, reliable, and secure manner. The evolving role technology plays in supporting this business function has become increasingly complex. IT operations (traditionally housed in a computer data center with user connections through terminals) have become more dynamic and may include distributed environments, integrated applications, telecommunications infrastructure, Internet connectivity, and an array of computer operating platforms. In addition, as the complexity of technology has grown, many institutions have increased their reliance on vendors, partners, and other third parties for a variety of technology solutions and services.

Information systems, whether centralized, distributed, in-house, or outsourced, are interconnected and highly interdependent. Management's failure to adequately understand the risks and properly implement the board's strategy and IT policy for any

part of the IT environment can heighten potential risks for all elements of IT operations and the institution as a whole. Consequently, the board must ensure that management coordinates IT controls throughout the institution's operating environment, including any outsourced functions and any critical third-party arrangements.

While the following list is not all inclusive, some key elements of IT operations risk management responsibilities include:

1) Identifying, measuring, monitoring, and controlling IT risks;
2) Implementing an IT organizational structure suitable to support the business activities of the institution;
3) Maintaining current documentation of the systems in place, and maintaining a satisfactory understanding of how each of these systems supports the associated business processes;
4) Ensuring outsourcing to third-parties is consistent with strategic plans and appropriately managed;
5) Establishing an effective control environment through appropriate risk identification, assessment, management, and monitoring processes;
6) Creating and maintaining physical and logical secured operating environments;
7) Providing for satisfactory operational continuity and resiliency;
8) Providing adequate staffing and personnel selection, succession, and training; and
9) Using qualified consultants and external auditors, when necessary.

Technology enables each institution to develop, deliver, and manage products and services. An effective IT risk management process should identify, measure, monitor, control, and report operations risk. Understanding the role technology plays in enabling the business strategy and core business operations establishes the framework for assessing risk. Accordingly, the risk identification process begins with a comprehensive survey of the institution's technology environment and an inventory of its technology assets.

The survey of the technology environment and inventory of its technology assets incorporate an assessment of the relative importance of systems, databases, applications, key interfaces and data criticality, and their importance to core business operations. The inventory helps clarify the enterprise architecture and highlights the relationships between the institution's internal systems and networks, and external systems.
Once the institution identifies and analyzes the universe of IT risks, management should prioritize the IT risk assessment results based on the business importance of the associated systems. In addition, management should prioritize risk mitigation actions based on the probability of occurrence and the financial, reputational, or legal implications for the institution. The effect is not always easy to quantify, but should include such considerations as lost revenue, loss of market share, increased cost of insurance premiums, litigation and adverse judgment costs, in addition to possible data recovery and reconstruction expenses.

Management's responsibilities include monitoring and maintaining IT infrastructure and appropriately planning for changes to the infrastructure in order to support the current and future strategic plans of the entity. Management should facilitate organization MIS, development and delivery of products and services, internal end-user information and processing requirements, data capture, data classification, and transaction processing. To accomplish this objective, management should ensure the institution has sufficient personnel in terms of knowledge, experience, and number. Additionally, system capacities, reliability/availability, storage capacity, and program integration are essential for proper support of business activities. Management should select or recommend technology solutions that can effectively meet strategic goals.

IT operations management should implement an organizational structure that addresses human resources and, where appropriate, multiple operating sites for supporting the institution's business activities. IT operations, whether centralized or decentralized, should adequately support products, services, and functional operations. Management should facilitate individual business unit's MIS needs. All internal end-user information and process requirements, data capture, data classification, and transaction processing is the responsibility of operations management.

Effective IT management requires knowledge and understanding of the institution's IT environment. Appropriate documentation should be in place that indicates how these systems support the associated business processes (enterprise architecture). Using its inventory of technology assets, management should recognize interdependencies of these systems, and should understand how these systems support the associated business activities. 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 support and maintenance of information systems.

For products or services that are provided by a vendor or other third-party, management of the institution should ensure that its security, infrastructure, and overall standards are met. Senior management must provide a means for management, including security personnel, to be involved early in the selection process of third-party provided products or services to help in this regard.

IT operations staff should be aware of the institution's information security program, how the program relates to their job function, and their role as information custodians. As custodians, the IT operations staff has the responsibility of protecting information as it is processed and stored. IT operations management should implement preventive, detective, and corrective logical security controls. Examples of each respective logical control include access controls, logging, and incident response. All three types of controls provide a framework for IT operations information security. These controls can be implemented by administrative, logical, or physical controls.

IT systems require resiliency, redundancy, and capacity sufficient to accommodate ordinary interruptions to operations and facilitate prompt restoration without escalation to more drastic and costly disaster recovery procedures. To ensure sound recovery operations, management should develop a business continuity plan (see the Business Continuity Planning examination module for more details). The business continuity plan should address the plans for ordinary interruptions, as well as the plans for extraordinary interruptions or disasters.

Sound IT operations management also requires 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. At times, it may be more efficient and cost effective to contract outside expertise, especially for functions that do not require permanent personnel.

Formal service level agreements (SLAs) should be established with any IT provider, for both in-house and outsourced functions. SLAs establish mutual expectations and provide a baseline to measure IT performance. Performance benchmarks and outcome-based measurements are examples of SLA issues.

Information Security Management

Protecting an institution's information, and the systems that support the information, is a shared responsibility of management, service providers and contractors. The board, management, and employees have different roles in developing and implementing an effective security program and a failure by any one might affect the entire organization. An information security management (ISM) program establishes the framework by which systems, media, facilities, and data vital to operations are maintained, secured, and protected. The ISM program should also include the institution's privacy program for protecting personally identifiable information. The institutions and their service providers must maintain an effective ISM program. The ISM program must be adequate for each institution's operational complexity. In addition, the ISM program 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.

The goal of an ISM program is to enable an organization to meet mission/business objectives by implementing systems with due consideration of IT-related risks to the organization, partners, and customers/members. This goal can be achieved by attaining the following security objectives[1]:

[1] Source: National Institute of Standards and Technology (NIST) Special Publication 800-33, Underlying Technical Models for Information Technology Security, December 2001

1) *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.

2) *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.

3) *Confidentiality of data or systems* – addresses the processes, policies, and controls employed to protect information of customers/members, borrowers, and the regulated entity against unauthorized access or use.

4) *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.

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

The ISM program is the method the institution uses to implement and achieve its security objectives. The ISM program must be designed to identify, measure, monitor, and control security risks. The ISM program should have an effective means that identifies risks allowing management to form strategies to manage risks, test the appropriateness of established standards, assess compliance with those standards, and provide ongoing risk assessments. Consequently, the ISM program should include policies and processes that address:

1) *Information Security Risk Assessment* – a process to identify threats, vulnerabilities, attacks, probabilities of occurrence, and outcomes. A security risk assessment gathers data regarding the information and technology assets of the organization, threats to those assets, vulnerabilities, existing security controls and processes, and the current security standards and requirements; analyzes the probability and effect associated with the known threats and vulnerabilities to institution assets; and prioritizes the risks present due to threats and vulnerabilities to determine the appropriate level of training, controls, and assurance necessary for effective mitigation.

2) *Information Security Strategy* – a plan to mitigate risk that integrates technology, policies, procedures, and training. An information security strategy includes appropriate consideration of prevention, detection, and response mechanisms; implementation of the least permissions and least privileges concepts; layered

controls that establish multiple control points between threats and organization assets; and policies that guide officers and employees in implementing the security program. An institution's information security strategy should be reviewed and approved by the board.

3) *Information Security Controls Implementation* – the acquisition and operation of technology, specific assignment of duties and responsibilities to managers and staff, 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.

4) *Information Security Monitoring/Testing 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. An information security monitoring/testing and updating process uses various tools and techniques to identify vulnerabilities, policy violations, and anomalous behavior. 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. In addition, the institution should perform active monitoring of cyber threats and vulnerabilities through the email advisory service provided by security leaders such as US-CERT and SANS.

The board is responsible for overseeing the development, implementation, and maintenance of the institution's ISM program, and holding senior management accountable for its actions. Oversight requires the board to provide management with adequate guidance; approve information security plans, policies, and programs; and review security reports on the effectiveness of the overall ISM program.

Management should ensure the operating environment is physically and logically secure. Protection of expensive and critical business assets, especially sensitive information, is essential. Dealing with confidential borrower and customer/member information requires management to establish and enforce access controls to facilities, equipment, applications, systems, and transaction and borrower/customer/member data.

Management should designate one or more individuals as information security officer(s). Security officers are responsible and accountable for the administration of the security program. At a minimum, they should directly manage or oversee the risk assessment process; 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 institution from any imminent loss of information or value. They need to have sufficient knowledge, background, training, and organizational authority to perform their assigned tasks.

Management also should consider and monitor the roles and responsibilities of external parties. The security responsibilities of technology service providers (TSPs), contractors, customers/members, and others who have access to the institution's systems and data should be clearly delineated and documented in contracts. Appropriate reporting mechanisms should be in place to allow management to make judgments as to the fulfillment of those responsibilities. Finally, sufficient controls should be included in the contract to enable management to enforce contractual requirements.

An effective security program requires that the business units play a significant role in the identification of their security needs. Examiners should be familiar with the security requirements of that business unit and evaluate the effectiveness of the business unit's overall ability to understand and meet those requirements. The business unit managers should take ownership of their applications supported by IT and ensure they maintain appropriate separation of duties and access controls standards (also supported by IT), and that systems in place meet their needs in an appropriately secured schema.

Information security risk assessment is the process used to identify and understand risks to the availability, integrity, confidentiality, and accountability of information and information systems. A risk assessment consists of the identification and valuation of assets and an analysis of those assets in relation to potential threats and vulnerabilities, resulting in a ranking of risks to mitigate. The resulting information is used to develop strategies to mitigate those risks.

An adequate assessment identifies the value and sensitivity of information and system components and then balances that knowledge with the exposure from threats and vulnerabilities. A risk assessment is a prerequisite to the formation of strategies that guide the institution as it develops, implements, tests, and maintains its information system's security posture. An initial risk assessment may involve a significant one-time effort, but the risk assessment process should be an ongoing part of the ISM program.

An information security strategy is a plan to mitigate risks while complying with legal, statutory, regulatory, contractual, and internally developed requirements. Typical steps to building a strategy include the definition of control objectives, identification and assessment of approaches to meet the objectives, selection of controls, establishment of benchmarks and metrics, and preparation of implementation and testing plans.

The selection of controls is typically grounded in a cost comparison of different strategic approaches to risk mitigation. The cost comparison typically contrasts the costs of various approaches with the potential gains a financial institution could realize in terms of increased confidentiality, availability, or integrity of systems and data. Those gains could include reduced financial losses, increased customer/member confidence, and regulatory compliance. Any particular approach should consider: (1) policies, standards, and procedures; (2) technology design; (3) resource dedication; (4) organization's risk tolerance level, (5) training; and (6) testing.

