Federal Financial Institutions Examination Council

FFIEC

Operations OPS

JULY 2004

IT Examination Handbook

Table of Contents

Introduction

This booklet is one in a series that comprise the Federal Financial Institutions Examination Council (FFIEC) Information Technology Handbook (IT Handbook). It provides guidance to examiners and financial institutions [1] on risk management processes that promote sound and controlled operation of technology environments. Information is one of the most important assets of an institution, and information technology (IT) operations should process and store information in a timely, reliable, secure, and resilient manner. This booklet addresses IT operations in the context of tactical management and daily delivery of technology to capture, transmit, process, and store the information assets and support the business processes of the institution. The examination procedures contained in this booklet assist examiners in evaluating an institution's controls and risk management processes relative to the risks of technology systems and operations that reside in, or are connected to the institution. This booklet rescinds and replaces Chapters 13 "Operations" and 17 "Document Imaging" of the 1996 FFIEC Information Systems Examination Handbook.

The evolving role technology plays in supporting the 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 include distributed environments, integrated applications, telecommunication options, Internet connectivity, and an array of computer operating platforms. As the complexity of technology has grown, the financial services industry has increased its reliance on vendors, partners, and other third parties for a variety of technology solutions and services. Institutions will frequently operate or manage various IT resources from these third-party locations.

The guidance in this booklet covers the risks and expected controls in IT operations and across the institution. It also emphasizes that risks involve more than IT technology and that controls include sound processes and well-trained people. Effective support and delivery from IT operations has become vital to the performance of most critical business lines in the institution. Therefore, IT management should work with business line management and end users to determine and deliver appropriate service levels.

Each section of the booklet begins with an "Action Summary" that summarizes the major themes in that section. The action summary is not a substitute for reading the entire booklet; however examiners can use the action summaries to review the most important points discussed in each section.

The concepts and principles in this booklet are applicable to complex core operations at centralized data center locations, distributed operations at lines of business, microcomputers used as stand alone processors, support functions, and affiliates under the enterprise umbrella. They are also applicable to smaller or less complex technology operations at community banks. The FFIEC member agencies expect institution management to implement controls across the institution to mitigate IT operations-related risk consistent with the nature and complexity of the institution's technology environment.

Institutions developing or reviewing their operational controls, procedures, standards, and processes have a variety of third-party sources to draw on for additional guidance, including outside auditors, consulting firms, insurance companies, industry and trade groups, and other technology professionals. In addition, many national and international organizations have developed guidelines and best practices. These guidelines and best

practices provide benchmarks institutions can use to develop sound practices. The following organizations are a sample of standard-setting groups.

- The National Institute of Standards and Technology (NIST) at www.nist.gov.
- The International Organization for Standardization (ISO) Information technology at www.iso.org.
- The Information Systems Audit and Control Association (ISACA) - Control Objectives for Information Technology (COBIT), at www.isaca.org/cobit.htm.
- The Institute of Internal Auditors, at www.theiia.org.
- The Committee of Sponsoring Organizations (COSO) of the Treadway Commission at www.coso.org.

The inclusion of these organizations in this booklet should not convey that the FFIEC endorses or approves their guidelines or guarantees the content or accuracy of the information they provide.

Roles and Responsibilities

Action Summary

A financial institution's board of directors and senior management are responsible for overseeing a safe and sound IT operating environment that supports the institution's goals and objectives. The institution's responsibilities apply to centralized and decentralized operations centers, including those located within lines of business; functional operations; affiliates under the enterprise umbrella; and outsourcing arrangements.

Key elements of these responsibilities include:

- Implementing an IT operational organization structure suitable to supporting the business activities of the institution;
- Documenting the systems in place, and understanding how these systems support the associated business processes;
- Establishing and supporting an appropriate control environment through risk identification, assessment, management, and monitoring;
- Creating a physically and logically secure operating environment;

- Providing for operational continuity and resiliency;
- Providing for adequate staffing and personnel selection, succession, and training; and
- Using qualified consultants and external auditors, when necessary.

Board of Directors and Senior Management

Senior management and the board of directors are responsible for ensuring IT operates in a safe, sound, and efficient manner throughout the institution. Because information systems-whether centralized or distributed-are tightly interconnected and highly interdependent, failure to adequately supervise any part of the IT environment can heighten potential risks for all elements of IT operations and the business as a whole. As a result, the board and senior management should coordinate IT controls throughout the institution's operating environment including all outsourcing and third-party arrangements.

Although senior management and the board can delegate implementation and oversight of daily operations to information technology management, they have final responsibility for safe, sound, controlled, and efficient operations. Consequently, the board and senior management are responsible for understanding the risks associated with existing and planned IT operations, determining the risk tolerance of the institution, and establishing and monitoring policies for risk management. The board and senior management are also responsible for strategic technology planning, which is critical to effective IT governance. The IT Handbook's "Management Booklet" addresses the role of senior management and the board.

Operations Management

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

Operations management should implement an organizational structure that addresses human resources and, where appropriate, multiple operating sites appropriate for supporting the business activities of the institution. IT operations, whether centralized or decentralized, should support business lines and functional operations. Operations should facilitate enterprise management information systems (MIS), product and service development and delivery, internal end-user information and process requirements, data capture, and transaction processing.

Effective IT operations 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). Management should also have an inventory of all of the institution's technology assets, should recognize interdependencies of these systems and should understand how these systems support the associated business lines. Additionally, management should understand the flow of data across and between systems. Adequate documentation of infrastructure and data flow facilitates risk identification, application of controls, and ongoing maintenance of information systems.

Effective IT operations management also requires that the institution establish and support an appropriate control environment. Management should implement a cost-effective and risk-focused control environment. The control environment should provide guidance, accountability, and enforceability while mitigating risk. Management should periodically assess the effectiveness of the control environment, which may be evaluated through self-assessments or other means. Management should also regularly test the results of the assessments through audits or other independent verification.

To ensure uninterrupted product and service delivery, as well as the institution's viability, operations management should develop a business continuity plan (BCP). For additional detailed information on this subject, refer to the IT Handbook's "Business Continuity Planning Booklet". IT systems should have robustness, resiliency, and capacity sufficient to accommodate ordinary interruptions to operations and to facilitate prompt restoration without escalating to more drastic and costly disaster recovery procedures.

Operations management should ensure the operating environment is physically and logically secure. Protection of expensive and critical business assets, especially the information essential to corporate activities and sensitive customer information, requires management to establish and enforce access controls to facilities, equipment, applications, systems, and transaction and customer data.

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

Operations management staff should recognize any limitations of IT operations staff and be prepared to obtain professional assistance. At times, it may be more efficient and cost effective to acquire outside expertise than to hire and train new employees, especially for functions that do not require full-time personnel.

Risk Management

Technology permeates the operations of the entire institution and therefore defies compartmentalization. Technology enables the institution to develop, deliver, and manage its products and services. An effective IT risk management process should identify, measure, control, and monitor operations risk. The process begins with identifying risks in the institution's overall business strategy. Understanding the role technology plays in enabling core business operations establishes the framework for understanding and assessing risks. Accordingly, the risk identification process should begin with a comprehensive survey of the institution's technology environment and inventory its technology assets.

The survey and inventory of the technology environment and assets also involves assessing the relative importance of systems, databases, and applications based on their function, the criticality of data they support, and their importance to core business operations. The inventory clarifies the enterprise architecture and highlights the relationships between the institution's systems, networks, and external systems.

Risk Identification

Action Summary

Management should have a thorough understanding of the institution's IT operations environment and should maintain appropriate supporting documentation. Documentation should be commensurate with the complexity of technology operations. Environmental surveys and asset inventories allow management to document data flow maps, system interfaces and dependencies, business technology processes, and hardware and software inventories. Management's ongoing environmental survey of technology operations is fundamental to enterprise risk identification, assessment, management, and monitoring.

Key elements include developing and maintaining:

- An inventory of all computing hardware;
- An inventory of all computing software (operating systems, applications, and back office and environmental applications);
- Network topologies or other diagrams that detail the internal and external connectivity of voice and data communication networks;
- Data flow and business process diagrams that depict operational interdependencies; and
- A comprehensive, holistic view of how technology operations support the strategic business goals of the institution.

Environmental Survey

To effectively identify, assess, monitor, and manage the risks associated with IT operations, management should have a comprehensive understanding of the institution's operations universe. Technology is increasingly embedded in business lines, in functional support areas, at the physical location of a business partner or affiliate, or at multiple data centers. An environmental survey allows the institution to gain an enterprise-level view by documenting resources, physical locations, hardware and

software configurations, and interfaces and interdependencies. The survey should track the capture, processing, flow, and storage of data throughout the institution. As an integral part of the environmental survey, management should perform and maintain an inventory of information technology assets.

With a comprehensive understanding of the institution's technology environment, management can promote resource allocation, appropriate capital expenditures, and adequate support for business activities, customer service, and product delivery. More narrowly, this understanding will facilitate cost control, configuration and standards management, root cause and problem analysis, prevention of loss or misuse of corporate resources, and license management. Management will also be able to control the purchasing process and prevent the introduction of unauthorized software and hardware. A thorough environmental survey and inventory also serve as the foundation for managing and monitoring daily operations. The survey and inventory provide information vital to the assessment of other important control processes such as information security, business continuity planning, and outsourcing risk management.

Management should ensure documentation of the technology environment is current, appropriate to the size and complexity of the institution, and prioritized based upon the criticality of the function supported and the location of equipment. Regardless of institution size, management should possess a basic inventory of resources as well as a topology or network map. For large, complex institutions, documentation should provide an overview with sufficient detail describing subordinate processes and systems. As an alternative to detailed documentation, there are also network management tools available to create a database or an electronic repository of inventory and topology information. Smaller and less complex institutions may be able to operate with less detailed or sophisticated documentation, but should nonetheless be responsible for understanding the inventory and topology of their IT environment. As the size and complexity of the institution increases, documentation should expand to include business processes and data flow maps. Management should ensure the survey and inventory are updated on an on-going basis to reflect the institution's technology environment at any point in time.

Technology Inventory

Hardware

The hardware inventory should be comprehensive. In addition to identifying institution-owned assets, it should also identify equipment owned by other parties but located within the environment. To the extent possible, hardware items should be marked with a unique identifier, such as a bar code, tamper-proof tag, or other label. The inventory should encompass stand-alone computing devices, including:

- Environmental control terminals;
- Physical access control systems;
- Service-provider-owned equipment, such as automated teller machine (ATM) administrative terminals;

- FedWire/Fedline terminals;
- Bank customer-owned equipment;
- Vendor-owned equipment;
- Personal computers (PCs);
- Mainframes; and
- Servers.

The following are examples of useful information to capture in hardware inventories:

- Mainframe, midrange or server:
  - Vendor and model;
  - Processor capacity in million instructions per second (MIPS);
  - Core or main memory;
  - Storage (internal and external tapes, tape silos, direct access storage device (DASD), etc.);
  - Function; and
  - Location.
- Desktop or stand-alone computing devices:
  - Vendor and model;
  - Owner and purpose;
  - Network connectivity (not applicable to stand-alone);
  - Dial-out capability; and
  - Location.
- Network devices:
  - Vendor and model;
  - Type;
  - Native storage (random access memory); and
  - Internet protocol (IP) address.
- Item processing equipment:

- Vendor and model; and

- Type.

Inventories of telecommunication equipment should contain similar information and should document use and connectivity. This is especially important when an institution uses either private branch exchanges (PBX) or voice over Internet protocol (VOIP) to provide voice and data connectivity. Inventories of telecommunications interconnections should include the following information:

- Number and configuration of trunks;
- Circuit numbers;
- Entry points to the premises;
- Central office connectivity;
- Types of service supplied, including:
  - POTS - plain old telephone service;
  - SONET - synchronous optical network;
  - ISDN - integrated services digital network;
  - Frame relay; and
  - Wireless.

Software

There are at least three major categories of software institutions should include in the software inventory: operating systems, application software, and back-office and environmental applications. Application software includes core processing applications, as well as desktop and workstation office productivity software. Back-office and environmental software consists of applications that reside above the operating system and that support primary applications. Examples of back office and environmental software include database engines, back-up and storage management software, Internet servers and application support software, file transmission systems, system performance monitoring applications, scheduling and change control systems, utilities, front-end processors (for mainframes only), and problem and issue tracking software.

The following provides examples of information to capture in software inventories:

- Type or application name (e.g. general ledger, payroll);
- Manufacturer or vendor;

- Serial number;
- Version level;
- Patch level;
- Number of copies installed;
- Number of licenses owned; and
- Types of licenses owned (e.g. site, individual).

Network Components and Topology

The institution's network infrastructure is critical to all facets of business operations. Voice and data communication networks form the backbone for information sharing and data transfer and facilitate tight integration of technology systems. In addition to maintaining a complete inventory of hardware and software connected to and operating on the network, management should also fully document the network configuration.

Depending on the size and complexity of the institution's network, management should develop and maintain high-level topologies that depict wide area networks (WANs), metropolitan area networks (MANs), and local area networks (LANs). The topologies should have sufficient detail to:

- Facilitate network maintenance and troubleshooting;
- Facilitate recovery in the event of a disruption; and
- Plan for expansion, reconfiguration, or addition of new technology.

Topologies should also:

- Identify all internal and external connectivity (including Internet and modems);
- Describe the type of connectivity (digital subscriber line (DSL), dialup, cable modem, wireless);
- Note the bandwidth of connectivity within and between network segments;
- Identify and describe encrypted or otherwise secure communication channels;
- Depict the type and capacity of network segment linkages (switches, routers, hubs, gateways, etc.);
- Portray information security systems (firewalls, intrusion detection systems, and hacker-trapping "honey pots");

- Identify primary vendors of telecommunications services; and
- Identify what information is available and where it resides

The network topology should be a technical blueprint of the network structure. Management should collect other important network documentation. Institutions should identify and document the type, location, and volume of information stored and transmitted on their networks. Management should develop a complete description of all network management tools and network administration console capability.

Management should also develop data flow diagrams to supplement its understanding of information flow within and between network segments as well as across the institution's perimeter to external parties. Data flow diagrams should identify:

- Data sets and subsets shared between systems;
- Applications sharing data; and
- Classification of data (public, private, confidential, or other) being transmitted.

Data flow diagrams are also useful for identifying the volume and type of data stored on various media. In addition, the diagrams should identify and differentiate between data in electronic format, and in other media, such as hard copy or optical images.

Media

Documentation of storage media should complement network topologies and hardware and software inventories without being redundant. Descriptive information should identify the type, capacity, and location of the media. It should also identify the location, type, and classification (public, private, confidential, or other) of data stored on the media. Additionally, management should document source systems, data ownership, back up frequency and methodology (tape, remote disk, compact disc (CD), or other), and the location of back-up media if other than at the primary off-site storage facility.

Risk Assessment

Action Summary

Management should analyze the survey of the IT operations environment and the inventory of technology resources to identify threats and vulnerabilities to IT operations. The assessment process should identify:

- Internal and external risks;
- Risks associated with individual platforms, systems, or processes as well as those of a systemic nature; and
- The quality and quantity of controls.

To the extent possible, the assessment process should quantify the probability of a threat or vulnerability and the financial consequences of such an event.

IT operations comprise the framework of service and product delivery to internal and external customers and are intrinsic to much of the risk management undertaken by the institution. For these reasons, management should not limit the risk assessment process to risks associated with specific platforms, their operating systems, resident applications and utilities, the connecting network, associated human processes, and the control environment. Management should also consider the interdependencies between these elements. Threats and vulnerabilities have the potential to quickly compromise interconnected and interdependent systems and processes.

The environmental survey and technology inventory provide the foundation for the risk identification and assessment processes. Once the survey and inventory are complete, management can employ a variety of techniques to identify and assess risks, including performing self-assessments, incorporating concerns identified in internal and external audits, reviewing business impact analyses prepared for contingency planning, assessing the findings of vulnerability assessments conducted for information security purposes, and understanding the concerns identified by insurance underwriters for establishing premiums. In risk identification and assessment management should emphasize events or activities that could disrupt operations, negatively affect earnings or reputation, or that might be categorized in the following general areas:

- Technology investment mistakes including improper implementation, failure of a supplier, inappropriate definition of business requirements, incompatibility with existing systems, or obsolescence of software (including loss of hardware or software support);
- Systems development and implementation problems including inadequate project management, cost and time overruns, programming errors, failure to integrate or migrate from existing systems, or failure of a system to meet business requirements;
- Systems capacity including lack of capacity planning, insufficient capacity for systems resiliency, or software inadequate to accommodate growth;
- Systems failures including interdependency risk, or network, interface, hardware, software, or internal telecommunications failure; and
- Systems security breaches including external or internal security breaches, programming fraud, or computer viruses.

The individual risk assessment factors management should consider are numerous and varied. The combination of factors used should be appropriate to the size, scale, complexity, and nature of the institution and its activities. These factors include:

- Importance and business criticality;
- Extent of system or process change;
- Source of system access (internal or external, including Internet, dial-up, or WAN);
- Source of application (commercial off the shelf (COTS), in-house developed, combination of these two, etc.);
- Scope and criticality of systems or number of business units affected;
- Sophistication of processing type (batch, real-time, client/server, parallel distributed);
- Transaction volume and dollar value of transactions;
- Classification or sensitivity of data processed or used;
- Impact to data (read, download, upload, update or alter);
- Experience level and capability of functional area management;
- Number of staff members and staff stability;
- Number of users and customers;
- Changes in the legal, regulatory, or compliance environments;
- Presence of new or emerging risks from developing technology or technology obsolescence; and
- Presence of audit or control self-assessment weaknesses.

Prioritizing Risk Mitigation Efforts

Once an institution identifies and analyzes the universe of risks, management should prioritize risk mitigation actions based on the probability of occurrence and the financial, reputational or legal impact to the institution. Organizational impacts are variable and not always easy to quantify, but include such considerations as lost revenue, loss of market share, increased cost of insurance premiums, litigation and adverse judgment costs, and data recovery and reconstruction expense. Management should prioritize the risk assessment results based on the business importance of the associated systems. The probability of occurrence and magnitude of impact provide the foundation for establishing or expanding controls for safe, sound, and efficient operations appropriate to the risk tolerance of the institution.

Risk Mitigation and Control Implementation

Action Summary

Management should implement a control environment consistent with its risk assessment. Sound IT operations controls are grounded in policies, standards, and procedures that provide for:

- Environmental controls;
- Preventive maintenance;
- Physical security;
- Logical security;
- Personnel controls;
- Change management;
- Information controls;
- User support/help desk;
- Controls over job scheduling, output, and negotiable instruments; and
- Event management.

Risk mitigation involves creating a sound control environment that reduces internal and external threats to the institution's tolerance level and establishes a structured environment for IT operations. Examples of controls include policies and procedures related to personnel and operations, segregation of duties and dual controls, data entry controls, quality assurance programs, industry certification, and operating thresholds and parameters. While not a control, insurance can be an effective risk mitigation tool. Management should balance controls against business operations requirements, cost, efficiency, and effectiveness.

Policies, Standards, and Procedures

Policies

Board-approved governing policies provide broad guidance in addressing risk tolerance and management. Policies should address key areas such as personnel, capital investment, physical and logical security, change management, strategic planning, and business continuity. The depth and coverage of IT operations policies will vary based on

institution size and complexity. Small, noncomplex institutions often embed IT policy in a variety of other policies or create one central guiding document. Larger, complex institutions often segregate policies based on business lines or other operational divisions. Boards of directors and management should enact policies and procedures sufficient to address and mitigate the risk exposure of their institutions.

Standards

Internally developed technology standards establish measurable controls and requirements to achieve policy objectives. Technology standards benefit an institution by defining and narrowing the scope of options and enabling greater focus by the supporting IT resources.

Standardization of hardware, software, and the operating environment offers a number of benefits and greatly facilitates the implementation and maintenance of "enterprise architecture." Standardization of hardware and software (including configurations and versions) simplifies the task of creating and maintaining an accurate survey and inventory of the technology environment. It can also improve IT operations performance, reduce IT cost (particularly in acquisition, development, training, and maintenance), allow the leveraging of resources, enhance reliability and predictability, contribute to improved interoperability and integration, reduce the time to market for projects that involve technology re-configuration, and alleviate complexity in technology risk management.

The degree to which an institution standardizes its hardware and software is a business decision. Management should weigh the benefits of standardization against the competing benefits offered by "best of breed" technology solutions. Management should also consider that certain applications will not function effectively on the "standard" platform, or that hardware will not function properly in a "standard" configuration. Institutions should adopt minimum technology standards to leverage purchasing power, ensure interoperability, provide for adequate information systems security, allow for timely recovery and restoration of critical systems, and ease the burden of maintenance and support.

Management should implement hardware, operating system, and application standardization through policies that address every platform from host to end user. A variety of automated systems and network management tools are available to monitor and enforce standards and promote version control in the mainframe, server, and desktop environments. Standardization is also enforced through the change management process and internal audits.

Procedures

Procedures describe the processes used to meet the requirements of the institution's IT policies and standards. Management should develop written procedures for an institution's critical operations. Procedures establish accountability and responsibility, provide specific controls for risk management policy guidance, define expectations for work processes and products, and serve as training tools. Because of the value procedures provide to these areas, management should update and review written procedures regularly. Updating written procedures is particularly important when processes, hardware, software, or configurations change.

The scope of required procedures depends on the size and complexity of the institution's IT operations and the variety of functions performed by IT operations. Examples of activities or functional areas where written procedures are appropriate include:

- Console operations or run manuals - mainframe and midrange systems;
- Network administration;
- Telecommunication administration;
- Data storage administration;
- Data library administration;
- Equipment maintenance;
- Problem management or incident response;
- Business continuity planning, disaster recovery, and emergency procedures;
- Security - physical and logical;
- Change management and change control;
- Data and system back-up and off-site storage;
- Imaging;
- Item processing;
- Balancing and reconciliation;
- Output control;
- Job scheduling; and
- Negotiable instruments.

Controls Implementation

Environmental Controls

Many financial institutions rely on IT operations that are complex, sensitive, or critical to daily functioning. Disruptions to the IT operations environment can pose significant operational, strategic, transaction, and reputation risks. Consequently, management should control and monitor environmental factors whether at the business line or the consolidated data center. Management should carefully assess the IT operations environment and implement relevant controls.

Computing equipment should have a continuous uninterrupted power source. Independent electrical feeds drawing on separate power grids are the most reliable

power source, however they may be cost prohibitive and may not be feasible in many geographic locations. Management should take reasonable action to protect computing equipment power sources. Where dual feeds or back-up power generators are used, wiring should support automatic switching in the event one power source is disrupted. Power surges can also damage computer equipment. Consequently management should monitor and condition or stabilize the voltage of electricity sources to prevent power fluctuations.

IT operations centers should have an alternative power source independent of local power grids. Typically, this is provided by a combination of a battery-based uninterruptible power supply (UPS) and a generator powered by gasoline, kerosene, natural gas, or diesel fuel. Management should configure the UPS to provide sufficient electricity within milliseconds to power equipment until there is an orderly shutdown or transition to the back-up generator. The back-up generator should generate sufficient power to meet the requirements of mission critical technology and environmental support systems. The institutions should have sufficient fuel in storage or readily available to sustain operations for at least two or three business days. In addition, management should make arrangements to replenish the fuel supply in the event of an extended outage. Gasoline becomes stale after an extended period of time; the tank should be drained and refilled with new gasoline at least annually. A lower cost alternative to installing a permanent generator is to configure the operations center with an exterior electrical box to connect a temporary generator. Under this scenario, management should also establish reliable arrangements for the availability and delivery of a generator and fuel within a required time frame.

Similarly, IT operations centers should have independent telecommunication feeds from different vendors. Wiring configurations should support rapid switching from one provider to another without burdensome rerouting or rewiring. Because vendors often share or sublease the same common cabling or are routed through the same central office, management should have the vendors perform line traces to ensure there is no single point of failure or path redundancy.

Even small IT operations centers with modest computer equipment can contain a significant amount of computer cabling. Management should physically secure these cables to avoid accidental or malicious disconnection or severing. In addition, management should document wiring strategies and organize cables with labels or color-codes to facilitate easy troubleshooting, repair, and upgrade.

Every operations center should have adequate heating, ventilation, and air conditioning (HVAC) systems in order for personnel and equipment to function properly. Older computer equipment produces a significant amount of heat, requiring cooling capacity exceeding that of a standard office building. Some newer models do not produce as much heat and thus do not require as much air conditioning. Organizations should plan their HVAC systems with the requirements of their computer systems in mind. Back-up sources of electricity should be able to sustain HVAC systems, because inadequate cooling could render computer equipment inoperable in a short period of time. Also, operations personnel should be familiar with written emergency procedures in the event of HVAC system disruption.

Personnel should also be able to function in the event utility service is interrupted. Therefore, management should keep a one- to two-day supply of bottled water and non-perishable food on the premises.

All operations centers should have heat and smoke detectors installed in the ceiling, in exhaust ducts, and under raised flooring. Detectors should not be situated near air

conditioning vents or intake ducts that can disburse smoke and prevent the triggering of alarms. Some large and complex operations centers are beginning to use very early smoke detection alert (VESDA) systems in place of conventional smoke detectors. VESDA systems sample the air on a continuous basis and are far more sensitive. They are capable of detecting a fire at the pre-combustion stage. Although more expensive than conventional systems, a VESDA system can detect a smoldering wire and alert management before a fire starts. The early notice may also prevent suppression equipment from deploying water or foam that can damage computer equipment.