Security requires the integration of people, processes, and technology. Each of the three components should be managed considering the capabilities and limitations of the other components. When the components are considered in total, they should provide for adequate overall risk mitigation.

Security strategies include prevention, detection, and response, and all three are needed for a comprehensive and robust security framework. Typically, security strategies focus most resources on prevention. Prevention is intended to reduce the likelihood of harm. Detection identifies a security breach and the response is designed to limit damage once a security breach has occurred. Weaknesses or limitations in prevention may be offset by strengths in detection and response.

Security strategies should establish information security control limitations on access and limitations on the ability to perform unauthorized actions. Those limitations derive from concepts known as security domains, least permissions, and least privileges.

The creation of security domains involves designing a network so that users and network resources are grouped in a logical or physical manner, and control sets are established to mitigate the risks relevant to each individual domain. At the network level, connectivity between network areas may be disabled or tightly controlled through perimeters. Tools could include firewalls, virtual local area networks, router access control lists, and directories. The tools allow for restrictions on access and authorizations at the network and application layers.

The concepts of least permissions and least privileges are used to provide functionality while limiting potentially harmful actions. They generally involve restricting authorizations at the network, server, and client level to as-needed only. For example, a user could be allowed access to only certain network resources, program functions or file areas and not allowed access to others. A program could be allowed access to some of a computer's or network's resources and disallowed access to others. Authorization for users most often is managed by assigning a user to a group or role and granting permissions to the group or role.

Security monitoring focuses on the activities and condition of network traffic and network hosts. Activity monitoring is primarily performed to assess policy compliance, identify non-compliance with the institution's policies, and identify intrusions and support an effective intrusion response. Because activity monitoring is typically an operational procedure performed over time, monitoring is capable of providing continual assurance.

Monitoring of conditions is typically performed in periodic testing. The assurance provided through testing can relate to the absence of an intrusion, compliance with authorized configurations, and overall resistance to intrusions. Testing does not provide continual assurance, but relates to the point in time of the test. Thus, testing needs to be conducted periodically.

Risk drives the degree of monitoring. In general, risk increases with system accessibility and the sensitivity of data and processes. For example, a high-risk system is one that is remotely accessible and allows direct access to funds, fund transfer mechanisms, or sensitive borrower/customer/member data. Information-only websites that are not connected to any internal system or transaction-capable service are lower-risk systems. Information systems that exhibit high risks should be subject to more rigorous monitoring than low-risk systems.

An institution's security monitoring should, commensurate with the risk, be able to identify control failures before a security incident occurs, detect an intrusion or other security incident in sufficient time to enable an effective and timely response, and support post-event forensics activities.

IT Development, Acquisition, and Maintenance

Development, acquisition, and maintenance are an organization's ability to identify, acquire, install, and maintain appropriate information technology systems. The process includes the internal development of software applications or systems and the purchase of hardware, software, or services from third parties.

An institution's ability to manage development, acquisition, and maintenance 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.

For development projects, an organization needs to have established standards that address the risks posed by developing technology solutions to business needs. These standards should address project management, system control, quality assurance, change management, and end-user-computing (EUC) applications (e.g., internally developed spreadsheets).

Institutions may use various methods to manage development projects. The systems development life cycle (SDLC) provides a systematic way to control the numerous tasks associated with development projects. Both large and small projects should be well defined in time, money, and effect to the institution while processes for smaller projects that present less risk may be less formalized.

Each large project should have a well-documented cost-benefit analysis and budgetary controls to help meet desired goals in an acceptable manner. In addition, the institutions must have clearly identified project management methodologies that are commensurate with a project's characteristics and risks. Project management methodologies should include:

1) Management sponsorship and commitment;
2) Project plans;
3) Definitions of project requirements and expectations;
4) Project management standards and procedures;
5) Quality assurance and risk management standards and procedures;
6) Definitions of project roles and responsibilities;
7) Approval authorities and procedures;
8) Involvement by all affected parties;
9) Project communication techniques; and
10) Validation of project execution

Smaller projects should at least be itemized in a centralized list and tracked to ensure that controls are effective. A 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 for lower-risk projects; however, all projects should include appropriate segregation of duties or other compensating controls.

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

Change management broadly encompasses change control, patch management, and conversions. This also includes the policies, procedures, and processes for implementing change. "Scope creep" is a common problem associated with software development projects. It occurs when developers receive requests to add or modify a program's features while the program is being developed. Although the addition or modification of functional, security, or control features may be appropriate, uncontrolled changes disrupt the development process. Establishing change approval procedures and cut-off dates (after which requested changes are deferred to subsequent versions) assists organizations in managing change during the development process.

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

Acquisition projects are similar to development projects because management approves project requests; defines functional, security, and system requirements; and appropriately tests and implements products. Organizations often employ structured acquisition methodologies similar to the SDLC when acquiring significant hardware and software products. However, the SDLC design and development phases are replaced with a bid solicitation process that involves developing detailed lists of functional, security, and system requirements and distributing them to third parties.

In addition to developing and distributing detailed lists of functional, security, and system requirements, the institutions should establish vendor selection criteria and review potential vendors' financial strength, support levels, security controls, and other essential matters, prior to obtaining products or services. Additionally, management should review contracts and licensing agreements to ensure the rights and responsibilities of each party are clear. Primary risks include inadequately defining requirements, ineffectively assessing vendors, and insufficiently reviewing contracts and agreements.

Contract and licensing issues may arise due to the complexity of contractual requirements. An institution's legal counsel should confirm that performance guarantees, source code accessibility, intellectual property considerations, potential conflicts of interest, and software/data security issues are appropriately addressed before management signs contracts.

Maintenance activities include the routine servicing and periodic modification of hardware, software, and related documentation. Hardware modifications are periodically required to replace outdated or malfunctioning equipment or to enhance performance or storage capacities. Software modifications are required to address user requirements, rectify software problems, correct security vulnerabilities, or implement new technologies. Documentation maintenance is necessary to maintain current and accurate technology-related records, standards, and procedures.

Failure to implement appropriate change controls can result in operational disruptions or degrade a system's performance or security. Change controls (sometimes referred to as configuration management) involve establishing baseline versions of products, services, or procedures and ensuring all changes are approved, documented, and disseminated. Change controls should address all aspects of the institution's technology environment including software programs, hardware and software configurations, operational standards and procedures, and project management activities.

Change controls can be applied universally to all systems and environments or stratified to particular systems, business lines, and support areas. Stratified procedures are often necessary to address the distinct control requirements of mainframe, network, and client/server environments; operating and application programs; and development and acquisition projects.

Management should establish detailed change control standards and procedures to ensure technology related modifications are appropriately authorized, tested, documented, implemented, and disseminated. The characteristics and risks of a system, activity, or change should dictate the formality of the change controls. Quality assurance, security, audit, network, and end-user personnel should be appropriately involved in the change process.

Outsourcing

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

Outsourcing does not reduce the fundamental risks associated with information technology nor does it eliminate the institution's responsibilities for controlling risk. Risks such as loss of funds, loss of competitive advantage, damaged reputation, improper disclosure of information, and adverse regulatory action remain. When the functions are performed by an organization outside the institution, the risks may be realized in a different manner than if the functions were inside the institution, resulting in the need for controls designed to monitor such risks. The institution is ultimately responsible for the safeguarding of data and the integrity of information when using a third-party for information processing.

The institutions may outsource many areas of operations, including all or part of any service, process, or system operation. Examples of IT operations frequently outsourced by institutions include: the origination, processing, and settlement of payments and financial transactions; information processing related to account creation and maintenance; information and transaction processing activities that support critical functions, such as 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:

1) Gaining operational or financial efficiencies;
2) Increasing management focus on core business functions;
3) Refocusing limited internal resources on core functions;
4) Obtaining specialized expertise;
5) Increasing availability of services;
6) Accelerating delivery of products or services through new delivery channels;
7) Increasing ability to acquire and support current technology and avoid obsolescence; and
8) Conserving capital for other business ventures.

Before considering the outsourcing of significant functions, an institution's board and senior management should establish and approve risk-based policies to govern the outsourcing process. The policies should recognize the risk to the institution from outsourcing relationships and should be appropriate to the size and complexity of the institution. In addition, the board 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.

The quantity of risk associated with an outsourced IT service is subject to the function outsourced, the service provider, and the technology used by the service provider. Management should consider the factors below in evaluating the quantity of risk at the inception of an outsourcing decision.

Risks pertaining to the function outsourced include:

1) Sensitivity of data accessed, protected, or controlled by the service provider;
2) Volume of transactions; and
3) Criticality to the institution's business.

Risks pertaining to the service providers include:

1) Strength of financial condition;
2) Turnover of management and employees;
3) Ability to maintain business continuity;
4) Ability to provide accurate, relevant, and timely applications;
5) Experience with the function outsourced;
6) Reliance on subcontractors;
7) Location, particularly if cross-border or foreign-based third-party service providers; and
8) Redundancy and reliability of communication lines.

Risks pertaining to the technology utilized include:

1) Reliability;
2) Security; and
3) Scalability to accommodate growth.

The institution should have a comprehensive outsourcing risk management process to govern the outsourced relationship(s). The process should include assessing the risk from outsourcing, creating requirements, selecting specific service providers, reviewing contracts, establishing service level agreements, and ongoing monitoring of service providers. Outsourced relationships should be subject to the same risk management,

security, privacy, business continuity, and other policies that would be expected if the institution were conducting the activities in-house.

Information Technology Audit (Internal and External)

A well-planned, properly structured audit program is essential to evaluate risk management practices, internal control systems, and compliance with corporate policies concerning risks at institutions of every size and complexity (see the Internal and External Audit examination module for more details). The IT 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, 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. An effective IT audit program should:

1) Identify areas of greatest IT risk exposure to the institution in order to focus audit resources;
2) Promote the confidentiality, integrity, and availability of information systems;
3) Determine the effectiveness of management's planning and oversight of IT activities;
4) Evaluate the adequacy of operating processes and internal controls;
5) Determine the adequacy of enterprise-wide compliance efforts related to IT policies and internal control procedures; and
6) 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 and senior management. Examiners should take into account the complexity and overall risk profile when performing this and other evaluations. Examiners should consider the following issues when evaluating the IT audit function:

1) Independence of the audit function and its reporting relationship to the board of directors or its audit committee;
2) Identification of the IT audit universe, risk assessment, scope, and frequency of IT audits;
3) Knowledge, skills, and experience of the IT audit staff;
4) Processes in place to ensure timely tracking and resolution of reported weaknesses; and
5) Documentation of IT audits, including workpapers, audit reports, and follow-up.

It is important to note that the Sarbanes-Oxley Act of 2002 (SARBOX) requirements for control self-assessments are not audits since the self-assessments are usually performed by the business lines and, thus, are not independent. Internal and 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.