A variety of strategies are available for fire suppression. One of the more widely used systems was a halon gas system that deprived a fire of oxygen. The government phased out production of halon because it determined that halon causes ozone depletion. The phase out deadline was December 31, 2003. Once existing reserves are depleted additional halon may not be purchased. Institutions still using halon systems should be prepared to switch to another fire suppression system. Newer systems rely on the same theory, but use inert agents such as Inergen, FM-200, FE-13, and carbon dioxide. Many facilities continue to rely on water as a fire suppressant, choosing a wet-pipe or dry-pipe configuration. In the wet-pipe configuration, the pipes are filled with water and may be subject to leakage. In the dry-pipe configuration, the pipes are empty until a fire is detected, minimizing the risk of water damage from burst or leaking pipes. Ideally, the fire suppression system should allow operators time to shut down computer equipment and cover it with waterproof covers before releasing the suppressant. Many facilities store waterproof covers throughout the data center to cover sensitive equipment quickly if sprinklers are activated.

Water leaks can cause serious damage to computer equipment and cabling under raised floors. For this reason, operations centers should be equipped with water detectors under raised flooring to alert management to leaks that may not be readily visible. Management should also consider installing floor drains to prevent water from collecting beneath raised floors or under valuable computer equipment. Furthermore, management has several considerations in protecting cables from water damage; running cables under raised flooring risks flooding from below but suspending cables overhead risks water damage from leaks resulting from the roof or floors above.

Preventive Maintenance

Preventive maintenance on equipment minimizes equipment failure and can lead to early detection of potential problems. This includes minor maintenance such as cleaning peripheral equipment as well as more extensive maintenance provided by the manufacturer, vendor, or maintenance contractor. Preventive maintenance also includes general housekeeping to keep the operations center clean and orderly.

Unless specifically authorized by management, computer operators should not repair equipment or perform other than the most routine maintenance. Even if they have the requisite knowledge and experience, many hardware and software warranties disclaim liability for unauthorized maintenance or alteration. Maintenance by computer operators should be performed according to manufacturers' recommendations. As a general rule, these duties include:

- Cleaning tape heads each shift;

- Cleaning printers daily;
- Checking and cleaning the magnetic ink character recognition (MICR) reader/sorter at the end of each shift; and
- Periodically checking and cleaning the area under raised flooring.

Maintenance schedules may vary considerably depending on the number and variety of technology systems and the volume of work processed. All maintenance should follow a predetermined schedule. Employees should document maintenance in logs or other records. Management review of these records will aid in monitoring employee and vendor performance.

The manufacturer or vendor will usually perform maintenance under contract. For leased equipment, maintenance may be part of the lease arrangement. When equipment is owned or leased from a third party, management should obtain a separate maintenance or service agreement between the operations center and the equipment manufacturer. The service or maintenance agreement should provide repair services, detail the preventive maintenance, and include a schedule for both. When an operations center uses hardware from more than one manufacturer, it may be desirable to enter into an arrangement whereby one vendor takes responsibility for all repair maintenance. Under this arrangement, the operations center would contact the designated vendor to determine the source of the problem and to make all the necessary repairs. In any event, management should ensure maintenance contracts guarantee timely performance.

Management should schedule time and resources for preventive maintenance and coordinate that schedule with production. During scheduled maintenance, the computer operators should dismount all program and data files and work packs, leaving only the minimum software required for the specific maintenance task on the system. If this is impractical, management should review system activity logs to monitor access to programs or data during maintenance. Also, at least one computer operator should be present at all times when the service representative is in the computer room.

Some vendors can perform computer maintenance online. Operators should be aware of the online maintenance schedule so that it does not interfere with normal operations and processing. Operators and information security personnel should adhere to established security procedures to ensure they grant remote access only to authorized maintenance personnel at predetermined times to perform specific tasks.

Operators should maintain a written log of all hardware problems and downtime encountered between maintenance sessions. A periodic report on the nature and frequency of those problems is a necessary management tool, and can be valuable for vendor selection, equipment benchmarking, replacement decisions, or planning increased equipment capacity.

Security

Physical Security

The personnel, equipment, records, and data comprising IT operations represent a critical asset. Management should deploy adequate physical security in a layered or zoned approach at every IT operations center commensurate with the value, confidentiality, and criticality of the data stored or accessible and the identified risks. This section summarizes some of the preventive and detective controls for physical security and discusses some minimum physical security requirements. Refer to the IT Handbook's "Information Security Booklet" for additional information.

An institution's main IT operations center should have a limited number of windows and external access points. The data center should preferably not be identified as such. The perimeter should have adequate lighting, and, if conditions warrant, perimeter security should have gates, fences, video surveillance, and alarms. Management should assess whether armed guards are suitable and should ensure they are trained, licensed, subjected to background checks, and follow standard security industry practices.

Management should consider using video surveillance and recording equipment in all or parts of the facility to monitor activity and deter theft. Management should also use inventory labels, bar codes, and logging procedures to control the inventory of critical and valuable equipment.

An institution should implement policies and procedures to prevent the removal of sensitive electronic information and data. These policies should address the use of laptop computers, personal digital assistants, and portable electronic storage devices. The policies and procedures should further address shredding of confidential paper documents and erasing electronic media prior to disposal. In addition, policies and procedures should delineate the circumstances under which employees' personal property may be subject to search.

Logical Security

Information security has specific implications for technology operations. Data center operations should support and complement the financial institution's information security architecture and processes. Refer to the IT Handbook's "Information Security Booklet" for additional information.

As part of the information security program, management should implement an information classification strategy appropriate to the complexity of its systems. Generally, financial institutions should classify information according to its sensitivity and implement controls based on the classifications. IT operations staff should know the information classification policy and handle information according to its classification.

IT operations management should implement preventive (e.g., access controls), detective (e.g., logging), and corrective (e.g., incident response) logical security controls. All three types of controls provide a framework for IT operations information security. These controls can be implemented by administrative (e.g., policy), logical (e.g., access controls), or physical (e.g., locked room) controls.

IT operations staff should be aware of the organization's information security program, how it relates to their job function and their role as information custodians. As custodians, the IT operations staff has the responsibility of protecting the information as it is processed and stored.

Management should employ the principle of least possible privilege throughout IT operations. The principle provides that individuals should only have privileges on systems and access to functions that are required to perform their job function and assigned tasks. Access privilege may include read-only, read/write, or create/modify. Even read-only access poses risk since employees can print or copy sensitive customer information for inappropriate use. System administrator and security administrator level access allow an individual to change access privileges to systems and information. Individuals with these roles and privileges should have minimal transactional authority. Independent employees should monitor the system and security administrator activity logs for unauthorized activity. Smaller operations centers are challenged in implementing separation of duties and the principle of least privilege because they frequently do not have the resources. Management at smaller institutions should establish compensating controls in these circumstances.

Network and system monitoring and maintenance tools can provide IT operations staff with inappropriate access to sensitive information. These hardware and software monitoring and maintenance tools observe equipment for error conditions, faulty links, or other problems. These utilities may also allow operations staff powerful access to operations center equipment. Because monitoring tools such as network sniffers, network diagnostics tools, and network management utilities can circumvent traditional safeguards, management should control access to them. Controls for such tools should include:

- Policies defining appropriate use;
- Least possible privilege;
- Usage logs;
- Reports to management and audit on use of monitoring tools;
- Password protection and lockout facilities;
- Physical protection (e.g., a locked cabinet); and
- Dual control of equipment (i.e., two individuals need to operate equipment together).

Remote monitoring and administration tools pose special risks to information security. Remote tools allow operators to connect through a remote function and perform activities they would normally perform on-site. Some financial institutions have approved remote access technologies as a central, common solution for all employees who require remote access. Information security personnel should scrutinize and monitor remote access closely. Remote access solutions that are available continuously or for extended periods of time pose the greatest risk to a financial institution. Because remote access solutions potentially bypass information security controls, management should evaluate and implement appropriate user access, activity logging, and time of day controls to minimize the risk of unauthorized access.

Other types of remote access such as modems attached to systems or special maintenance ports may circumvent the central, approved remote access solution. Information security personnel may overlook these remote access points, which might

allow unauthorized individuals to access sensitive equipment. Management should routinely review the network topology and hardware inventory to ensure the identification and control of all remote access points. Management should also document strict policies about the consequences of unauthorized use of modems or other access devices without implicit approval.

Database Management

Databases are centralized collections of data for use by business applications. They typically store critical and sensitive information including customer account data. Databases can exist on mainframes, networks, and stand alone PCs. Because they can be repositories of the financial institution's most critical information, databases pose unique risks. Failure to adequately manage and secure databases can lead to unintentional or unauthorized modification, destruction, or disclosure of sensitive information. Unauthorized disclosure of confidential information can result in reputation, legal, and operational risk to the institution and possible financial loss.

The sensitivity and classification of the information stored in the database form the basis for establishing controls. A database that stores confidential information may require a more significant control environment than a database that stores non-sensitive information. Management should consider the security and performance implications of the security options available with modern database management systems. It is possible to control, monitor, and log access to data down to the record and row level, but there is a systems performance cost.

Database administrators use a database management system (DBMS) to configure and operate databases. Because DBMS software provides high level, privileged database access, management should restrict use of this software to authorized personnel. One function of the database administrator is to create particular views of information stored in the database that are unique for each type of user. For example, a loan processor will have a different view of information in the database than a branch teller. The different user groups will also have different abilities to add, modify, or delete information. The database administrator is responsible for providing users with access to the appropriate level of information. The primary risk associated with database administration is that an administrator can alter sensitive data without those modifications being detected. A secondary risk is that an administrator can change access rights to information stored within the database as well as their own access rights. As a preventive control against these risks, the institution should restrict and review access administration and data altering by the administrator. Close monitoring of database administrator activities by management is both a preventive and detective control.

An independent testing environment is particularly important for maintaining data integrity, but represents an information security risk in database environments. The independent testing environment prevents the corruption of actual production data because the users conduct the tests on copies of data rather than the actual database. Testing on a live production database can lead to a compromise of data integrity or prevent users from accessing data when they need it. For example, a live test of an Internet banking database may slow processing speeds and ultimately prevent customers from accessing their account information if additional operational problems develop. Where testing environments utilize copies of actual production data, security controls over access to the viewing and copying of sensitive data should be as strong as in the production environment. Alternatively, management might consider scrambling of

production data for use in testing as a way to protect confidentiality. Changes to databases should follow the financial institution's change control procedures once testing is complete.

Database administrators monitor the database and maintain general awareness of normal operations. Trained and aware administrators performing these activities can complement the information security function. Because databases can store sensitive information, they are often the targets of malicious activity by both internal and external sources. Administrators monitoring databases should be alert to changes in normal activities that may indicate inappropriate error conditions or activity. For example, a virus may infect a database and cause the response times for user queries to increase significantly. An administrator who becomes aware of this or other unusual conditions should act appropriately to protect sensitive information, restore normal operations, and notify the information security officer.

Connections to databases have important information security implications. Databases store critical information but perform no processing. Application software processes information through information queries, modifications, additions, and deletions. In order for an application to access a database a user account and password should be established. In some cases, these are hard-coded or built into the application and transparent to the actual employee. Security is established through the employee's access level and user ID/password to gain access to the application. This user account should only permit those functions required by the application instead of a broad administrator user account.

Personnel Controls

Change Management

Technology operations environments are dynamic, and processes, procedures, and controls should be in place to manage change. Change management broadly encompasses change control, patch management, and conversions. It also includes the institution's policies, procedures, and processes for implementing change, which are discussed more fully in the IT Handbook's "Management Booklet" and "Development and Acquisition Booklet".

Large and complex institutions should have a change management policy that defines what constitutes a "change" and establishes minimum standards governing the change process. Processes and procedures for implementing change may be universal for the institution-applicable to all business lines and environments-or may be stratified, such as changes affecting the entire institution and those affecting a business line, support area, or affiliate.

Smaller and less complex institutions may successfully operate with less formality, but should still have written change management policies and procedures. Because mainframe, network, client-server, and application changes are different, institutions may choose to develop individualized procedures. However, individualized procedures do not instill consistency in the change management process. Consistency contributes to a change management process that is defined, managed, repeatable, and optimized.

Change Control

Increasingly, technology systems are tightly integrated and interdependent. As a result, creating a central change control oversight function is a sound practice for management of the change process. This may be a specialized change control or management committee in a large, complex institution, or a technology steering committee in a small, noncomplex institution. All changes should flow through the oversight function, which should include appropriate representation from business lines, support areas, technology management, information security, and internal audit. In establishing a framework for managing change, a policy should be present describing minimum standards and including such factors as notification, oversight, and control. Control standards should address risk, testing, authorization and approval, timing of implementation, post-installation validation, and back-out or recovery.

Patch Management

Vendors frequently develop and issue patches to solve problems, improve performance, and enhance security of their software products. Management should establish procedures to stay abreast of patches, to test them in a segregated environment, and to install them when appropriate. Change management procedures should require documentation of any patch installations. Management should develop a process to ensure version control of operating and application software to ensure implementation of the latest releases. Management should also maintain a record of the versions in place and should regularly monitor the Internet and other resources for bulletins about product enhancements, security issues, patches or upgrades, or other problems with the current versions of the software.

Conversions

Conversions involve major changes to existing systems or applications, or the introduction of systems or data sets resulting from acquisitions or mergers. Conversions are a unique and more complex type of systems change, which may span multiple platforms. Consequently, they have a higher level of risk requiring additional, specialized controls. Strong conversion policies, procedures, and controls are critical. Improperly handled, conversions can result in corrupt data. Moreover, because the ramifications of conversion span technology operations, it is important for management to re-evaluate periodically all operations processes and consider the appropriateness of process re-engineering. Conversions require management to draw on a number of control disciplines involving change processes and strategic planning, including project management, change control, testing, contingency planning, back-up, vendor management, and post-implementation review. An improperly executed conversion can create inefficiencies including serious degradation of IT performance, internal and external user dissatisfaction, accounting problems, customer dissatisfaction, reputation damage, and critical operational disruptions.

Information Distribution and Transmission

Output

System output-whether in electronic form or hard copy reports-can contain sensitive or confidential information. Unnecessary output increases operating expense and reduces the efficiency of IT operations. Management should analyze output and implement necessary controls to limit the production of unnecessary confidential data output. Automated report management software and similar tools can facilitate the implementation of output controls. Management should also develop specific physical and logistical procedures for hardcopy and electronic report distribution to ensure a secure environment including assessing the use of locked containers, limited access mailboxes, or secure communications. There should also be appropriate controls and procedures to insure the proper disposal or destruction of output whether hardcopy or electronic format. For example, hardcopy output should be shredded to a level to prevent reconstruction of information.

Transmission

Transmission controls should address both physical and logical risks. In large, complex institutions, management should consider segregating WAN and LAN segments with firewalls that restrict access as well as the content of inbound and outbound traffic. Management should also consider using encryption technology-including basic encryption as well as the use of digital certificates and public key infrastructure-to secure data transmissions. Refer to the IT Handbook's "Information Security Booklet" for additional discussion of encryption and other security technology.

Telecommunications technology typically incorporates message content and completion validation. Network management should continuously monitor telecommunications traffic for problems involving high rates of lost packets, interference that degrades connectivity, capacity problems that reduce throughput, or other anomalies. In addition, administrators should periodically review network devices to identify any that are operating in promiscuous mode and acting as packet "sniffers" for network traffic.

Management should implement strong access controls to secure telecommunication equipment. Telecommunications closets should be locked and carry no specific identification to provide an additional measure of security. Changes to telecommunications equipment and equipment settings or configuration should follow enterprise change control standards including approval, testing, and migration to production. An institution should authenticate and approve any remote access to telecommunication equipment. Identification, authorization, and authentication to access telecommunications systems should follow enterprise standards including approval and documentation of exceptions.

Voice communication is essential to many functions of an institution. The business continuity plan should include telecommunication resources. Loss of telecommunications can have a material impact on the ability of an institution to function, exposing it to legal, reputation, and financial risks. Therefore, institutions need to have resiliency and redundancy in their telecommunications architecture. Where available, planning should ensure access to a diversity of suppliers. Management should consider implementing route diversity to ensure data can travel along an alternate route if its primary path is blocked. Management can also improve diversity by connecting IT operations to multiple telephone company central offices. An institution should thoroughly test in-house and

outsourced telecommunications recovery processes. It should also implement physical security for telecommunications equipment at any alternate operations site(s) similar to that of the primary data center.

Management should monitor the financial health of its telecommunications providers. To ensure continuity of service, there should be at least one back-up vendor in the event the primary provider cannot deliver the required service. Large, complex operations centers and those critical to payment systems should have multiple primary and secondary providers for bandwidth and security purposes.

Along with diversity, building redundancy into telecommunications networks enhances resiliency. An institution should avoid exposure to single points of failure. Establishing multiple network entry points into the operations center and connecting them to redundant infrastructure strengthens a network's survivability.

Outsourced back-up facilities should meet all institution requirements. All telecommunications equipment housed in recovery facilities should follow institution standards for security, availability, and change control. Management should test back-up telecommunications functions during business continuity plan testing. Management should also document test results and ensure appropriate changes are made to the business continuity plan. Contracts with recovery facilities should specify which party is responsible for telecommunications. They should also ensure telecommunications controls meet the institution's enterprise standards.

Institutions should be aware of the priority level of recovery services contracted from their providers.See Financial and Banking Information Infrastructure Committee Policy on the Sponsorship of Priority Telecommunications Access for Private Sector Entities through the National Communications System Government Emergency Telecommunications Service (GETS). http://www.fbiic.gov/policies.htm Having a sound relationship with a telecommunications provider can greatly facilitate recovery after a business interruption. Institutions that choose to outsource the management of their telecommunications networks to third party providers should receive reports from the vendor on performance, capacity, availability, and other key metrics.

Refer to the IT Handbook's "Business Continuity Planning Booklet" and "Outsourcing Technology Services Booklet" for additional discussion on these topics.

Storage/Back-Up

Management's primary objectives in providing data storage solutions are to ensure the integrity and availability of data, particularly mission critical data. Management and institution customers should receive current, complete, and accurate data. Management also needs to implement a storage solution that is manageable from an administrative perspective and usable and accessible from the customer and end-user perspectives. Storage solutions should be appropriately scalable to allow for future growth.

Management's primary defense against such risks is proper planning. There should be written standards that ensure consistent application of data management standards. Management should choose data storage solutions after careful consideration of configuration options, vendor options, cost/benefit analyses, and anticipated institution growth. Management should maintain an inventory of data sets and primary locations, so it is aware of the scope and breadth of its data storage systems. Management should also be aware of the impact an outage will have on each business line application at any

point in time in order to implement appropriate recovery operations. Where feasible an institution should develop redundancy, either through duality in storage architecture or secondary on-site copies of data, to minimize the need to use off-site back-up materials.

An institution should back up and store its data and program files in a secure off-site location to allow restoration of systems, applications, and associated data in the event normal processing is disrupted by a disaster or other significant event. Management should develop a rotation scheme that addresses varying storage durations as well as how to transport and store multiple formats of media at the off-site storage location. Another consideration is the ability to retrieve media stored off-site in a timely manner. In the event of a disruption, management should not have to reconstruct data from more than one business day. The process of designing strategies for the back-up of program and data files should begin with a comprehensive inventory of all of the institution's systems and data. The inventory should include a risk assessment of the criticality of the applications and the associated data. This will provide management with the information necessary to determine what back-up methodologies are appropriate for the institution.

The primary risk associated with data and program back-up is the inability to recover systems, applications, and data in case of a disaster or other disruptive event. This can be caused by incomplete or sporadic performance of back-up procedures, unreliable back-up media, or the inability to access off-site back-up material. Written standards should document back-up methodologies, delineate responsibilities of appropriate personnel, and ensure uniform performance throughout the institution. Management should maintain inventories of back-up media stored off-site and periodically perform physical inventories to ensure all required back-up material is available. Procedures should include verifying adherence to the back-up schedule and reviewing actual back-up copies for readability. Similarly, management should periodically test back-up copies by actually using them to restore programs and data.

For further details on back-up processes, refer to the IT Handbook's "Business Continuity Planning Booklet", specifically the sections on off-site storage, software back-up, data file back-up, and back-up and storage strategies.

Disposal of Media

Proper disposal of media is essential protect against reputational exposure and to ensure compliance with the Gramm-Leach-Bliley Act (GLBA) regarding the safeguarding of customer information. Management should have procedures for the destruction and disposal of media containing sensitive information. [2] These procedures should be risk-based relative to the sensitivity of the information and the type of media used to store the information. For example, prior to disposing of electronic media containing sensitive customer information, they should be degaussed as a matter of standard procedure; obsolete optical media, such as "write once, read many times" (WORM), should be destroyed or defaced so that the data is unrecoverable; and printed material containing sensitive data should be destroyed in a safe and systematic manner, such as shredding or burning. Furthermore, disposal procedures should recognize that records stored on electronic media, including tapes, and disk drives present unique disposal problems in that residual data can remain on the media after erasure. Since that data can be recovered, additional disposal techniques should be applied to remove sensitive information.

Imaging

An imaging system is a computer system that converts paper documents to electronic files. Through imaging, financial institutions can electronically store and manage records. Imaging systems provide the means to quickly find, retrieve, and share documents in a networked environment.

Item processing imaging systems (IPIS) are generally high speed systems (up to 1,850 documents per minute, or dpm) designed to capture checks and other items in the data processing environment. Common uses for IPIS in financial institutions include proof of deposit, sales draft processing (credit card or point of sale [POS]), remittance processing, cash letter settlement, account reconciliation, and statement rendering. The Check Clearing for the 21st Century Act ("Check 21 Act") is an example of an IPIS, in which the processing bank captures negotiable items in an image format. Instead of forwarding physical items to the Federal Reserve or other clearing house, the processing bank electronically sends image replacement documents. This system saves the financial institution significant costs by streamlining the proof and capture processes and reducing the cost of shipping physical items.

Document management imaging systems (DMIS) are generally low-speed systems (approximately 10-200 dpm) designed to capture a range of documents, such as loan and mortgage file information, IRA and Keogh files, trust documents, and signature cards. DMIS are often used in a network environment to facilitate processes, such as a teller electronically viewing a signature card for verification purposes or a loan officer reviewing a credit file from a remote branch location.

Computer output to laser disk (COLD) is the computer process that outputs electronic records and printed reports to laser disk instead of a printer. This system is used to archive data to one or more optical disks in a compressed but easily retrievable format. COLD systems are often used with an imaging system for storage of archived reports, loan documents, and other customer records.

Quality control is important for all types of imaging and imaging processes including storage, the scanning and indexing process, and equipment-scanning rates. Management should ensure there are adequate controls to protect imaging processes, as many of the traditional audit and controls for paper-based systems may be reduced. Failure to maintain adequate controls can result in unusable or irretrievable images, alteration or counterfeiting of images, and loss or compromise of confidential customer information. Management should also consider issues such as converting existing paper storage files, integration of the imaging system into the organization workflow, and business continuity planning needs to achieve and maintain business objectives.

The following items are important imaging system control points. As a part of management's efforts to develop controls, audit should be involved to ensure the establishment of appropriate audit controls and audit trails.

Capture - Management should ensure adequate controls are in place at the point where image capturing occurs. Capturing can be accomplished through scanning documents, converting word processing documents and spreadsheets into unalterable images, or importing existing images into the institution's system. Poor controls over capturing can result in poor quality images, high rejection and exception rates, improper indexing, and capturing incomplete or forged documents. Procedures should be in place to prevent destruction of original documents before verifying image quality, especially when the

imaged information is used to process transactions.

Indexing - Management should maintain indexing-system integrity to ensure users can retrieve accurate files in a timely manner based upon business needs (e.g., customer service, business continuity planning). For document imaging, naming processes should be in place in order to easily identify what particular documents are being captured and how they should be sorted and presented upon retrieval.

Security - The institution-wide security risk assessment should include imaging systems. Management should ensure there are adequate security controls to protect the imaging system and confidential customer information. Such security should provide for separation of duties, input/output controls, and prevent unauthorized modifications of imaged data or insertion of fraudulent images.

Training - Appropriate training is key for proper system use. Inadequate instruction for imaging procedures could lead to quality control issues and misplaced or unavailable data.

Audit - Like any other system, imaging needs to be scrutinized to ensure adequate controls have been enabled.

Back-Up and Recovery - Imaging system back-up and recovery planning should ensure restoration and retrieval of information within recovery time objectives as defined within the business continuity plan. The complexity of back-up and recovery solutions will vary based upon the use of imaged data (e.g., as a reference copy, to support transaction processing,). Since imaging allows the storage of large volumes of documents, the loss of imaged files can significantly affect business operations if back-up electronic or paper files are not readily available. Further, the loss or malfunction of indexing software could leave the institution without a mechanism to pull related imaged documents together into a single coherent view such as an electronic credit file.

Legal Issues - Institutions installing imaging systems should carefully evaluate the legal implications of converting the original documents to image. The institution may be required to demonstrate through audit trails, access records, and electronic storage practices that the images presented are unaltered. Management should consult with attorneys to discuss issues such as record retention and destruction of original documents.

Event/Problem Management

An effective event/problem management process helps protect institutions from financial risks, operational risks, and reputation risks. Management should ensure appropriate controls are in place to identify, log, track, analyze, and resolve problems that occur during day-to-day operations.