TSPs that process work for several institutions often are 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.

A third-party audit, in this context, is an audit of a TSP 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 regulated institution's 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 activities.

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

1) Directly auditing the TSP's operations and controls;
2) Employing the services of external auditors to evaluate the TSP's operations and controls; or
3) Receiving and reviewing sufficiently detailed independent audit reports from the TSP.

If an institution uses independent audits to complement its own coverage, it should ensure that the independent auditor was qualified to perform the review, that the scope satisfies their own audit objectives, and that any significant reported deficiencies are corrected. The examiner and the institution must understand the nature and scope of the engagement and the level of assurance accruing from the accounting firm's work product.

Since 1992, Statement on Auditing Standards (SAS) no. 70, Service Organizations, has been the source of the requirements and guidance for auditors reporting on controls at service organizations (also known as TSPs) and for auditors auditing the financial statements of entities that use service organizations to accomplish tasks that may affect their financial statements. SAS no. 70 has been divided and replaced by two new standards. One is a Statement on Standards for Attestation Engagements (SSAE), also known as an attestation standard; the other is a SAS (an auditing standard). The requirement for reporting on controls at service organizations has been placed in SSAE no. 16, Reporting on Controls at a Service Organization. The requirements for auditing the financial statements of entities that use service organizations remain in the auditing

standards in a new SAS, Audit Considerations Relating to an Entity Using a Service Organization.

SSAE no. 16 enables a TSP auditor to issue two types of reports. In a type 1 report, the TSP auditor expresses an opinion on whether the service organization's description of controls is fairly presented (that is, whether it describes what actually exists) and whether the controls included in the description are suitability designed. Controls that are suitably designed are able to achieve the related control objectives if they operate effectively. In a type 2 report, the TSP auditor's report contains the same opinions as those in a type 1 report but also includes an opinion on whether the controls were operating effectively. Controls that operate effectively achieve the control objectives they were intended to achieve. A type 2 report also includes a description of the TSP auditor's tests of operating effectiveness and the results of those tests.

In the past, many auditors used SAS no. 70 to report on controls at a TSP that are unrelated to internal control over financial reporting, for example, controls over the privacy of borrowers'/customers'/members' information. However, SAS no. 70 is not applicable to audits of controls over subject matter other than financial reporting, and neither is SSAE no. 16.

There is increasing demand for reports on controls over subject matter other than financial reporting. For example, many institutions are required by law or regulation to maintain the privacy of the information they collect from customers/members, including the privacy of that information when it is at a TSP. To address these requirements, management of the institutions may ask the TSP for an auditor's report on the effectiveness of its controls over the privacy of information it processes.

If an auditor is engaged to issue a report on controls over subject matter other than financial reporting, such an engagement should be performed under AT section 101, Attest Engagements, of the attestation standards, but not under SSAE no. 16 (nor under SAS no. 70).[2]

Management Information Systems

A Management Information System (MIS) is a process that provides the information necessary to effectively manage an institution. Accurate and timely MIS reports are an essential component of prudent and reasonable business decisions. Many levels of management view and use MIS, which should support the institution's longer-term, strategic goals and objectives. All business units deploy and use MIS, frequently in the form of EUCs.

[2] Source: American Institute of CPAs (AICPA) web site, Service Organization Control Reports (formerly SAS 70 reports).

Examiners should evaluate the effectiveness of the MIS. Examiners assigned to IT, should evaluate the effectiveness of MIS as it relates to the IT operations. Examiners should be familiar with end-user-computing (EUC) applications. EUCs are small applications, sometimes spreadsheets, which business units use to make informed business decisions. Information derived from EUCs is part of an institution's MIS.

IT management typically sets departmental policies, procedures, and controls to govern various MIS areas. Common areas affecting MIS where an institution typically needs separate policies include database management, infrastructure standards, security, and processing scheduling. Examiners should evaluate the adequacy of operations managers in addressing the institution's departmental MIS policy needs.

Management should design MIS to:

1) Facilitate the assessment and management of risks within the institution;
2) Provide management with an adequate decision support system by providing information that is timely, accurate, consistent, complete, and relevant;
3) Deliver complex material throughout the institution;
4) Support the institution's strategic goals and objectives;
5) Provide an objective system for recording and aggregating information;
6) Reduce expenses related to labor-intensive manual activities; and
7) Enhance communication with employees and customers/members.

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

Because report generation systems can rely on manual data entry or extract data from many different financial and transaction systems, management should establish appropriate control procedures to ensure information is correct and relevant. Since MIS can originate from multiple equipment platforms and systems, the controls should ensure all information systems have sufficient and appropriate controls to maintain the integrity of the information and the processing environment.

To function effectively, as a feedback tool for management and staff, MIS should be useable. The five elements of information technology processing activities that create useable MIS are:

1) *Timeliness* – To facilitate prompt decision-making, an institution's MIS should be capable of providing and distributing current information to appropriate users. Developers should design IT systems to expedite the availability of reports. The system should support timely data collection and prompt editing and correction.

2) *Accuracy* –All information should receive appropriate editing, balancing, and internal control checks to ensure accuracy.

3) *Consistency* – To be reliable, data should be processed and compiled consistently and uniformly. Variations in data collection and reporting methods can distort information and trend analysis.

4) *Completeness* – Decision makers need complete information in a summarized form. Management should design reports to eliminate clutter and voluminous detail to avoid information overload.

5) *Relevance* – Information that is inappropriate, unnecessary, or too detailed for effective decision-making has no value. MIS should be relevant to support its use to management. The relevance and level of detail provided through MIS directly correlates to what the board, executive management, departmental or area mid-level managers, and employees need to perform their jobs.

Sound fundamental principles for MIS review include proper internal controls, operating procedures, safeguards, and audit coverage. When reviewing MIS examiners should consider change controls, documentation and communication of procedures, controls over the underlying data, and audit's coverage of MIS and data management.

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:

1) Potential liability and violations for inaccurate or incomplete information about products, services, and advance pricing presented on the website;
2) Potential access to confidential financial institution or member information if the website server is not properly isolated from the financial institution's internal network;
3) Potential liability for spreading viruses and other malicious code to computers communicating with the institution's website; and

4) Negative public perception should the institution's on-line services be unavailable during normal business hours, 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 institution to higher risk than basic informational websites.

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

1) Security controls for safeguarding member information;
2) Authentication processes necessary to initially verify the identity of new members and authenticate existing members who access electronic banking services;
3) Liability for unauthorized transactions;
4) Losses from fraud if the institution fails to verify the identity of individuals or businesses applying for new accounts or credit on-line;
5) Possible violations of laws or regulations pertaining to privacy, anti-money laundering, anti-terrorism, or the content, timing, or delivery of required disclosures; and
6) 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.

Regulatory Environment

The primary authorities governing or relevant to IT risk management activities of the regulated institutions are set forth below. The examiner is expected to understand the implications and applicability of each of the referenced resources below. In addition, the examiner should ensure that the application of such authorities to an institution has been considered by the institution and its legal counsel.

1) Laws and Statutes pertaining to information technology:

18 USC 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.

2) Rules and Regulations of the Federal Housing Finance Agency (FHFA), which include the following parts and sections relevant to information technology:

12 CFR Part 1235 establishes minimum requirements for a record retention program for all regulated entities (including the Office of Finance). It is intended to further prudent management as well as to ensure that complete and accurate records of each regulated entity and the Office of Finance are readily accessible to FHFA.

12 CFR Part 1236 of FHFA's regulations - Prudential Management and Operations Standards (PMOS) - establishes the PMOS and specifies the possible consequences for any Enterprise, FHLBank or the Office of Finance that fails to operate in accordance with the standards or otherwise fails to comply with this part. Although other standards may apply depending upon the circumstances, the primary PMOS standards are:

Standard 1 – Internal Controls and Information Systems

a) Principle 8 – A regulated entity should have an effective risk assessment process that ensures that management recognizes and continually assesses all material risks, including credit risk, market risk, interest rate risk, liquidity risk, and operational risk.
b) Principle 12 – A regulated entity should have secure information systems that are supported by adequate contingency arrangements.

Standard 8 – Overall Risk Management Processes

a) Principle 1 - Regarding overall risk management processes, the board of directors is responsible for overseeing the process, ensuring senior management are appropriately trained and competent, ensuring processes are in place to identify, manage, monitor and control risk exposures (this function may be delegated to a board appointed committee), approving all major risk limits, and ensuring incentive compensation measures for senior management capture a full range of risks.
b) Principle 2 - Regarding overall risk management processes, the board of directors and senior management should establish and sustain a culture that promotes effective risk management. This culture includes timely, accurate and informative risk reports, alignment of the regulated entity's overall risk

profile with its mission objectives, and the annual review of comprehensive self-assessments of material risks.

c) Principle 7 – A regulated entity should measure, monitor, and control its overall risk exposures, reviewing market, credit, liquidity, and operational risk exposures on both a business unit (or business segment) and enterprise-wide basis.
d) Principle 8– A regulated entity should have the risk management systems to generate, at an appropriate frequency, the information needed to manage risk. Such systems should include systems for market, credit, operational, and liquidity risk analysis, asset and liability management, regulatory reporting, and performance measurement.
e) Principle 9– A regulated entity should have a comprehensive set of risk limits and monitoring procedures to ensure that risk exposures remain within established risk limits, and a mechanism for reporting violations and breaches of risk limits to senior management and the board of directors.

Standard 10 – Maintenance of Adequate Records

a) Principle 2 – A regulated entity should ensure that assets are safeguarded and financial and operational information is timely and reliable.
b) Principle 5 – A regulated entity should ensure that reporting errors are detected and corrected in a timely manner.

3) Rules and Regulations of FHFA, which include the following parts and sections relevant to information technology:

12 CFR Part 1239 of the FHFA regulations addresses powers and responsibilities of FHLBank boards of directors. In particular, 12 CFR 1239.11, Risk Management, 1239.30, Bank Member Products Policy, and 1239.32, Audit Committee, are pertinent.

12 CFR 1239.31 requires the FHLBank board of directors to have a strategic business plan that describes how the business activities of the institution will achieve its mission consistent with 12 CFR Part 1265 (formerly, Part 940) (Core mission activities).

12 CFR 1239.32 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. 12 CFR 1273.9 addresses the audit committee requirements for the Office of Finance.

12 CFR 1274 addresses the preparation and completion of the institution's financial statements, and the distribution of financial information and other information to the Finance Board and the Office of Finance.

4) Advisory Bulletins of the Federal Housing Finance Agency (FHFA) that provide supervisory guidance relating to the topic of information technology are the following:

Advisory Bulletin 2014-05 dated May 19, 2014, provides guidance on cyber risk management.

Advisory Bulletin 2015-06 dated September 21, 2015, provides guidance on IT investment management by the Enterprises.