The event/problem management process should be communicated and readily available to all IT operations personnel. Appropriate personnel-from IT operations, institution management, internal audit, fraud and loss prevention, information security, and computer security incident response teams-should participate in the event/problem management process. Event/problem management plans should cover hardware, operating systems, applications, and security devices and should address at a minimum:

- Event/problem identification and rating of severity based on risk;
- Event/problem impact and root cause analysis;
- Documentation and tracking of the status of identified problems;
- The process for escalation;
- Event/problem resolution;
- Management reporting; and
- Contact and communication information, including:

  - Current names and/or positions of individuals that should be contacted;

  - Current phone numbers of contacts; and

  - Who should be notified (e.g. regulators; FBI; public relations group; media; affected business lines) and the circumstances under which they should be notified.

Operations personnel plan the work for each shift in advance to ensure that it is finished in an accurate and timely manner. However, unusual events often occur during production, which management should monitor and correct. Examples of common production events include the following:

Production Program Failure - Operations personnel should properly log and record program failures that require immediate intervention. They should also notify the appropriate personnel so proper change management procedures can be initiated. Some production failures require immediate intervention by programming staff in order to meet an important production goal (such as month-end or cycle processing). In these cases, emergency procedures, sometimes called "fire call" procedures (who to call, what to report, etc.), are invoked, and the programming staff members perform emergency repairs either at the IT operations facility or from a remote location.

Out-of-Balance Conditions - Personnel responsible for scheduling should document and correct all production processes that do not contain proper run control balances. Personnel should rerun the data to check for operator error or erroneous transactions. When totals do not balance after being re-run, operations personnel should log and record the event and notify management of the need for further investigation and resolution.

Operations Tasks Performed by Different Parties than Normal - Operations personnel customarily are cross-trained and have back-up duties in case another employee is absent or temporarily assigned other functions. For example, operators may act as back-up to tape librarians or production control analysts. In these circumstances, it may be possible for the parties to intentionally or unintentionally cause an error, fraud, or service disruption. Where back-up employees have the potential to compromise segregation of duties, management should establish mitigating controls.

Logging Issues - Most problem-solving techniques in an IT operations center depend on the ability to read, consolidate, and interpret various operations logs. Consequently, an institution should not destroy or modify its logs. Disclosure of log tampering or

manipulation is an event that requires management resolution and the involvement of the computer incident response team. Operations management should periodically review all logs for completeness and ensure they have not been deleted, modified, overwritten, or compromised.

Database Operations - Although various security devices protect databases, it may be possible for the operator to use system utilities or unauthorized compilations to modify the system. In such cases, the database may become corrupt or inaccessible. Operations management should regularly and carefully review all logs involving database programs and files and should report all unauthorized modifications to the computer incident response team.

Termination of Operations Personnel - Whenever the employment of someone with access to sensitive or confidential material is terminated for any reason, management should revoke or change all physical and logical access controls including all key locks, badges, common locks, and cyber locks. It is sound practice to ask the employee to leave at the time notice is served. If this is not practical, management should carefully monitor and review the employee's activities to ensure the protection of all data, files, and security devices. There should be written procedures to define the responsibilities for all operations, IT management, and human resources personnel when a termination occurs.

Run Time Anomalies - Management, a shift supervisor, or another independent person should review run time logs, identify any anomalies, and review their cause and resolution. It is possible for computer operators to run programs out of sequence or with improper inputs to cause error or fraud. Automated scheduling programs commonly used in large, complex institutions significantly reduce the risk of this type of event. Unexplained or inadequately explained anomalies should prompt a production rerun. Event report logs for unexplained anomalies should be forwarded to the computer incident response team for review.

Management should train and test operations personnel on their ability to recognize security events that require referral to the computer security incident response team, security guards, management, or other parties. Social engineering is a growing concern for all personnel, and in some organizations personnel may be easy targets for hackers trying to obtain information through trickery or deception.

Management should consider the safety of its employees as paramount when there is a life-threatening event. Policies and procedures should reflect this philosophy. Management should ensure it trains all operations personnel to act appropriately during significant events. Employees should also receive training to understand event response escalation procedures.

Management should properly train operations personnel to recognize events that could trigger implementation of the business continuity plan. Although an event may not initially invoke the plan, it may become necessary as conditions and circumstances change. Management should train and test institution personnel to implement and perform appropriate business continuity procedures within the timeframes of the BCP. Operations personnel should properly log and record any events that trigger BCP response and document their ultimate resolutions. Refer to the IT Handbook's "Business Continuity Planning Booklet" for additional discussion on this topic.

User Support/Help Desk

User support and help desk functions are relevant both within the institution and for third-party service providers. Financial institutions that outsource elements of IT operations may themselves be end users requiring help desk support.

User support processes and activities should ensure end users continuously have the resources and services needed to perform their job functions in an efficient and effective manner. An institution can combine user support processes with internal service level agreements (SLAs) to include such functions as root cause analysis, impact analysis, problem correction, and preventive procedures. While larger institutions frequently use internal SLAs to establish performance objectives, they are less common in smaller, noncomplex environments. Internal SLAs and user support goals and objectives should align with users' business requirements. User support and help desk functions that are not linked with user requirements contribute to diminished revenue, increased overhead, and degraded customer product and service delivery.

In larger institutions, the help desk function provides user support. The help desk typically consists of dedicated staff trained in problem resolution, equipped with issue tracking software, and supported with knowledge-based systems that serve as a reference resource to common problems. In a smaller, noncomplex institution user support may consist of a single person, a very small staff, or a contract with a support vendor.

A variety of technology solutions are available to assist in the effective management and operation of a help desk function. Dedicated internal and toll-free phone numbers support problem screening, call routing, and issue recording. Internet, intranet, and voice response unit (VRU) systems also enable problem reporting and can reduce the number of help desk operators dedicated to customer support. The help desk should record and track incoming problem reports, whether handled by live operators or automated systems. Documentation in the tracking system should include such data as user, problem description, affected system (platform, application, or other), prioritization code, current status toward resolution, party responsible for resolution, root cause (when identified), target resolution time, and a comment field for recording user contacts and other pertinent information. The tracking system helps prioritize issues, track problems through resolution, analyze the problem database for systemic concerns, and analyze help desk performance and management. Some tracking systems support Internet and intranet access so users can monitor problem resolution.

The help desk should evaluate and prioritize issues to ensure the most critical problems receive prompt attention. Key factors the help desk should consider when establishing priority include the number of users or customers affected, revenue losses, expenses incurred, or the number of SLAs affected, impacted or breached.

Help desk functions are also supported by knowledge base systems that provide support staff with action responses to common problems. Strong support functions continually update the knowledge base systems with information obtained from vendors and from the experiences of help desk staff. Because attrition rates in the help desk function can be high, a knowledge base system can ensure an institution retains knowledge and facilitates the training and development of new employees. Users may also access the knowledge base through the telephone, the Internet, or intranet to diagnose their own problems, which can contribute to a more streamlined help desk function.

Proper authentication of users is critical to risk management within the user support function. Typically, user authentication is uniform for all help desk requests. However, an institution may choose to use different levels of authentication depending upon the problem reported, the type of action requested, or the platform, system, or data involved. If the help desk uses a single authentication standard for all requests, it should be sufficiently rigorous to cover the highest risk scenarios. If the help desk function is outsourced, management should determine the servicer's information access level, assign the functions it will perform, and ensure that security and confidentiality remain in place. Refer to the IT Handbook's "Outsourcing Technology Services Booklet" for further information on vendor management.

Other Controls

Scheduling

Sound scheduling practices and controls prevent degraded processing performance that can affect response time, cause delays in completing tasks, and skew capacity planning. Management should implement policies and procedures for creating and changing job schedules and should supplement them with automated tools when cost effective. Automated tools improve management's ability to analyze and maximize scheduling efficiency. Automated scheduling tools are necessary for large, complex systems to support effective job processing. In addition to routine scheduling, these tools also assign priorities and allocate computer resources to non-routine processing. Job accounting systems are useful adjuncts to scheduling systems, helping management determine who is using the resources and for what purpose. Smaller and less complex technology systems generally have a standard job stream with little need for change.

Negotiable Instruments

Negotiable instruments require specific controls to prevent financial loss. IT operations staff members should handle or originate negotiable instruments following the institution's security procedures. Management should establish strong controls over the inventory of negotiable instruments, both in blank (unprocessed) form and after processing. Management should restrict and monitor physical and logical access to negotiable instruments and maintain a precise audit trail of issued and unissued items. Typically, negotiable instruments are numbered, and management can quickly identify missing items or sequences of items.

Additional controls are necessary if the organization uses signature writers (devices that automatically sign negotiable instruments as they are printed). At a minimum, the organization should secure the signature plates under dual control when not in use.

Risk Monitoring and Reporting

Action Summary

Management should monitor IT operations risks and the effectiveness of established controls. Institutions should use performance monitoring to provide an assessment of IT operations efficiency relative to controls. Management should use self-assessments to validate the adequacy and effectiveness of the control environment. Thorough self-assessments lead to early identification of emerging or changing risks. Internal audits are also beneficial for validating controls. Management should ensure they receive timely, accurate, and complete risk monitoring and assessment reports.

Regular risk monitoring provides management and the board with assurance that established controls are functioning properly. Comprehensive MIS reports are important tools for validating that IT operations are performing within established parameters. Examples of MIS include reports on hardware and telecommunications capacity utilization, system availability, user access, system response times, on time processing, and transaction processing accuracy. Periodic control self-assessments allow management to gauge performance, as well as the criticality of systems and emerging risks. Control self-assessments, however, do not eliminate the need for internal and external audits. Audits provide independent assessments conducted by qualified individuals regarding the effective functioning of operational controls. For additional detailed information on the IT audit function, refer to the IT Handbook's "Audit Booklet."

Management should regularly monitor technology systems-whether centralized or decentralized at business lines, support functions, affiliates, or business partners-to ensure resources are operating properly, used efficiently, and achieving the desired results predictably. Effective monitoring and reporting help identify insufficient resources, inefficient use of resources, and substandard performance that detract from customer service and product delivery. Monitoring and reporting also support proactive systems management that can help the institution position itself to meet its current needs and plan for periods of growth, mergers, or expansion of product lines.

Management should conduct performance monitoring for outsourced technology solutions as a part of a comprehensive vendor management program. Reports from service providers should include performance metrics, and identify the root causes of problems. Where service providers are subject to SLAs, management should ensure the provider complies with identified action plans, remuneration, or performance penalties. Vendor performance results should be considered in combination with internal performance as a part of sound capacity planning.

Performance Monitoring

Performance monitoring and management involves measuring operational activities, analyzing the resulting metrics, and comparing them to internally established standards and industry benchmarks to assess the effectiveness and efficiency of existing

operations. Measurable performance factors include resource usage, operations problems, capacity, response time, and personnel activity. Management should also review metrics that assess business unit and external customer satisfaction. Diminished system or personnel performance not only affects customer satisfaction, but can also result in noncompliance with contractual SLAs that could result in monetary penalties. Refer to the IT Handbook's "Outsourcing Technology Services Booklet" for more detailed information.

If economically practicable, management should automate monitoring and reporting processes. Large mainframe systems have numerous automated tools available at the application and operating system level for generating technology and process-related metrics. Mid-range systems also typically possess native capability for capturing and reporting technology. There are also after-market reporting tools and vendor-supplied performance analysis tools available for mid-range systems. Client-server systems are not always equipped with analysis and reporting tools. Often management should decide between purchasing expensive after-market reporting tools to automate the data gathering and reporting or generating the reports manually.

Much of IT operations can and should be subject to measurement based on the size and complexity of the institution. The information gained from analysis supports not only daily management of operations and early diagnostics on impending problems, but provides the baseline and trend data used in capacity planning.

Examples of technology related metrics include:

- Central processing unit (CPU) utilization by application or time of day;
- Network availability;
- On-line performance measurements including availability, response time, distribution of access types by service, or average connect time;
- VRU performance (e.g. calls answered, average talk time, average wait time, call distribution by time of day, distribution of information access requests); and
- Abnormal program endings.

Examples of operations performance metrics include the following:

- Check processing - statement processing:
  - Percent of statements mailed by internal guideline;
  - Percent of exception statements mailed by internal guideline; and
  - Percent and volume of mismatched debit and credit items.
- Item processing - proof of deposit:
  - Average fields encoded per hour;

- Ratio of errors per number of items encoded; and
- Percentage of overall rejects for items captured.

- Operations:
  - Total debit and credit transactions for the month;
  - Percent of unposted items resolved the same day received; and
  - Percent of unposted items versus total posted debits and credits.
- Imaging operations:
  - Volume and percentage by document type (e.g. new account documents, loan documents, item processing) scanned and processed within internal guidelines;
  - Volume of transactions; and
  - Number of errors reported and percent to total maintenance volume.
- Electronic funds transfer and electronic banking:
  - Number of wire processing errors caused by department and percent of total volume;
  - Number of wires not processed due to failure to execute; and
  - Number of incidents reported and compensation paid due to department processing errors.
- Technology services - IT help desk:
  - Volume of calls received;
  - Percent of calls dropped compared to internal guidelines;
  - Average incoming call wait time compared to internal guidelines; and
  - Average duration of incoming calls.
- Human resource:
  - Actual versus budgeted staff size;
  - Department or group staffing compared with averages for the two previous years and budgeted headcount; and
  - Percent of staff with required training or certification.

Capacity Planning

Capacity planning involves the use of baseline performance data to model and project future needs. Capacity planning should address internal factors (growth, mergers,

acquisitions, new product lines, and the implementation of new technologies) and external factors (shift in customer preferences, competitor capability, or regulatory or market requirements). Management should monitor technology resources for capacity planning including platform processing speed, core storage for each platform's central processing unit, data storage, and voice and data communication bandwidth.

Capacity planning should be closely integrated with the budgeting and strategic planning processes. It also should address personnel issues including staff size, appropriate training, and staff succession plans.

Control Self-Assessments

Control self-assessments validate the adequacy and effectiveness of the control environment. They also facilitate early identification of emerging or changing risks. Management should base the frequency of controls self-assessments on the risk assessment process and should coordinate the self-assessments with the internal audit plan. Control self-assessments are not a substitute for a sound internal audit program. The audit function should review the self-assessments for quality and accuracy. Internal audit also may reference the self-assessments as a part of the audit risk assessment process and may use them to plan the scope of audit work.

Depending on the size and complexity of the institution, the content and format of the controls self-assessment may be standardized and comprehensive or highly customized, focusing on a specific process, system, or functional area. IT operations management should collaborate with the internal audit function in creating the templates used. Typically, the self-assessment form combines narrative responses with a checklist. The self-assessment form should identify the system, process, or functional area reviewed, and the person(s) completing and reviewing the form. In general, the form should address the broad control topics in this booklet, including policies, standards, and procedures, as well as the specific controls implemented. Management review and analysis of reported events is an important supplement to the control self-assessment process. Forensic review of events and their resolution provides valuable insight into the effectiveness of the control environment and any need for additional controls.

Endnotes

[1]	This booklet uses the terms "institution" and "financial institution" to describe insured banks, thrifts and credit unions, as well as technology service providers that provide services to such entities.
[2]	See also section 216 of the Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C.1681w, which requires the Federal banking agencies, the NCUA, and the FTC to issue regulations requiring any person that maintains or otherwise possess consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose to properly dispose of such information or compilation.

Appendix A: Examination Procedures

EXAMINATION OBJECTIVES: Assess the quality and effectiveness of the institution's technology operations. These procedures will help disclose the adequacy of risk management of, and controls around, the institution's technology operations.

Examiners may choose to use only particular components of the workprogram based upon the size, complexity, and nature of the institution's business or upon a risk-focused examination plan.

The objectives and procedures are divided into Tier I and Tier II:

- Tier I assesses an institution's process for identifying and managing risk.
- Tier II provides additional verification where risk warrants it.

Tier I and Tier II are a tool set examiners will use when selecting examination procedures for their particular examination. Examiners should use these procedures as necessary to support examination objectives. Examiners should coordinate this coverage with other examiners to avoid duplication of effort while including the operations-related issues found in other workprograms.

Tier I Objectives and Procedures

Objective 1: Determine scope and objectives for reviewing the technology operations.

1. Review past reports for outstanding issues or previous problems. Consider:

- Regulatory reports of examination;
- Internal and external audit reports, including third-party reviews;
- Any available and applicable reports on entities providing services to the institution or shared application software reviews (SASR) on software it uses; and
- The institution's overall risk assessment and profile.

2. Review management's response to issues raised during the previous regulatory

examination and during internal and external audits performed since the last examination. Consider:

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

3. Interview management and review the operations information request to identify:

- Any significant changes in business strategy or activities that could affect the operations environment;
- Any material changes in the audit program, scope, or schedule related to operations;
- Changes to internal operations infrastructure, architecture, information technology environment, and configurations or components;
- Key management changes;
- Changes in key service providers (core banking, transaction processing, website/ Internet banking, voice and data communication, back-up/recovery, etc.) and software vendor listings; and
- Any other internal or external factors that could affect the operations environment.

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

1. Describe the operational organization structure for technology operations and assess its effectiveness in supporting the business activities of the institution.

2. Review documentation that describes, or discuss with management, the technology systems and operations (enterprise architecture) in place to develop an understanding of how these systems support the institution's business activities. Assess the adequacy of the documentation or management's ability to knowledgeably discuss how technology systems support business activities.

3. Review operations management MIS reports. Discuss whether the frequency of monitoring or reporting is continuous (for large, complex facilities) or periodic. Assess whether the MIS adequately addresses:

- Response times and throughput;

- System availability and/or down time;
- Number, percentage, type, and causes of job failures; and
- Average and peak system utilization, trends, and capacity.

Objective 3: Determine whether senior management and the board periodically conduct a review to identify or validate previously identified risks to IT operations, quantify the probability and impact of the risks, establish adequate internal controls, and evaluate processes for monitoring risks and the control environment.

1. Obtain documentation of or discuss with senior management the probability of risk occurrence and the impact to IT operations. Evaluate management's risk assessment process.

2. Obtain copies of, and discuss with senior management, the reports used to monitor the institution's operations and control environment. Assess the adequacy and timeliness of the content.

3. Determine whether management coordinates the IT operations risk management process with other risk management processes such as those for information security, business continuity planning, and internal audit.

Objective 4: Obtain an understanding of the operations environment.

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

- Computer equipment - vendor and model number;
- Network components;
- Names, release dates, and version numbers of application(s), operating system(s), and utilities; and
- Application processing modes:
  - On-line/real time;
  - Batch; and
  - Memo post.

2. Review systems diagrams and topologies to obtain an understanding of the physical

location of and interrelationship between:

- Hardware;
- Network connections (internal and external);
- Modem connections; and
- Other connections with outside third parties.

3. Obtain an understanding of the mainframe, network, and telecommunications environment and how the information flows and maps to the business process.

4. Review and assess policies, procedures, and standards as they apply to the institution's computer operations environment and controls.

Objective 5: Determine whether there are adequate controls to manage the operations-related risks.

1. Determine whether management has implemented and effectively utilizes operational control programs, processes, and tools such as:

- Performance management and capacity planning;
- User support processes;
- 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; and
- Event/problem management.

2. Determine whether management has implemented appropriate daily operational controls and processes including:

- Scheduling systems or activities for efficiency and completion;
- Monitoring tools to detect and preempt system problems or capacity issues;
- Daily processing issue resolution and appropriate escalation procedures;
- Secure handling of media and distribution of output; and
- Control self-assessments.

3. Determine whether management has implemented appropriate human resource management. Assess whether:

- The organizational structure is appropriate for the institution's business lines;
- Management conducts ongoing background checks for all employees in sensitive areas;
- Segregation and rotation of duties are sufficient;
- Management has policies and procedures to prevent excessive employee turnover; and
- There are appropriate policies and controls concerning termination of operations personnel.

Objective 6: Review data storage and back-up methodologies, and off-site storage strategies.

1. Review the institution's enterprise-wide data storage methodologies. Assess whether management has appropriately planned its data storage process, and that suitable standards and procedures are in place to guide the function.

2. Review the institution's data back-up strategies. Evaluate whether management has appropriately planned its data back-up process, and whether suitable standards and procedures are in place to guide the function.

3. Review the institution's inventory of data and program files (operating systems, purchased software, in-house developed software) stored on and off-site. Determine if the inventory is adequate and whether management has an appropriate process in place for updating and maintaining this inventory.

4. Review and determine if management has appropriate back-up procedures to ensure the timeliness of data and program file back-ups. Evaluate the timeliness of off-site

rotation of back-up media.

5. Identify the location of the off-site storage facility and evaluate whether it is a suitable distance from the primary processing site. Assess whether appropriate physical controls are in place at the off-site facility.

6. Determine whether management performs periodic physical inventories of off-site back-up material.

7. Determine whether the process for regularly testing data and program back-up media is adequate to ensure the back-up media is readable and that restorable copies have been produced.

Objective 7: Determine if adequate environmental monitoring and controls exist.

1. Review the environmental controls and monitoring capabilities of the technology operations as they apply to:

- Electrical power;
- Telecommunication services;
- Heating, ventilation, and air conditioning;
- Water supply;
- Computer cabling;
- Smoke detection and fire suppression;
- Water leaks; and
- Preventive maintenance.

Objective 8: Ensure appropriate strategies and controls exist for the telecommunication services.

1. Assess whether controls exist to address telecommunication operations risk, including:

- Alignment of telecommunication architecture and process with the strategic plan;
- Monitoring of telecommunications operations such as downtime, throughput, usage, and capacity utilization; and
- Assurance of adequate availability, speed, and bandwidth/capacity.

2. Determine whether there are adequate security controls around the telecommunications environment, including:

- Controls that limit access to wiring closets, equipment, and cabling to authorized personnel;
- Secured telecommunications documentation;
- Appropriate telecommunication change control procedures; and
- Controlled access to internal systems through authentication.

3. Discuss whether the telecommunications system has adequate resiliency and continuity preparedness, including:

- Telecommunications system capacity;
- Telecommunications provider diversity;
- Telecommunications cabling route diversity, multiple paths and entry points; and
- Redundant telecommunications to diverse telephone company central offices.

Objective 9: Ensure the imaging systems have an adequate control environment.

1. dentify and review the institution's use of item processing and document imaging solutions and describe the imaging function.

- Describe or obtain the system data flow and topology.
- Evaluate the adequacy of imaging system controls including the following:

  - Physical security;

  - Data security;

- Documentation;
- Error handling;
- Program change procedures;
- System recoverability; and
- Vital records retention.

2. Evaluate the adequacy of controls over the integrity of documents scanned through the system and electronic images transferred from imaging systems (accuracy and completeness, potential fraud issues).

3. Review and assess the controls for destruction of source documents (e.g., shredded) after being scanned through the imaging system.

4. Determine whether management is monitoring and enforcing compliance with regulations and other standards, including if imaging processes have been reviewed by legal counsel.

5. Assess to what degree imaging has been included in the business continuity planning process, and if the business units reliant upon imaging systems are involved in the BCP process.

6. Determine if there is segregation of duties where the imaging occurs.

Objective 10: Determine whether an effective event/problem management program exists.

1. Describe and assess the event/problem management program's ability to identify, analyze, and resolve issues and events, including:

- Escalation of operations disruption to declaration of a disaster; and
- Collaboration with the security and information security functions in the event of a security breach or other similar incident.

2. Assess whether the program adequately addresses unusual or non-routine activities, such as:

- Production program failures;
- Production reports that do not balance;
- Operational tasks performed by non-standard personnel;
- Deleted, changed, modified, overwritten, or otherwise compromised files identified on logs and reports;
- Database modifications or corruption; and
- Forensic training and awareness.

3. Determine whether there is adequate help desk support for the business lines, including:

- Effective issue identification;
- Timely problem resolution; and
- Implementation of effective preventive measures.

Objective 11: Ensure the items processing functions have an adequate control environment.

1. Assess the controls in place for processing of customer transactions, including:

- Transaction initiation and data entry;
- Microfilming, optical recording, or imaging;
- Proof operations;
- Batch processing;
- Balancing;
- Check in-clearing;
- Review and reconcilement;
- Transaction controls; and
- Terminal entry.

Conclusions

Objective 12: Discuss corrective action and communicate findings.

1. Determine the need to proceed to Tier II procedures for additional review related to any of the Tier I objectives.

2. From the procedures performed, including any Tier II procedures performed:

- Document conclusions related to the effectiveness and controls in the operations environment; and
- Determine and document to what extent, if any, you may rely upon the procedures performed by the internal and external auditors in determining the effectiveness of the operations controls.

3. Review your preliminary conclusions with the examiner in charge (EIC) regarding:

- Violations of law, rulings, regulations;
- Significant issues warranting inclusion as matters requiring board attention or recommendations in the report of examination; and
- Noncompliance with supervisory guidance.

4. Discuss your findings with management and obtain proposed corrective action. Relay those findings and management's response to the EIC.

5. Document your conclusions in a memo to the EIC that provides report ready comments for all relevant sections of the FFIEC report of examination.

6. Develop an assessment of operations sufficient to contribute to the determination of the Support and Delivery component of the Uniform Rating System for Information Technology (URSIT) rating.