Advisory Bulletin 2016-04 dated September 29, 2016, provides supervisory expectations for the Enterprises' management of data.

5) Advisory Bulletins of the predecessor Finance Board that provide supervisory guidance relating to the topic of information technology activities are the following:

Advisory Bulletin 03-2 dated February 10, 2003 and Advisory Bulletin 02-3 dated February 13, 2002, provide guidance on specific attributes to be considered by FHLBanks and the Office of Finance 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, 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 (e.g., SSAE 16).

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

6) 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) Development and Acquisition;

c) Information Security;
d) Operations;
e) Outsourcing Technology Services;
f) Retail Payment Systems;
g) Supervision of Technology Service Providers;
h) Wholesale Payment Systems;
i) Supervision of Technology Service Providers; and
j) Business Continuity Planning.

6) 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.

7) Issuances of the Board of Governors of the Federal Reserve System (Board) and FFIEC 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.

8) National Institute of Standards and Technology (NIST) Special Publication 800-12, An Introduction to Computer Security, October 1995. Provides assistance in securing computer-based resources (including hardware, software, and information) by explaining important concepts, cost considerations, and interrelationships of security controls.

9) NIST Special Publication 800-33, Underlying Technical Models for Information Technology Security, December 2001. Provides a description of the technical foundations, termed 'models,' that underlie secure information technology.

10) NIST Special Publication 800-64 (rev. 2), Security Considerations in the System Development Life Cycle, October 2008. Guidance for institutions to consider information security requirements and incorporate automated controls into internally developed programs, or ensure the controls are incorporated into acquired software, before the software is implemented.

11) ***NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment***. Guidance for institutions on the basic technical aspects of conducting information security assessments. Also presents technical testing and examination methods and techniques an organization might use as part of its assessment.

12) ***American Institute of CPAs (AICPA) web site: Service Organization Control Reports (formerly SAS 70 reports).*** Service Organizations Control reports are internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service.

13) ***Federal Risk and Authorization Management Program Penetration Test Guidance Version 1.0.1.*** Guidance for organizations regarding planning, conducting, and analyzing findings of penetration tests.

Issues Specific to the Regulated Entities and Office of Finance

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

The regulated entities and the OF have taken different approaches to how they meet processing needs of the organization. Some have entire in-house applications and infrastructure support, others have a mix of in-house and vendor support and others outsource some of their processing needs. Each board of directors should be aware of how the organization meets its processing needs. Security, infrastructure, applications, and all other critical IT functions must be documented to justify a well secured, safe and sound environment.

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

Examination Guidance

The workprogram for the Information Technology Risk Management Program examination module is detailed below. If this module is included in the examination scope, the examiner must perform worksteps sufficient in coverage to document the basis for conclusions on the quantity of risk and quality of risk management pertaining to this area. Transaction testing is mandatory and the examiner must document sufficient worksteps from Section 4, *Testing,* to support the findings and conclusions from this examination module.

In determining the extent of review and testing to be conducted in completing each analysis, the examiner should take into account any applicable FHFA off-site monitoring or analysis reports, such as analysis of the quality and effectiveness of corporate governance practices, financial condition and performance, economic and housing industry conditions, internal controls, and audit coverage relating to the institution's Information Technology Risk Management Program activities. In addition, where suggested worksteps overlap with other workprograms or analyses undertaken by FHFA economists, financial analysts, accountants, or examiners, the examiner should collaborate with those responsible for completing the corresponding workprograms or analyses to ensure adequate and consistent coverage.

NOTE: Text in (*italics*) referenced in a workstep represents illustrative guidance that serves as suggestions for specific inquiry.

1. Scope of Examination Work Performed

1) Review past reports of examination for outstanding issues or previous problems related to the information technology risk management program.

2) Review applicable FHFA off-site monitoring or analysis reports, and workpapers produced as part of on-going monitoring, related to the information technology risk management program.

3) Assess the status of outstanding Matters Requiring Attention and Violations pertaining to the information technology risk management program.

4) Review internal audit reports for outstanding issues relating to the information technology risk management program.

5) Review minutes of meetings of the board of directors and relevant board and management committees for any issues regarding the information technology risk management program.

6) Review the following for outstanding issues and/or previous problems:

   a) Internal and external audit reports, including SAS 70/SSAE 16/AT 101 reports and correspondence/communication between the institution and auditors;
   b) Independent security tests;
   c) Regulatory, audit, and security reports from service providers;
   d) Any available and applicable reports on organizations providing services to the institution or shared application software reviews (SASR) on software it uses; and
   e) Audit information and summary packages submitted to the board or its audit committee.

   (What have been the historical issues/problems? What were the identified root causes for the historical issues/problems? Was management aware of the historical issues/problems prior to being identified in any of the reports reviewed?)

7) Review management's response to issues raised during the previous examination and during internal and external audits performed since the last examination. *(Was management's response adequate? Was the timing of corrective action appropriate? Did management resolve the root causes of the issues rather than just the specific issue? Are any issues still outstanding?)*

8) Interview management and review the information requested for the examination to understand the institution's current and planned structure, policies, procedures, standards, and practices. The most recent versions of the following may be items that were considered as the requested information:

   a) Pertinent policies and procedures;
   b) Pertinent MIS reports;
   c) Strategic plans;
   d) Operational plans;
   e) Organizational charts;
   f) Network topology maps; and
   g) Résumés of key technology positions.

   (The following are questions that may be considered after interviewing management and reviewing the information requested:

a) *What has changed within the institution since the last examination?*
b) *What has changed outside of the institution [industry, regulatory environment] since the last examination?*
c) *What are the significant changes in business strategy or activities that could affect the IT operations environment?*
d) *Are there any changes to internal operations infrastructure, architecture, information technology environment, or configurations or components?*
e) *Are there any key management or personnel changes?*
f) *Are there any changes in key service providers (transaction processing, website/Internet providers, voice and data communication, back-up/recovery, etc.) or software vendors?*
g) *Are there any changes to any other internal or external factors that could affect the IT environment?*
h) *Are there any changes to products or services delivered to either internal or external users?*
i) *Are there any changes to the network topology including any changes to configuration or components?*
j) *Have there been any significant changes to hardware or software?*
k) *Are there any significant changes to the type or frequency of development, acquisition, or maintenance projects?*
l) *Are there any significant changes to the formality or characteristics of project management techniques?*
m) *Are there any significant changes to internal business processes?*
n) *Are there any plans for significant changes to internal organization structures?*
o) *Have there been any significant volume changes for products/services that are outsourced?*
p) *What is the significance of any change?)*

9) Determine the existence of new threats and vulnerabilities to the institution's information security. *(Have there been any changes in technology employed by the institution? Has management or staff identified any specific threats? Are there any known threats identified by information sharing and analysis organizations, or other non-profit and commercial organizations that may be applicable to the institution? Are there any vulnerabilities raised in security testing reports?)*

10) Review the most recent IT audit reports, plans, and scopes, and any external audit or internal audit outsourcing engagement letters. *(What is management's role in IT*

audit activities? Are there any material changes in the audit program, scope, or schedule related to IT operations? Are there any significant changes in business strategy, activities, or technology that could affect the audit function? Are there any material changes in the audit program, scope, schedule, or staffing related to internal and external audit activities? Are there any other internal or external factors that could affect the audit function?)

11) Assess the quality of the IT audit function. *(What are the IT qualifications of the audit staff? Is the IT audit staff appropriately qualified? What are the practices for ensuring the IT audit staff is appropriately trained and in a timely manner, including maintain continuing education? What are the IT audit policies, procedures, and processes? Are they appropriate for the size and complexity of the regulated entity? Are IT audits appropriately documented to support the conclusions reached? Does the IT audit staff appropriately follow-up on IT issues until they are satisfactorily resolved? How are issues and follow-up reported to an audit committee or similar?)*

12) 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.

a) Obtain copies of:

i) Outsourcing contracts and engagement letters,
ii) Outsourced internal audit reports, and
iii) Policies on outsourced audit.

b) Review the outsourcing contracts/engagement letters and policies.

(The following are questions that may be considered after reviewing this information:

i) Are the expectations and responsibilities for both parties defined in the contract?
ii) Does the contract set the scope, frequency, and cost of work to be performed by the vendor?
iii) Does the contract 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?

iv) Does the contract 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?

v) Does the contract state that audit reports are the property of the institution, that the institution will be provided with any copies of the related workpapers it deems necessary, and that employees authorized by the institution will have reasonable and timely access to the workpapers prepared by the outsourcing vendor?

vi) Does the contract state that any information pertaining to the institution must be kept confidential?

vii) Does the contract specify the period of time that vendors must maintain the workpapers?

viii) If the workpapers are maintained in electronic format, does the contract call for vendors to maintain proprietary software that allows the institution and examiners access to electronic workpapers during a specified period?

ix) Does the contract state that outsourced 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 workpapers and other materials prepared by the outsourcing vendor?

x) Does the contract 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?

xi) Does the contract 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, that they are subject to professional or regulatory independence guidance?)

c) Consider the need to arrange a meeting with the IT audit vendor to discuss the vendor's audit program and determine the auditor's qualifications. *(What are the IT qualifications of the vendor's staff assigned to the institution? Is the vendor's staff appropriately qualified? What are the practices for ensuring the vendor's staff is appropriately trained and in a timely manner? What are the vendor's audit policies, procedures, and processes? Are they appropriate for the size and complexity of the institution? Are the vendor's IT audits appropriately*

documented to support the conclusions reached? Does the vendor's IT audit staff appropriately follow-up on IT issues until they are satisfactorily resolved?)

13) Review previous IT and MIS related examination findings or any reports (including any internal or external audits that targeted MIS) that discuss deficiencies or strengths. Review management's response to those findings. *(What have been the historical issues/problems? What were the identified root causes for the historical issues/problems? Was management aware of the historical issues/problems prior to being identified in any of the reports reviewed? Was management's response adequate? Was the timing of corrective action appropriate? Did management resolve the root causes of the issues rather than just the specific issue? Are any issues still outstanding?)*

14) Discuss with other examiners the usefulness and applicability of any MIS issues that have been reviewed or are pending review. *(Have other examiners identified any issues with MIS that are caused by, or otherwise affect any IT systems?)*

Summarize the work performed in the examination of the institution's information technology risk management program. To the extent there were modifications to the originally planned scope based on concerns identified during the examination, document those changes and the reasons for such changes.

2. Description of Risks

1) Review and assess the degree of reliance on service providers for information processing and technology support including security management. *(How effective have the service providers been? Has each service provider met all service level agreements? If not, why not? When any service level agreement was not met, how effective was the institution's response? How well does the institution oversee each service provider? How quickly is the institution aware of any issues with any service provider?)*

2) Determine if the institution has identified any new IT risks since the last examination. *(How effective is the institution's process for identifying new risks? Are there any new risks that the institution failed to identify?)*

3) Evaluate the institution's analyses of trends in the risk(s) to the organization. *(How effective is the institution's process for identifying and assessing the effects of trends in the risks? Are there any trends in the risks that the institution failed to identify?)*

4) Determine if the institution has undergone any changes that would expose it to new risks, affect its exposure to existing risks, or change the trends of any risks. *(If yes, how effective was the institution's process to identify and assess the effect of the change?)*

5) Determine if there have been any changes in the industry that would expose the institution to any new risks, affect the institution's exposure to risks, or change the trends of any risks. *(If yes, how effective was the institution's process to identify and assess the effect of the change?)*

3. Risk Management

Risk Identification Process

1) Determine how the information flows and maps to the business process for the mainframe, network, and telecommunications environments. *(Has any of this changed from the last examination? Is the institution's key staff knowledgeable of how the information flows?)*

2) Assess the adequacy of the environmental survey(s) and inventory listing(s) or other descriptions of hardware and software. Consider the following:

   a) Computer equipment – vendor and model number;
   b) Network components;
   c) Names, release dates, and version numbers of application(s), operating system(s), and utilities;
   d) Application processing modes;
   e) On-line/real time;
   f) Batch;
   g) Memo post;
   h) Maintenance agreements; and
   i) Recovery time and points objectives.

(Is the information accurate? Is the information complete? How effective is the process to update this information whenever there is a change?)

3) Review and assess systems diagrams and topologies. Determine whether they capture the physical locations and interrelationships of:

   a) Hardware;
   b) Network connections (internal and external);
   c) Modem connections; and
   d) Other connections with outside third parties.

   (Is the information accurate? Is the information complete? How effective is the process to update this information whenever there is a change?)

4) Evaluate the institution's risk assessment process. Obtain documentation of and discuss with senior management the probability of risk occurrence and the effect on IT operations. *(How effective is the institution's risk assessment process? Is it timely? Is it accurate? Is it complete? Does it involve appropriate personnel? Is the documentation timely, accurate, and complete? Is management appropriately knowledgeable of the risk assessment process and the institution's specific risk exposures?)*

5) Review the risk assessment to determine whether the institution has characterized its system properly and assessed the risks to information assets. *(Has the institution identified and ranked information assets (e.g., data, systems, physical locations) according to a rigorous and consistent methodology that considers the risks to customer/member non-public information as well as the risks to the institution? Has the institution identified all reasonably foreseeable threats to the institution's assets? Has the institution analyzed its technical and organizational vulnerabilities? Has the institution considered the potential effect of a security breach on customers/members as well as the institution?)*

6) Determine whether the risk assessment provides adequate support for the security strategy, controls, and monitoring that the institution has implemented. *(Does the risk assessment justify the approach the institution has taken?)*

7) Evaluate the effectiveness of risk assessment process. *(Is it a multidisciplinary and knowledge-based approach? Is it systematic and centrally controlled? Is it an*

integrated process? Are there specific accountable activities? Is it well documented? Does it enhance the knowledge of the institution's risk exposure for those involved? Is it regularly updated? Does the institution identify vulnerabilities and anomalies in a timely fashion? Are corrective actions adequate and conducted timely? Has the institution appropriately identified any unique products and services that involve third-party access requirements? Does the institution effectively update the risk assessment prior to making system changes, implementing new products or services, or confronting new external conditions that would affect the risk analysis? If nothing changes, is the risk assessment still reviewed at least once a year?)

8) Assess the level of oversight and support of the board and management. *(Do the business and technology objectives appropriately align? Is technology-related board reporting of good quality and frequency? What is the level and quality of board-approved project standards and procedures? What are the qualifications of technology managers? Is the technology budget sufficient? What does the board resolution and audit charter state regarding the authority and mission of the IT audit function? Do the minutes of the board or audit committee capture member attendance and supervision of IT audit activities? Do the minutes reflect that the board reviews and approves IT policies, procedures, and processes? Do the minutes reflect that the board approves audit plans and schedules, reviews actual performance of plans and schedules, and approves major deviations to the plan? Do the minutes reflect that the content and timeliness of audit reports and issues presented to and reviewed by the board of directors or audit committee are appropriate? Do the minutes reflect that 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? Do the minutes reflect that the board has demonstrated commitment to ensure the institution maintains appropriate security controls? Do the credentials of board members reflect that the directors responsible for audit oversight have appropriate level of experience and knowledge of IT and related risks? If not, does the board or audit committee bring in outside independent consultants to support their oversight efforts through education and training? Is the composition of the audit committee appropriate considering entity type and complexity?)*

9) Assess the adequacy of management's ability to knowledgeably discuss how technology systems support business activities. *(Is management aware of the specific technology systems that support business activities? Does management understand*

the risks posed by these technology systems? Does management understand the effect of any mitigating actions taken to address the risks?)

10) Determine whether management has implemented and effectively utilizes operational control programs, processes, and tools. *(How effective are the institution's programs, processes, or tools for: Performance management and capacity planning? Project, change, and patch management? Conversion management? Standardization of hardware, software, and their configuration? Logical and physical security? Imaging system controls? Environmental monitoring and controls? Event/problem management?)*

11) Determine whether management has implemented appropriate daily operational controls and processes. *(Are there scheduling systems or activities for efficiency of systems and completion of projects? Are there monitoring tools to detect and preempt system problems or capacity issues? Are there daily processing issue resolution procedures and appropriate escalation procedures? Are media handled securely? Is there secure distribution of output? Does the institution perform a control self-assessment?)*

12) Evaluate the adequacy of contractual terms regarding security responsibilities, controls, and reporting. *(Does the contract clearly state which party is responsible for security controls? Does the contract clearly state which party is responsible for security reporting? Have there been any instances where security responsibilities have been questioned by either party?)*

13) Evaluate the appropriateness of nondisclosure agreements regarding the institution's systems and data. *(Does the institution have nondisclosure agreements on file for all appropriate contracts? What processes are in place to ensure that new contract personnel are aware of nondisclosure agreements? Have there been any incidents where contract personnel have violated a nondisclosure agreement? If so, was the institution's response appropriate?)*

14) Assess the institution's monitoring plans and activities, including both activity monitoring and condition monitoring. *(Are the institution's monitoring plans appropriate given its risk exposure? Is monitoring conducted to ensure the institution receives timely, complete, relevant, accurate, and consistent information?)*

15) Determine if the institution has experienced unauthorized access to sensitive information. *(If so, did the institution conduct a prompt investigation to determine the likelihood the information accessed had been or may be misused? Did the institution appropriately notify FHFA? What steps has the institution taken to ensure a similar breach will not occur again? Are these steps sufficient?)*

16) Determine whether management and department heads are adequately trained and sufficiently accountable for the security of their personnel, information, and systems. *(How often do management and department heads receive security training? How is it communicated to management and department heads that they are accountable for the security of their personnel, information, and systems? Is this method of communication effective?)*

17) Review and assess security guidance and training provided to ensure awareness among employees and contractors, including annual certification that personnel understand their responsibilities. *(How often do employees and contractors receive security training?)*

18) Evaluate the institution's change control process which enables management to effectively control the pace of change to its environment, including the process used to gain assurance that changes to be made will not pose undue risk in a production environment. *(How does the institution determine what IT projects to implement and when to implement them? Is this process effective? Have there been any instances where an IT project failed to meet its implementation schedule? If so, what was the root cause of the failure to meet its implementation schedule? What processes does the institution utilize to minimize risk to the production environment from any IT changes? Does the institution incorporate effective security requirements for the changes? Have there been any instances where appropriate staff was not properly trained prior to an IT change? How effective is the institution's testing process for IT changes? Does the institution perform post-change monitoring? If so, is it timely and relevant?)*

19) Evaluate the adequacy of risk management programs. *(How effective are the risk reporting and monitoring procedures? Does the institution document risk acceptance, mitigation, and transfer strategies?)*

20) Evaluate the outsourcing process for appropriateness given the size and complexity of the institution. *(Is the institution's evaluation of service providers consistent with*

scope and criticality of outsourced services? Does the institution's policy for outsourcing include requirements for ongoing monitoring?)

21) Evaluate the outsourcing requirements definition process. *(Does the institution develop requirements to allow for subsequent use in request for proposals (RFPs), contracts, and monitoring? Does the institution require that all significant actions be documented? Does the institution have processes in place to ensure that the requirements definition is sufficiently complete to support the future control efforts of service provider selection, contract preparation, and monitoring?)*

22) Evaluate the service provider selection process. *(Do RFPs adequately encapsulate the institution's requirements? If so, are the requirements definitions complete and sufficiently detailed to support subsequent RFP development, contract formulation, and monitoring? How effective are the institution's processes to ensure that any differences between the RFP and the submission of the selected service provider are appropriately evaluated? Has the institution taken appropriate actions to mitigate risks arising from requirements not being met? Do the institution's due diligence requirements encompass all material aspects of the service provider relationship, such as the provider's financial condition, reputation (e.g., reference checks), controls, key personnel, disaster recovery plans and tests, insurance, communications capabilities, and use of subcontractors?)*

23) Evaluate the sufficiency of security-related due diligence in service provider research and selection. *(How effective is the institution's process for researching a potential service provider's security controls? How well is the process documented? How well is the actual research documented?)*

24) Evaluate the process for entering into a contract with a service provider. *(Do contracts contain adequate and measurable service level agreements? Does the institution ensure that allowed pricing methods do not adversely affect the institution's safety and soundness, including the reasonableness of future price changes? Does the institution ensure that the rights and responsibilities of both parties are sufficiently detailed? Are there required contract clauses to address significant issues, such as financial and control reporting, right to audit, ownership of data and programs, confidentiality, subcontractors, continuity of service, etc.? Does legal counsel review the contract and any legal issues? Do contracts adequately address any inducement concerns?)*

25) Evaluate the institution's use of user groups and other mechanisms to monitor and influence the service provider. *(Does the institution participate in any user groups? What other means does the institution utilize to leverage best practices that other customers of service providers may have implemented?)*

26) Assess the level of risk present in outsourcing arrangements. *(What are the types and volumes of functions outsourced? What are the types and characteristics of service providers, including, where appropriate, unique risks inherent in foreign-based service provider arrangements? What are the types of technology used by service providers?)*

27) Determine whether management effectively oversees and monitors any significant data processing services provided by technology service providers. *(Does management directly audit the service provider's operations and controls, employ the services of external auditors to evaluate the servicer's controls, or receive sufficiently detailed copies of audit reports from the technology service provider? Does management adequately review all reports to ensure the audit scope was sufficient and that all deficiencies are appropriately addressed? Are the key service level agreements and contract provisions appropriate? Is the financial condition of the service provider sound? Does the institution obtain and review the service provider's disaster recovery program and testing results? Does the institution obtain and review the service provider's information security policy? Does the institution obtain and review the service provider's insurance coverage? How does the institution ensure the appropriate risk mitigation of a service provider's use of subcontractors? How does the institution ensure the appropriate risk mitigation of a service provider's relationships with any foreign third-parties? How does the institution ensure the service provider appropriately responds to changes to the institution's external environment including competitors and industry trends?)*

28) Determine the existence of timely and formal follow-up and reporting on management's resolution of identified IT problems or weaknesses. *(Does management take appropriate and timely action on IT audit findings and recommendations? Does audit or management report progress and effectiveness of corrective action to the board of directors or its audit committee? Does IT audit review or test management's statements regarding the resolution of findings and recommendations? Is there any discrepancy between management reports of outstanding IT audit items and items contained within audit reports? Does*

management appropriately correct the root causes of all significant deficiencies noted in the audit reports?)