7. Organize your work papers to ensure clear support for significant findings and conclusions.

Tier II Objectives and Procedures

The Tier II examination procedures for operations provide additional verification procedures to evaluate the effectiveness of a financial institution's technology operations. They also enable the examiner to identify potential root causes of weaknesses. These procedures may be used in their entirety or selectively, depending upon the scope of the examination and the need for additional verification. Examiners should coordinate this coverage with other examiners to avoid duplication of effort while including the operations-related issues found in other workprograms.

The procedures provided below are not requirements for control implementation. The selection of controls and control implementation should be guided by the risks facing the institution's operations environment and the size and complexity of the technology operations. Thus, the controls necessary for any single institution or any area of an institution may differ based on size and complexity of operations.

A. Operating Environment

1. Review the process in place to ensure the system inventories remain accurate and reflect the complete enterprise, including:

- Computer equipment (mainframes, midranges, servers, and standalone):
  - Vendor, model and type;
  - Operating system and release/version;
  - Processor capability (millions of instructions per second [MIPS], etc.);
  - Memory;
  - Attached storage;
  - Role;
  - Location, IP address where applicable, and status (operational/not operational); and
  - Application processing mode or context.
- Network devices:
  - Vendor, model, and type;
  - IP address;
  - Native storage (random access memory);
  - Hardware revision level;

- Operating systems; and
- Release/version/patch level.

- Software:
  - Type or application name;
  - Manufacturer and vendor;
  - Serial number;
  - Version level;
  - Patch level; and
  - Number of licenses owned and copies installed.

B. Controls Policies, Procedures and Practices

1. Determine if supervisory personnel review the console log and retain it in safe storage for a reasonable amount of time to provide for an audit trail.

C. Storage/Back-Up

1. Determine if management has processes to monitor and control data storage.

2. If the institution has implemented advanced data storage solutions, such as storage area network (SAN) or network-attached storage (NAS):

- Ensure management has appropriately documented its cost/benefit analysis and has conclusively justified its use.
- Review the implemented storage options and architectures for critical applications to ensure they are suitable and effective.
- Ensure data storage administrators manage storage from the perspective of the individual applications, so that storage monitoring and problem resolution addresses the unique issues of the specific business lines.

3. If a tape management system is in use, verify that only appropriate personnel are able to override its controls.

4. Determine if management has adequate off-site storage of:

- Operations procedures manuals;
- Shift production sheets and logs; and
- Run instructions for corresponding shift production sheets.

D. Environmental Monitoring and Control

1. Assess whether the identified environmental controls and monitoring capabilities can detect and prevent disruptions to the operations environment and determine whether:

- Sufficient back-up electrical power is available (e.g. separate power feed, UPS, generator);
- Sufficient back-up telecommunications feeds are available;
- HVAC systems are adequate and can operate using the back-up power source;
- Computer cabling is documented, organized, labeled, and protected;
- The operations center is equipped with an adequate smoke detection and fire suppression system and if it is designed to minimize or prevent damage to computer equipment if activated;
- Appropriate systems have been installed for detecting and draining water leaks before equipment is damaged;
- Management schedules and performs preventive maintenance in a reliable and secure manner that minimizes disruption to the operating environment; and
- Employee training for the use of various monitoring and control systems is adequate.

E. Physical Security

1. Review and determine whether the identified physical security measures are sufficient to reasonably protect the operations center's human, physical, and information assets. Consider whether:

- The operations center is housed in a sound building with limited numbers of windows and external access points;
- Security measures are deployed in a zoned and layered manner;
- Management appropriately trains employees regarding security policies and procedures;

- Perimeter if securities measures (e.g. exterior lighting, gates, fences, and video surveillance) are adequate;
- Doors and other entrances are secured with mechanical or electronic locks;
- Guards (armed or unarmed) are present. Also determine if they are adequately trained, licensed, and subjected to background checks;
- There are adequate physical access controls that only allow employees access to areas necessary to perform their job;
- Management requires picture ID badges to gain access to restricted areas. Determine whether more sophisticated electronic access control devices exist or are necessary;
- Management adequately controls and supervises visitor access through the use of temporary identification badges or visitor escorts;
- Doors, windows, and other entrances and exits are equipped with alarms that notify appropriate personnel in the event of a breach and whether the institution uses internal video surveillance and recording;
- Personnel inventor, label, and secure equipment;
- Written procedures for approving and logging the receipt and removal of equipment from the premises are adequate;
- Confidential documents are shredded prior to disposal; and
- Written procedures for preventing information assets from being removed from the facility are adequate.

F. Event/Problem Management

1. Determine whether there is adequate documentation to support a sound event/ management program, including:

- Problem resolution logs;
- Logs indicating personnel are following requirements in operations procedures manual(s);
- Problem resolution notifications to other departments;
- Training records indicating operations personnel training for:
- Business continuity event escalation procedures;
- Security event escalation procedures; and

- Unusual activity resolution procedures.
- Historical records of:
- Business continuity event escalation;
- Security event escalation; and
- Unusual activity event and corresponding resolution.

2. Determine whether there is adequate documentation to support a sound event/ management program, including:

- Personnel evacuation;
- Shutting off utilities;
- Powering down equipment;
- Activating and deactivating fire suppression equipment; and
- Securing valuable assets.

3. Determine whether emergency procedures are posted throughout the institution.

4. Assess whether employees are familiar with their duties and responsibilities in an emergency situation and whether an adequate employee training program has been implemented.

5. Determine if the institution periodically conducts drills to test emergency procedures.

G. Help Desk/User Support Processes

1. Evaluate whether MIS is appropriate for the size and complexity of the institution.

- Determine whether effective an MIS is in place to monitor the volume and trend in key metrics, missed SLAs, impact analysis, root cause analysis, and action plans for unresolved issues.
- Assess whether action plans identify responsible parties and time frames for corrective action;

2. Determine if the technology used to manage help desk operations is commensurate with the size and complexity of the operations. Consider:

- Help desk access;
- Logging and monitoring of issues;
- Automated event/problem logging and tracking process for issues that cannot be resolved immediately; and
- Automated alerts when issues are in danger of not being resolved within the SLA requirements, or alternatively, the effectiveness of the manual tracking processes.

3. Determine whether user authentication practices are commensurate with the level of risk and whether the types of authentication controls used by the help desk are commensurate with activities performed.

4. Determine whether the quality of MIS used to manage help desk operations is commensurate with the size and complexity of the institution. Consider the need for metrics to monitor issue volume trends, compliance with SLA requirements, employee attrition rates, and user satisfaction rates.

5. Determine whether the institution uses risk-based factors to prioritize issues. Identify how the institution assigns severity ratings and prioritizations to issues received by the call center.

6. Assess management's effectiveness in using help desk information to improve overall operations performance.

- Identify whether management has effective tools and processes in place to effectively identify systemic or high-risk issues.
- Determine whether management identifies systemic or high-risk issues and whether it has an effective process in place to address these issues. Effective processes would include impact and root cause analysis, effective action plans, and monitoring processes.

H. Items Processing

1. Determine if there are adequate controls around transaction initiation and data entry, including:

- Daily log review by the supervisor including appropriate sign-off;
- Control over and disposal of all computer output (printouts, microfiche, optical disks, etc.);
- Separation of duties;

- Limiting operation of equipment to personnel who do not perform conflicting duties;
- Balancing of proof totals to bank transmittals;
- Maintaining a log of cash letter balances for each institution;
- Analyzing out-of-balance proof transactions to determine if personnel identify discrepancies and adjust and document them on proof department correction forms. Also determine if the supervisor approves the forms;
- Balancing cash letter totals to the cash letter recap; and
- Daily management review of operation reports from the shift supervisors.

2. Determine if the controls around in-clearings are adequate, including:

- Courier receipt logs completion;
- Approval of general ledger tickets by a supervisor or lead clerk;
- Input and reporting of captured items in a system-generated report with totals balanced to the in-clearing cash letter;
- Analyzing and correcting rejected items;
- Logging of suspense items sent to the originating institution for resolution;
- Approval of suspense items by a supervisor;
- Timely transmission of the capture files; and
- Captured paid items that are securely maintained or returned to the client.

3. Determine if there are adequate controls for exception processing, including:

- Adequate and timely review of exception and management reports including supporting documentation;
- Accounting for exception reports from client institutions;
- Verification of client totals of return items to item processing site totals;
- Prior approval for items to be paid and sent to the proof department for processing;
- Accounting and physical controls for return item cash letters and return items being sent to Federal Reserve or other clearinghouse; and
- Filming of return item cash letters and return items prior to being shipped to the Federal Reserve or other clearinghouse.

4. Determine the adequacy of controls for statement processing, including:

- Logging and investigation of unresolved discrepancies; and
- Supervisor review of the discrepancy log.

I. Imaging Systems

1. Review and evaluate the imaging system. Determine:

- How the system communicates with the host;
- The system's capacity and future growth capability;
- Whether the topology is based on a mainframe, midrange, or PC;
- The vendor;
- The imaging standard being used; and
- The document conversion process.

2. Review and evaluate back-up and recovery procedures.

3. Review and evaluate the procedures used to recover bad images. Does it re-scan all or re-scan only defective images

4. Review and evaluate the process and controls over document indexing. Does the system index documents after each one is scanned or after all documents are scanned

5. Review and evaluate whether imaging hardware and software are interchangeable with that of other vendors. If they are, does management utilize normal processes or procedures when making changes or repairs? If they are not, has management identified alternate solutions should the current imaging hardware and software become unavailabl

6. Review and evaluate the access security controls, with particular attention to the following:

- Data security administrator access;
- Controls over electronic image files;
- Controls over the image index to prevent over-writing an image, altering of images, or insertion of fraudulent images;

- Controls over the index file to prevent the file from being tampered with or damaged; and
- Encryption of image files on production disks and on back-up media.

Appendix B: Glossary

Access - The ability to physically or logically enter or make use of an IT system or area (secured or unsecured). The process of interacting with a system.

Administrator privileges - Computer system access to resources that are unavailable to most users. Administrator privileges permit execution of actions that would otherwise be restricted.

Air-gapped environment - Security measure that isolates a secure network from unsecure networks physically, electrically, and electromagnetically.

Asset - In computer security, a major application, general-support system, high-impact program, physical plant, mission-critical system, personnel, equipment, or a logically-related group of systems.

Baseline configuration - A set of specifications for a system, or configuration item (CI) within a system, that has been formally reviewed and agreed on at a given point in time and that can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, or changes.

Border router - A device located at the organization's boundary to an external network.

Change management - The broad processes for managing organizational change. Change management encompasses planning, oversight or governance, project management, testing, and implementation.

Critical system (infrastructure) - The systems and assets, whether physical or virtual, that are so vital that the incapacity or destruction of such may have a debilitating impact.

Cyber event - A cybersecurity change or occurrence that may have an impact on organizational operations (including mission, capabilities, or reputation).

Data center - A facility that houses an institution's most important information systems components, including computer systems, telecommunications components, and storage systems.

Data loss prevention (DLP) - A comprehensive approach (covering people, processes, and systems) of implementing policies and controls designed specifically to discover, monitor, and protect confidential data wherever it is stored, used, or in transit over the network and at the perimeter.

Database - A collection of data that is stored on any type of computer storage medium and may be used for more than one purpose.

Direct access storage device (DASD) - A magnetic disk storage device historically used in mainframe environments. DASD may also include hard drives used in personal computers.

DSL - Digital subscriber line. A technology that uses existing copper telephone lines and advanced modulation schemes to provide high-speed telecommunications to businesses and homes.

Encryption - A data security technique used to protect information from unauthorized

inspection or alteration. Information is encoded so that data appears as a meaningless string of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using an encryption key.

End-of-life - All software products have life cycles. End-of-life refers to the date when a software development company no longer provides automatic fixes, updates, or online technical assistance for the product.

Enterprise network - The configuration of computer systems within an organization. Includes local area networks (LANs), wide area networks (WANs), bridges, applications, etc.

External Connections - An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

Fibre channel - A high performance serial link supporting its own, as well as higher-level protocols such as the small computer system interface, high performance parallel interface framing protocol and intelligent peripheral interface. The Fibre Channel standard addresses the need for very fast transfers of large amounts of information. The fast (up to 1 Giga byte per second) technology can be converted for LAN technology by adding a switch specified in the Fibre Channel standard that handles multipoint addressing. Fibre Channel gives users one port that supports both channel and network interfaces, unburdening the computers from large number of input and output (I/O) ports. Fibre Channel provides control and complete error checking over the link.

Firewall - A hardware or software link in a network that relays only data packets clearly intended and authorized to reach the other side.

Frame relay - A high-performance WAN protocol that operates at the physical and data link layers of the Open Systems Interconnect (OSI) reference model. Frame Relay is an example of a packet-switched technology. Packet-switched networks enable end stations to dynamically share the network medium and the available bandwidth. Frame relay uses existing T-1 and T-3 lines and provides connection speeds from 56 Kbps to T-1.

FTP (file transfer protocol) - A standard high-level protocol for transferring files from one computer to another, usually implemented as an application level program.