Organizational Structure

1) Evaluate organizational responsibilities to assess the effectiveness of board and management. *(Has the board and management clearly defined and appropriately assigned responsibilities? Has the board and management appropriately assigned security, audit, and quality assurance personnel to technology-related projects? Has the board and management established appropriate segregation-of-duty or compensating controls? Has the board and management established appropriate project, technology committee, and board reporting requirements?)*

2) Assess the effectiveness of the operational organization structure for technology operations in supporting the business activities of the institution. *(Does the organizational structure promote segregation-of-duty or compensating controls?)*

3) Assess the size and quality of the institution's security staff. *(Does the security staff have appropriate security training and certifications? Are the staffing levels adequate? Do the staffing levels account for the effect of any turnover? To what extent does the institution incorporate background investigations? Is the security staff afforded adequate time to perform security responsibilities?)*

4) Assess whether management has implemented appropriate human resource management. *(Is the organizational structure appropriate for the institution's business lines? Does management conduct ongoing background checks for all employees in sensitive areas? Are segregation and rotation of duties sufficient? Does management have policies and procedures to minimize excessive employee turnover? Are there appropriate policies and controls concerning termination of operations personnel?)*

5) Review the appropriateness of the organizational unit and personnel responsible for performing the functions of a security response center. *(Are the personnel in the security response center appropriately trained?)*

6) Determine that the institution utilizes sufficient expertise to perform its monitoring and testing. *(What are the qualifications of personnel performing monitoring and testing? Are they appropriately trained?)*

7) For independent tests, evaluate the degree of independence between the persons testing security from the persons administering security. *(Is there segregation-of-duty? Are there compensating controls?)*

8) Determine whether security responsibilities are appropriately apportioned among senior management, front-line management, IT staff, information security professionals, and other staff, recognizing that some roles must be independent from others. *(How are security responsibilities allocated? Are the allocations appropriate?)*

9) Determine whether the individual or department responsible for ensuring compliance with security policies has sufficient position and authority within the organization to implement the corrective action. *(Within the organizational structure, who is responsible for ensuring compliance with security policies? Is this structure effective? Have there been instances where the responsible party has not had adequate authority to implement corrective actions?)*

10) Determine if the institution has established an Office of Minority and Women Inclusion, or has designated an office of the institution that shall be responsible for carrying out all matters of the institution relating to diversity in management, employment, and business activities, including those pertaining to IT risk management. *(What is the institution's process to ensure diversity in management, employment, and business activities?)*

Policy and Procedure Development

1) Review and assess policies, procedures, and standards as they apply to the institution's IT environment and controls. *(Are the written policies, procedures, and standards appropriate for the regulated entity's size and complexity? How effective and timely is the regulated entity's process to update policies, procedures, and standards after a change warrants an update? Does the regulated entity have a process to regularly review the policies, procedures, and standards even if no changes have been made to the documents? Does the regulated entity obtain employee certification that they have read and understood the policies?)*

2) Review and assess security policies and standards to ensure that they sufficiently address the appropriate security issues considering the risks identified by the institution. *(Do the security policies and standards appropriately address:*

Authentication and authorization; acceptable-use policy that dictates the appropriate use of the institution's technology including hardware, software, networks, and telecommunications; administration of access rights at enrollment, when duties change, and at employee separation; authentication mechanisms including token-based systems, digital certificates, or biometric controls and related enrollment and maintenance processes as well as database security; network access; security domains; perimeter protections including firewalls, malicious code prevention, outbound filtering, and security monitoring; application access controls; remote access controls including wireless, VPN, modems, and Internet-based; host systems; secure configuration (hardening); operating system access; application access and configuration; malicious code prevention; logging; monitoring and updating; user equipment; physical controls over access to hardware, software, storage media, paper records, and facilities; encryption controls; software development and acquisition, including processes that evaluate the security features and software trustworthiness of code being developed or acquired, as well as change control and configuration management; personnel security; media handling procedures and restrictions, including procedures for securing, transmitting and disposing of paper and electronic information; service provider oversight including contractual notification requirements; business continuity; incident response center functions, including monitoring, classification, escalation, and reporting; and insurance?)

3) Evaluate the institution's policies and program for responding to unauthorized access to information. *(Are the policies appropriate? Has the institution experienced any instances where there was a suspected unauthorized access to information? If so, did the institution respond in compliance with policy? Was the response appropriate? Was there a post-response analysis to determine if any changes to policies or procedures were warranted?)*

4) Review the policies regarding periodic ranking of service providers by factors such as risk or criticality for decisions regarding the intensity of monitoring (i.e., risk assessment). *(Do the policies include objective criteria? Do the policies support consistent application? Do the policies consider the degree of service provider support for the institution's strategic and critical business needs? Do the policies specify subsequent actions when rankings change?)*

5) Determine if the institution has developed and implemented standards and procedures to ensure, to the maximum extent possible, the inclusion and utilization of minorities and women, and minority- and women-owned businesses in all business and activities

of the institution at all levels, including IT risk management. *(Are the institution's standards and procedures effective? What types of reports are produced for management? What are the trends in the number of minorities and women included and utilized in all business activities?)*

Risk Metrics

Where metrics are used, evaluate the standards used for measurement, the information measures and repeatability of measured processes, and appropriateness of the measurement scope. *(Are the metrics accurate, timely, complete, relevant, and consistent?)*

Reporting

1) Assess operations management MIS reports. *(Is the frequency of monitoring or reporting continuous or periodic? Is the information accurate, timely, complete, relevant, and consistent? Do reports present response times and throughput? Do reports present system availability and/or down time? Do reports present number, percentage, type, and causes of job failures? Do reports present average and peak system utilization, trends, and capacity? Do reports provide the status of software development/maintenance activities? Do reports present system use and planning efforts?)*

2) Evaluate the adequacy of information used by the security response center. *(Does the security response center obtain external information on threats and vulnerabilities? Does the security response center obtain internal information related to controls and activities?)*

Internal Audit

1) Determine if the internal audit staff is adequate in number and is technically competent to accomplish its mission. *(Are internal audit personnel qualifications appropriately aligned with responsibilities detailed in their respective job descriptions? Is staff competency commensurate with the technology in use at the regulated entity? What are the trends in internal audit staffing? Do the trends suggest that the regulated entity may experience inadequate number or competencies within the internal audit personnel?)*

2) Determine if the reporting process for the internal IT audit is independent in fact and in appearance. *(Have there been any instances where persons outside of the audit function have unduly influenced what is reported to the board or audit committee?)*

3) Review the internal audit organization structure for independence and clarity of the reporting process. *(Does the internal audit manager report functionally to a senior management official (i.e., CFO, controller, or similar officer)? Is the internal audit manager's compensation and performance appraisal being done by someone other than the board or audit committee? Are auditors responsible for operating a system of internal controls or actually performing operational duties or activities?)*

4) Determine the adequacy of the overall internal audit plan in providing appropriate coverage of IT risks. *(Is the internal audit plan consistent with the institution's risk assessment? Is the internal audit plan consistent with the institution's products and services delivered to either internal or external users? Does the internal audit plan effectively address the loss or addition of key personnel? Does the internal audit plan effectively address technology service providers and software vendor listings?)*

5) Assess the adequacy of internal audit policies and standards as they relate to IT audits. *(Are the policies and standards appropriately risk-based? Do the policies and standards appropriately address the format and content of reports, distribution of reports, resolution of internal audit findings, format and contents of workpapers, and security over audit materials?)*

6) Determine the adequacy of internal audit's risk analysis methodology in prioritizing the allocation of audit resources and formulating the internal IT audit schedule. *(Is the internal audit universe well defined? For the entire internal audit universe, are the audit schedules and audit cycles reasonable? Are the internal audit schedules being consistently met? Does the methodology 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? How effective is the process for assessing and documenting risk and control factors and its application in the formulation of internal audit plans, resource allocations, internal audit scopes, and internal audit cycle frequency?)*

7) Determine the adequacy of the scope, frequency, accuracy, and timeliness of IT-related internal audit reports. *(Do internal audit reports and workpapers comply with board and audit committee-approved standards? Is the internal auditor's evaluation*

of IT controls commensurate with FHFA's evaluation during this examination? Is the scope of the internal auditor's work appropriate for the institution's size, the nature and extent of its activities, and its risk profile? Do the workpapers disclose that specific program steps, calculations, or other evidence support the procedures and conclusions set forth in the reports? Do the internal auditors accurately identify and consistently report weaknesses and risks? Are internal audit reports timely, relevant, accurate, complete, and consistent?)

8) Determine the extent of internal audit's participation in application development, acquisition, and testing, as part of the institution's process to ensure the effectiveness of internal controls. *(Does the institution have an effective methodology to notify the internal auditor of proposed new applications, major changes to existing applications, modifications/additions to the operating system, and other changes to the data processing environment? Is internal audit effective and independent while participating in the systems development life cycle? Is internal audit effective and independent while reviewing major changes to applications or the operating system? Is internal audit effective and independent while updating internal audit procedures, software, and documentation for changes in the systems or environment? Is internal audit effective and independent while recommending changes to new proposals or to existing applications and systems to address audit and control issues?)*

9) If the internal IT audit function, or any portion of it, is outsourced to external vendors, determine its effectiveness and whether the institution can appropriately rely on it. *(Does the outsourcing arrangement maintain or improve the quality of the internal audit function and the institution's internal controls? How appropriate are the performance and contractual criteria for the audit vendor and any internal evaluations of the audit vendor? Are outsourced audit reports and audit workpapers adequate and prepared in accordance with the audit program and the outsourcing agreement? Do workpapers disclose that specific program steps, calculations, or other evidence support the procedures and conclusions set forth in the audit reports? Is the scope of the outsourced audit procedures adequate? Do 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? Does management or the audit vendor revise the scope of outsourced audit work appropriately when the institution's environment, activities, risk exposures, or systems change significantly? Does the board or audit committee demonstrate commitment that the institution effectively manages any outsourced audit function? Does the board or audit committee perform sufficient due*

diligence to satisfy themselves of the audit vendor's competence and objectivity before entering the outsourcing arrangement? Does the institution have an adequate contingency plan to reduce any lapse in internal audit coverage, particularly coverage of high-risk areas, in the event the outsourced audit relationship is terminated suddenly?)

Information Technology

1) Assess the adequacy of the documentation that describes the technology systems and operations (enterprise architecture) in place to support business activities. *(Does the institution have an effective process to ensure that the documentation is accurate, complete, timely, relevant, and consistent? Is the documentation routinely reviewed?)*

2) Determine the extent of network connectivity internally and externally, and the boundaries and functions of security domains. *(Does the institution effectively account for internal and external network connectivity, and boundaries and functions of security domains in its risk assessment?)*

3) Evaluate management's ability to control security risks given the frequency of changes to the computing environment. *(Have there been any instances where there has been a security breach? If so, how effective was managements' response?)*

4) Evaluate security maintenance requirements and the extent of historical security issues with installed hardware/software. *(Does the institution have an effective process to ensure that it remains current with all security patching requirements? Is the institution current with security patches for hardware and software? What types of reports are produced to validate compliance with security requirements?)*

5) Assess the design of protective measures used to define, identify, and classify security vulnerabilities, such as vulnerability scans and penetration tests. *(Are the parties that perform the scans/tests sufficiently independent, i.e. not responsible for the design, installation, maintenance, and operation of any of the tested systems? Does the institution's security risk assessment inform the frequency of the scans and tests? Are the scopes and strategies of the scans and tests commensurate with the institution's technology environment? Did the institution adequately address findings from the scans/tests? If not, does the institution have an adequate plan for remediation?)*

6) Determine whether external standards are used as a basis for the security program, and the extent to which management tailors the standards to the institutions' specific

circumstances. *(If external standards are used, are they appropriate? What process does the institution use to determine which external standards to adopt? How effective is the process to tailor external standards for the institution's specific circumstances?)*

7) Assess the institution's enterprise-wide data storage methodologies. *(Has the institution appropriately planned its data storage process? Are suitable standards and procedures in place to guide the function? How appropriate are the assumptions used for forecasting storage needs? Have there been any instances where the institution did not have enough storage, or nearly ran out of storage? If so, how effective was managements' response? What changes has the institution implemented to prevent a similar scenario from occurring again?)*

8) Evaluate whether management has appropriately planned its data back-up process, and whether suitable policies, standards, and procedures are in place to guide the function. *(Do back-up policies address all critical hardware and software, including personnel workstations? Does the process appropriately address data and program files? Does the policy appropriately address records disposition from back-up storage media? Has the institution assessed if back-up processes are necessary for portable devices (e.g., cell phones, tablets, thumb drives, external hard drives)? Does the institution have an appropriate back-up tape rotation process? How appropriate is the schedule and frequency of back-ups? Does the institution utilize appropriate off-site storage of back-up material? Is the off-site storage location a suitable distance from the primary processing site? Are there appropriate physical controls at the off-site storage location? Does the institution have an appropriate process for regularly testing data and program back-up media to ensure the back-up media is readable and that restorable copies have been produced?)*

9) Assess the institution's inventory of data and program files (operating systems, purchased software, in-house developed software) stored on and off-site. *(Is the inventory accurate? Does the inventory include off-site back-up material? How effective is management's process for updating and maintaining this inventory? Does the institution periodically perform physical audits for the items on the inventory?)*

10) Review and assess the environmental controls and monitoring capabilities of the technology operations. *(Do the controls and monitoring address electrical power, telecommunication services, heating, ventilation, air conditioning, water supply, computer cabling, smoke detection, fire suppression, water leaks, and preventive maintenance?)*

11) Assess whether appropriate controls exist to address telecommunication operations risk. *(Is there proper alignment of telecommunication architecture and process with the strategic plan? Is there appropriate monitoring of telecommunications operations such as downtime, throughput, usage, and capacity utilization? Does the institution obtain assurance of adequate availability, speed, and bandwidth/capacity?)*
12) Determine whether there are adequate security controls around the telecommunications environment. *(Are there controls that limit access to wiring closets, equipment, and cabling to authorized personnel only? Is the telecommunications documentation adequate and secured? Are there appropriate telecommunication change control procedures? Is there controlled access to internal systems through authentication?)*

13) Assess whether the telecommunications system has adequate resiliency and continuity preparedness. *(Does the institution have an appropriate process to ensure the telecommunications system has suitable capacity? Does the institution appropriately address telecommunications provider diversity? Does the institution appropriately address telecommunications cabling route diversity, and multiple paths and entry points? Does the institution appropriately address redundant telecommunications to diverse telephone company central offices?)*

14) Assess the institution's use of document imaging solutions. *(How effective was the institution's analysis of document imaging needs? Did the analysis include any OCR (optical character recognition) needs? Did the analysis include any encryption or other security needs? Did the analysis include a quality of image threshold assessment for the image? Does the institution periodically review document imaging requirements to determine if any changes need to be incorporated? Does the institution have an effective quality assurance process that tests whether document images are in compliance with the institution's needs?)*

15) Evaluate the adequacy of imaging system controls. *(Do the controls address physical security, data security, documentation, error handling, program change procedures, system recoverability, and vital records retention? Do the controls provide assurance that all hard copy document page inputs equate to the same number of imaged pages? Do the controls address electronic images transferred from imaging systems to other media? Do the controls adequately address the destruction of hard copy source documents after being scanned through the imaging system?)*

16) Assess to what degree imaging has been included in the business continuity planning process. *(Has the institution assessed if any business units are reliant upon imaging systems for critical business functions? How often does the institution reevaluate reliance upon imaging systems?)*

17) Asses the institution's critical system data flow depictions and topology. *(Is the information accurate? Is the information presented in a manner that is understandable by the users who need to rely upon it? How timely are any necessary changes made? How often is the information reviewed?)*

18) Evaluate the adequacy of automated tools to support secure configuration management, security monitoring, policy monitoring, enforcement, and reporting. *(How effective is the institution's analyses for selecting these particular tools? How often are the requirements reviewed to ascertain if these tools continue to be the best choice? Does the institution have an appropriate process to ensure that necessary updates or patches to the tools are implemented in an effective and timely manner?)*

19) Evaluate the adequacy of development activities. *(Does the institution have adequate development standards and controls? Do the standards and controls adequately address the design, development, testing, and implementation phases? How effectively does the institution adhere to the development standards and controls? Does the institution have a process to ensure appropriate testing of development activities? Have there been any instances where changes were implemented into a production environment that included defects that needed subsequent changes? If so, what steps were taken to minimize the risk of a similar scenario from occurring again? Are there effective change implementation procedures? Does the institution have a process to ensure an adequate contingency plan is in place for any failed implementations? Has the institution implemented effective project management methodologies? Are the project managers' experience and qualifications commensurate with the institution's volume and complexity of IT projects? Does the institution utilize adequate project plans? Do the project plans include clearly defined phase expectations, phase acceptance criteria, security and control requirements, testing requirements, training, implementation, and documentation requirements? Does the institution have an effective quality assurance program? Is the risk management program effective? Are the procedures for project requests and approvals adequate? Does the institution conduct feasibility studies as appropriate? How effective are project change controls? Does the institution include appropriate*

organizational personnel throughout the project's life cycle? How effective are the project communication and reporting procedures? Does the institution have an appropriate process to ensure the accuracy, effectiveness, and control of project management tools?)

20) Assess the adequacy of acquisition activities. *(Does the institution have adequate acquisition standards and controls? Do the standards and controls adequately address the design, development, testing, and implementation phases? How effectively does the institution adhere to the acquisition standards and controls? Does the institution have a process to ensure appropriate testing of acquisition activities? Have there been any instances where changes were implemented into a production environment that included defects that needed subsequent changes? If so, what steps were taken to minimize the risk of a similar scenario from occurring again? Are there effective change implementation procedures? Does the institution have a process to ensure an adequate contingency plan is in place for any failed implementations? Has the institution implemented effective project management methodologies? Are the project managers' experience and qualifications commensurate with the institution's volume and complexity of IT projects? Does the institution utilize adequate project plans? Do the project plans include clearly defined phase expectations, phase acceptance criteria, security and control requirements, testing requirements, training, implementation, and documentation requirements? Does the institution have an effective quality assurance program? Is the risk management program effective? Are the procedures for project requests and approvals adequate? Does the institution conduct feasibility studies as appropriate? How effective are project change controls? Does the institution include appropriate organizational personnel throughout the project's life cycle? How effective are the project communication and reporting procedures? Does the institution have an appropriate process to ensure the accuracy, effectiveness, and control of project management tools? Does the institution have adequate standards that require request-for-proposals and invitations-to-tender to include well-detailed security, reliability, and functionality specifications; well-defined performance and compatibility specifications; and well-defined design and development documentation requirements? Are there adequate standards that require thorough reviews of vendors' financial condition and commitment to service; and thorough reviews of contracts and licensing agreements prior to signing? Does the institution have a process to ensure that contract and licensing provisions adequately address performance assurances; software and data security provisions; and source-code accessibility/ escrow assertions?)*

21) Assess the adequacy of maintenance project management standards, methodologies, and practices. *(Does the institution have adequate maintenance standards and controls? Are the procedures for project change requests and approvals adequate? Does the institution have a process to ensure appropriate testing of maintenance activities? Have there been any instances where changes were implemented into a production environment that included defects that needed subsequent changes? If so, what steps were taken to minimize the risk of a similar scenario from occurring again? Are there effective change implementation procedures? Does the institution have a process to ensure an adequate contingency plan is in place for any failed implementations? Are there effective change documentation procedures? Are there effective change notification procedures? Are there effective library controls? Are there effective utility program controls? How effectively does the institution adhere to the maintenance standards and controls?)*

22) Evaluate the effectiveness of any conversion projects. *(Did the institution perform an appropriate analysis and implement appropriate lessons learned comparing initial budgets and projected time lines against actual results? Are project management and technology committee reports effective? Does the institution routinely review and appropriately react to testing documentation and after-action reports? Does the institution routinely review and appropriately react to conversion after-action reports?)*

23) Assess the adequacy of quality assurance programs. *(Has the board demonstrated a willingness to provide appropriate resources to quality assurance programs? Are there adequate quality assurance procedures? Are the deliverables of each project, and project phase, including the validation of initial project assumptions and approvals, appropriately assured? Are quality assurance procedures appropriately scalable? Are the procedures appropriately tailored to match the characteristics of the project? Are quality assurance standards measurable? Are deliverables assessed against predefined standards and expectations? Does the institution adhere to problem-tracking standards that require appropriate problem recordation; appropriate problem reporting; appropriate problem monitoring; and appropriate problem correction? Does the institution adhere to testing standards that require the use of predefined, comprehensive test plans; the involvement of end users; the documentation of test results; the prohibition against testing in production environments; and the prohibition against testing with live data? Does the institution have a process to ensure effective testing programs regarding the accuracy of*

programmed code; the inclusion of expected functionality; the interoperability of applications and network components; and the independence of quality assurance personnel?)

24) Assess the adequacy of program change controls. *(Does the institution have a process to ensure routine and emergency program-change standards that require appropriate request and approval procedures; testing procedures; implementation procedures; backup and backout procedures; documentation procedures; and notification procedures? Are there appropriate controls that restrict the unauthorized movement of programs or program modules/objects between development, testing, and production environments? Are there appropriate controls (such as policy prohibitions, monitoring of use, and logical access controls) that restrict the unauthorized use of utility programs? Are there appropriate library controls (such as logical access controls on all libraries or objects within libraries; and automated library controls that restrict library access and produce reports that identify who accessed a library, what was accessed, and what changes were made) that restrict unauthorized access to programs outside an individual's assigned responsibilities? Are there appropriate version controls that facilitate the appropriate retention of programs, and program modules/objects, revisions, and documentation?)*

25) Evaluate the sufficiency of, and adherence to, patch-management standards and controls. *(Does the institution have a process to ensure that there are detailed hardware and software inventories, appropriate patch identification procedures, effective patch evaluation procedures, appropriate patch request and approval procedures, adequate patch testing procedures, effective backup and backout procedures, effective patch implementation procedures, and adequate patch documentation?)*

26) Assess the adequacy of documentation controls by evaluating the sufficiency of, and adherence to, documentation standards. *(Does the institution have a process to ensure the appropriate assignment of documentation/custodian responsibilities, assignment of document authoring and approval responsibilities, establishment of standardized document formats, and establishment of appropriate documentation library and version controls?)*

27) Assess the quality of application documentation. *(Does the institution have appropriate application design and coding standards? Does the institution adhere to*

the standards? Do applications have accurate descriptions? Are application designs well documented? Are application source-code listings (or in the case of object-oriented programming: object listings) complete and accurate? Do applications follow routine naming conventions (or in the case of object-oriented programming: object naming conventions)? How appropriate and timely are application operator instructions and user manuals?)

28) Assess the quality of any open source-code system documentation. *(Does the institution have appropriate system design and coding standards? Does the institution adhere to the standards? Do systems have accurate descriptions? Are system designs well documented? Are system source-code listings (or in the case of object-oriented programming: object listings) complete and accurate? Do system source-codes follow routine naming conventions (or in the case of object-oriented programming: object naming conventions)? How appropriate and timely are system operation instructions?)*

29) Assess the quality of project documentation. *(Does the institution have appropriate project documentation standards? Does the institution adhere to the standards? Does the institution appropriately document feasibility studies? Does the institution appropriately document all phases of projects (initiation phase, planning phase, design phase, development phase, testing phase, and implementation phase)? Does the institution appropriately document post-implementation reviews?)*

30) Assess the security and integrity of system and application software. *(Does the institution have adequate quality assurance and testing programs? Does the institution have adequate security and internal-control design standards? Does the institution have adequate program change controls? Does the institution have adequate involvement by audit and security personnel in software development and acquisition projects? Does the institution have adequate internal and external security and control audits?)*

31) Assess the ability of information technology solutions to meet the needs of the end users. *(What types of processes does the institution employ to ascertain the satisfaction of end users with technology solutions? What is the level of satisfaction? Do interviews with end-user personnel indicate their business needs are being met?)*

32) Assess the extent of end-user involvement in the system development and acquisition process. *(Does the institution have documentation to support the level of end-user*

involvement in the system development and acquisition process? Is the level of involvement appropriate?)

Compliance

1) Determine whether management is monitoring and enforcing compliance with regulations and other standards, including if imaging processes have been reviewed by legal counsel. *(Are there any instances of violations? If so, what are the root causes of the violations? How should internal controls be strengthened to ensure there are no future regulatory violations?)*

2) Specifically assess compliance with 12 CFR Part 1236 Prudential Management and Operating Standards of FHFA's regulations (these apply to the FHLBanks and the Enterprises, but not to the Office of Finance). In particular:

   a) Standard 1 – Internal Controls and Information Systems

      i) Principle 8 - A regulated entity should have an effective risk assessment process that ensures that management recognizes and continually assesses all material risks, including credit risk, market risk, interest rate risk, liquidity risk, and operational risk. *(Based upon the findings from this examination, does the regulated entity comply with the requirements of this Principal?)*
      ii) Principle 12 – A regulated entity should have secure information systems that are supported by adequate contingency arrangements. *(Based upon the findings from this examination, does the regulated entity comply with the requirements of this Principle?)*

   b) Standard 8 – Overall Risk Management Processes

      i) Principle 1 - Regarding overall risk management processes, the board of directors is responsible for overseeing the process, ensuring senior management are appropriately trained and competent, ensuring processes are in place to identify, manage, monitor and control risk exposures (this function may be delegated to a board appointed committee), approving all major risk limits, and ensuring incentive compensation measures for senior management capture a full range of risks. *(Based upon the findings from this examination, does the regulated entity comply with the requirements of this Principle?)*

ii) Principle 2 - Regarding overall risk management processes, the board of directors and senior management should establish and sustain a culture that promotes effective risk management. This culture includes timely, accurate and informative risk reports, alignment of the regulated entity's overall risk profile with its mission objectives, and the annual review of comprehensive self-assessments of material risks. *(Based upon the findings from this examination, does the regulated entity comply with the requirements of this Principle?)*

iii) Principle 7 - A regulated entity should measure, monitor, and control its overall risk exposures, reviewing market, credit, liquidity, and operational risk exposures on both a business unit (or business segment) and enterprise-wide basis. *(Based upon the findings from this examination, does the regulated entity comply with the requirements of this Principle?)*

iv) Principle 8 - A regulated entity should have the risk management systems to generate, at an appropriate frequency, the information needed to manage risk. Such systems should include systems for market, credit, operational, and liquidity risk analysis, asset and liability management, regulatory reporting, and performance measurement. *(Based upon the findings from this examination, does the regulated entity comply with the requirements of this Principle?)*

v) Principle 9 - A regulated entity should have a comprehensive set of risk limits and monitoring procedures to ensure that risk exposures remain within established risk limits, and a mechanism for reporting violations and breaches of risk limits to senior management and the board of directors. *(Based upon the findings from this examination, does the regulated entity comply with the requirements of this Principle?)*

c) Standard 10 – Maintenance of Adequate Records

i) Principle 2 - A regulated entity should ensure that assets are safeguarded and financial and operational information is timely and reliable. *(Based upon the findings from this examination, does the regulated entity comply with the requirements of this Principle?)*

ii) Principle 5 - A regulated entity should ensure that reporting errors are detected and corrected in a timely manner. *(Based upon the findings from this examination, does the regulated entity comply with the requirements of this Principle?)*

3) Evaluate the process used to monitor and enforce policy compliance (e.g., granting and revocation of user rights). *(Does the institution have an appropriate process to ensure effective monitoring and enforcement of policy compliance?)*

4. Testing

1) 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 policies, practices, and procedures concerning that project. Determine how management determines they are in satisfactory compliance. Consider if major projects have control points before releasing additional funding.

2) Select a recent outsourced project and evaluate if management has implemented sufficient controls to ensure data protection.

3) 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.

4) 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 workflows or lack of security points.

5) Obtain and review management asset inventories. Evaluate the process used to maintain the inventories current.

6) Select 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.

7) 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.

8) Obtain a list of all information security reports that are completed on a regular basis, and evaluate the effectiveness of the information and management's action(s) to address risks identified.

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

   a) Timeliness,
   b) Accuracy,
   c) Consistency,
   d) Completeness, and
   e) Relevance.

5. Conclusions

1) Summarize conclusions for all examination work performed, including work performed by other FHFA staff as it relates to the institution's information technology risk management program. Develop a memorandum describing the risks to the institution resulting from the information technology risk management practices and the institution's management of those risks. The memorandum should clearly describe the basis of conclusions reached and summarize the analysis completed. Within the memorandum, discuss the types of risk the institution is exposed to (e.g., market, credit, operational); the level of risk exposure; the direction of risk (stable, decreasing, increasing); and the quality of risk management practices (strong, adequate, weak). A memorandum must be prepared irrespective of whether the examiner's assessment is positive or negative.

2) Conclude on the responsiveness to previous examination findings. Evaluate the adequacy of the institution's response to previous examination findings and concerns.

3) Develop findings and prepare findings memorandums, as appropriate. Based on examination work performed, develop findings communicating concerns identified during the examination. Findings should identify the most significant risks to the institution and the potential effect to the institution resulting from the concerns identified. Such documents should describe a remediation plan specifying the appropriate corrective action to address examination concerns and establish a

reasonable deadline for the institution to remediate the finding. Communicate preliminary findings to the EIC, other interested examiners, and senior FHFA staff, as appropriate. Discuss findings with institution personnel to ensure the findings are free of factual errors or misrepresentations in the analysis.

4) Develop a list of follow-up items to evaluate during the next annual examination. In addition to findings developed in the steps above, include concerns noted during the examination that do not rise to the level of a finding. Potential concerns include issues the institution is in the process of addressing, but require follow-up work to ensure actions are completed appropriately. In addition, potential concerns should include anticipated changes to the institution's practices or anticipated external changes that could affect the institution's future oversight of the information technology risk management program.

Workprogram

1. Scope of Examination Work Performed

Workpapers must document the examination activities undertaken to evaluate potential risks related to the information technology risk management.

2. Description of Risks

- Identify areas of concern related to the information technology risk management
- Assess current risks and trends in the risk to the organization emanating from the information technology area
- Evaluate changes within the organization or industry affecting risk
- Evaluate the institution's own risk-identification practices and conclude on their adequacy

3. Risk Management

- Assess and conclude on the adequacy of the institution's risk identification process
- Assess and conclude on the overall adequacy of internal controls, including an evaluation of:
    - The institution's organizational structure
    - Policy and procedure development for this area
    - Appropriateness of risk metrics established in this area
    - Reporting by management and the board
- Assess and conclude on the internal and external audit of risks
- Assess and conclude on the adequacy of the institution's efforts to ensure:
    - Compliance with laws, regulations and other supervisory guidance
    - Compliance with the organization's policies and procedures

4. Testing

- Complete testing, as appropriate, to assess adherence with examination standards

5. Conclusions

- Summarize conclusions for all examination work performed related to the Information Technology Risk Management Program
    - Conclude on the level of risk to the institution
    - Include an assessment of the adequacy of an institution's monitoring of risk and establishment of internal controls to mitigate risk
- Conclude on responsiveness to examination findings from previous examinations
- Develop examination findings, as appropriate
- Identify areas requiring follow-up examination activities or monitoring