HBA - Host bus adapter. A host bus adapter provides I/O processing and physical connectivity between a server and storage. As the only part of a storage area network that resides in a server, HBAs also provide a critical link between the storage area network and the operating system and application software.

Hub - Simple devices that pass all data traffic in both directions between the LAN sections they link. Hubs forward every message they receive to the other sections of the LAN, even those that do not need to go there.

HVAC - Heating, ventilation, and air conditioning.

Hypervisor - A piece of software that provides abstraction of all physical resources (such as central processing units, memory, network, and storage) and thus enables multiple computing stacks (consisting of an operating system, middleware and application programs) called virtual machines to be run on a single physical host.

I/O - Input/output.

Infrastructure - Describes what has been implemented by IT architecture and often include support facilities such as power, cooling, ventilation, server and data redundancy and resilience, and telecommunications lines. Specific architecture types may exist for the following: enterprise, data (information), technology, security, and application.

Internet service provider (ISP) - A company that provides its customers with access to the Internet (e.g., AT&T, Verizon, CenturyLink).

Intrusion detection system (IDS) - Software/hardware that detects and logs inappropriate, incorrect, or anomalous activity. IDS are typically characterized based on the source of the data they monitor: host or network. A host-based IDS uses system log files and other electronic audit data to identify suspicious activity. A network-based IDS uses a sensor to monitor packets on the network to which it is attached.

iSCSI - Internet small computer system interface. An Internet protocol based storage networking standard for linking data storage facilities, used to facilitate. iSCSI is data transfers over intranets and to manage storage over long distances.

ISDN - Integrated systems digital networking. A hierarchy of digital switching and transmission systems that provides voice, data, and image in a unified manner. ISDN is synchronized so that all digital elements communicate in the same protocol at the same speed.

LAR - Legal amount recognition. The handwritten dollar amount of the check.

Mainframe - An industry term for a large computer, typically used for the commercial applications of businesses and other large-scale computing purposes. Generally, a mainframe is associated with centralized rather than distributed computing.

Media - Physical objects that store data, such as paper, hard disk drives, tapes, and compact disks (CDs).

Midrange - Computers that are more powerful and capable than personal computers but less powerful and capable than mainframe computers.

MIPS - Millions of instructions per second. A general measure of computing performance and, by implication, the amount of work a larger computer can do.

Mirroring - A process that copies data to multiple disks over a computer network in real time or close to real time. Mirroring reduces network traffic, ensures better availability of the website or files, or enables the site or downloaded files to arrive more quickly for users close to the mirror site.

MIS - Management information systems. A general term for the computer systems in an enterprise that provide information about its business operations.

Mobile device - A portable computing and communications device with information-storage capability. Examples include notebook and laptop computers, cellular telephones and smart phones, tablets, digital cameras, and audio recording devices.

NAS - Network attached storage. Hard disk storage set up with its own network address rather than being attached to the department computer that is serving applications to a network's workstation users. By removing storage access and its management from the department server, both application programming and files can be served faster because they are not competing for the same processor resources. The network-attached storage

device is attached to a local area network (typically, an Ethernet network) and assigned an IP address. File requests are mapped by the main server to the NAS file server.

National Institute of Standards and Technology (NIST) - An agency of the U.S. Department of Commerce that works to develop and apply technology, measurements, and standards. NIST developed a voluntary cybersecurity framework based on existing standards, guidelines, and practices for reducing cyber risks to critical infrastructures.

Network - Two or more computer systems grouped together to share information, software, and hardware.

Network administrator - The individual responsible for the installation, management, and control of a network.

Network diagram - A description of any kind of locality in terms of its physical layout. In the context of communication networks, a topology describes pictorially the configuration or arrangement of a network, including its nodes and connecting communication lines.

Operating system - A system that supports and manages software applications. Operating systems allocate system resources, provide access and security controls, maintain file systems, and manage communications between end users and hardware devices.

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

Patch - Software code that replaces or updates other code. Frequently patches are used to correct security flaws.

PBX - Private branch exchange. A telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines.

Penetration test - The process of using approved, qualified personnel to conduct real-world attacks against a system to identify and correct security weaknesses before they are discovered and exploited by others.

Platform - The underlying computer system on which applications programs run. A platform consists of an operating system, the computer system's coordinating program, which in turn is built on the instruction set for a processor or microprocessor, and the hardware that performs logic operations and manages data movement in the computer.

POD - Proof of deposit. The verification of the dollar amount written on a negotiable instrument being deposited.

POTS - Plain old telephone system. Basic telephone service.

Privileged access - Individuals with the ability to override system or application controls.

RAID - Redundant array of independent disks. The use of multiple hard disks to store the same data in different places. By placing data on multiple disks, I/O operations can overlap in a balanced way, improving performance. Since multiple disks increase the mean time between failures (MTBF), storing data redundantly also increases fault-tolerance.

Real-time network monitoring - Immediate response to a penetration attempt that is detected and diagnosed in time to prevent access.

Recovery site - An alternate location for processing information (and possibly conducting business) in an emergency. Usually distinguished as “hot” sites that are fully configured centers with compatible computer equipment and “cold” sites that are operational computer centers without the computer equipment.

Remote access - The ability to obtain access to a computer or network from a remote location.

Remote deposit capture (RDC) - A service that enables users at remote locations to scan digital images of checks and transmit the captured data to a financial institution or a merchant that is a customer of a financial institution.

Removable media - Portable electronic storage media, such as magnetic, optical, and solid-state devices, which can be inserted into and removed from a computing device and which is used to store text, video, audio, and image information. Such devices have no independent processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks (CD), thumb drives, pen drives, and similar storage devices.

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

Rlogin - Remote login. A UNIX utility that allows a user to login to a remote host on a network, as if it were directly connected, and make use of various services. Remote login is an information exchange between network-connected devices where the information cannot be reliably protected end-to-end by a single organization’s security controls.

Rogue wireless access - An unauthorized wireless node on a network.

Sandbox - A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized.

SAS 70 report - An audit report of a servicing institution prepared in accordance with guidance provided in the American Institute of Certified Public Accountant's Statement of Auditing Standards Number 70.

Scalability - A term that refers to how well a hardware and software system can adapt to increased demands. For example, a scalable network system would be one that can start with just a few nodes but can easily expand to thousands of nodes. Scalability can be a very important feature because it means the entity can invest in a system with confidence they will not quickly outgrow it.

SCSI - Small computer systems interface (pronounced ”scuzzy”). A standard way of interfacing a computer to disk drives, tape drives, and other devices that require high-speed data transfer. Also, a secondary SAN protocol that allows computer applications to talk to storage devices.

Security log - A record that contains login and logout activity and other security-related events and that is used to track security-related information on a computer system.

Server - A computer or other device that manages a network service. An example is a print server, which is a device that manages network printing.

Service level agreement (SLA) - Formal documents between an institution and its third-party provider that outline an institution's predetermined requirements for a service and establish incentives to meet, or penalties for failure to meet, the requirements. SLAs should specify and clarify performance expectations, establish accountability, and detail remedies or consequences if performance or service quality standards are not met.

SQL Injection Attack - An exploit of target software that constructs structure query language (SQL) statements based on user input. An attacker crafts input strings so that when the target software constructs SQL statements based on the input, the resulting SQL statement performs actions other than those the application intended. SQL injection enables an attacker to talk directly to the database, thus bypassing the application completely. Successful injection can cause information disclosure as well as ability to add or modify data in the database.

Storage area network (SAN) - A high-speed special-purpose network (or sub-network) that connects different types of data storage devices with associated data servers on behalf of a larger network of users.

Storage virtualization - The process of taking many different physical storage networks and devices, and making them appear as one "virtual" entity for purposes of management and administration.

Switch - A device that connects more than two LAN segments that use the same data link and network protocol.

System administration - The process of maintaining, configuring, and operating computer systems.

T-1 line - A special type of telephone line for digital communication and transmission. T-1 lines provide for digital transmission with signaling speed of 1.544Mbps (1,544,000 bits per second). This is the standard for digital transmissions in North America. Usually delivered on fiber optic lines.

TCP/IP - Transmission control protocol/Internet protocol. A communication standard for transmitting data packets from one computer to another. TCP/IP is used on the Internet and other networks. The two parts of TCP/IP are TCP, which deals with constructions of data packets, and IP, which routes them from machine to machine.

Telnet - An interactive, text-based communications session between a client and a host. It is used mainly for remote login and simple control services to systems with limited resources or to systems with limited needs for security.

Threat intelligence - The acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of action to enhance decision-making.

Total cost of ownership (TCO) - The true cost of ownership of a computer or other technology system that includes original cost of the computer and software, hardware and software upgrades, maintenance, technical support, and training.

Trusted zone - A channel in which the end points are known and data integrity is protected in transit. Depending on the communications protocol used, data privacy may

be protected in transit. Examples include secure socket layer, internet protocol security and a secure physical connection.

US-CERT - The U.S. Computer Emergency Readiness Team, part of the U.S. Department of Homeland Security's National Cybersecurity and Communications Integration Center. US-CERT is a partnership between the Department of Homeland Security and the public and private sectors, established to protect the nation's Internet infrastructure. US-CERT coordinates defense against and responses to cyber attacks across the nation.

VESDA - Very early smoke detection alert. A system that samples the air on a continuing basis and can detect fire at the pre-combustion stage.

Virtual machine - A software emulation of a physical computing environment.

Virtual private network (VPN) - A computer network that uses public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

VOIP - Voice over Internet protocol. A term used in IP telephony for a set of facilities for managing the delivery of voice information using the Internet Protocol.

Vulnerability - A hardware, firmware, or software flaw that leaves an information system open to potential exploitation; a weakness in automated system security procedures, administrative controls, physical layout, internal controls, etc., that could be exploited to gain unauthorized access to information or to disrupt critical processing.

Workstation - Any computer connected to a local-area network.

WORM (Acronym) - Write once, read many times. A type of optical disk where a computer can save information once, can then read that information, but cannot change it.

Zero-day attack - An attack on a piece of software that has a vulnerability for which there is no known patch.

Appendix C: Item Processing

Item processing operations play a critical role in an institution's ability to receive, record, and process customer transactions in an accurate, reliable, and timely manner. The item processing function converts data into an electronic format the institution's systems can capture and use in an automated environment. It is a function institutions can do internally or outsource, in a centralized or decentralized manner. This appendix reviews key item processing elements and controls.

Item processing systems convert data from source documents, including checks and customer transaction tickets, to formats that can be processed electronically. Three common methods of capturing source document data for information systems are:

- Item Magnetic Ink Character Recognition (MICR) Capture - MICR encoded documents are pre-encoded to industry standards with account number and other transaction information, except for the dollar amounts. The item processing phase encodes (prints) a dollar amount on items.
- Optical Character Recognition - Optical character recognition (OCR) reads data that is printed or typed with a special type font. Handwriting recognition systems are similar and can remove the need for a special type font.
- Direct Item Entry - Direct item entry involves manually entering data into systems. In these systems, users enter data from source documents directly into application files or onto magnetic media for subsequent capture and processing. Data sources can include teller terminals, ATMs, POS terminals, PCs, and items that are not MICR-encoded.

MICR ENCODING

MICR-encoded documents are generally pre-encoded with transit number, account number and other transaction information, except for the dollar amounts. The dollar amount is typically encoded during the proof phase of item processing. The MICR encoding area at the bottom of a check, deposit slip, loan payment coupon and other transaction documents meet national standards accepted by all financial institutions using data processing equipment.

MICR-encoded items can be machine-read and processed with little or no human intervention. Large blocks or trays of MICR-encoded documents can be passed through a high-speed reader/sorter where the MICR information on the checks and transaction tickets is captured by the computer for processing. Alternatively a multi-pocket proof machine can be used to encode and capture for computer processing. Multi-pocket proof machines and reader/sorters are described in more detail later in this Appendix. At the end of the workday, batch totals of the items captured by the reader/sorter or multi-pocket proof machine are balanced and reconciled to the appropriate applications (deposit accounting system, loan accounting system, general ledger, etc.) and balanced to the proof batch totals.

At some point in item processing an image of both the front and back of each item is

captured. Images may be captured by the multi-pocket proof machine, the high-speed reader/sorter or other equipment designed specifically for the purpose of image capture such as a microfilmer.

ITEM PROCESSING OVERVIEW

From an enterprise-wide perspective, management's main responsibility is to ensure data integrity, reliability, and accuracy with proper control procedures throughout all phases of transaction processing. Whether the item processing controls are manual or automated, they should cover transaction initiation, data entry, and computer processing. Management should update the control environment for new item processing technologies (e.g., truncation, electronic presentment and return). The board and management are responsible for adequate business continuity planning. They should also ensure the institution meets GLBA privacy and security requirements.

Technology advances continue moving the data capture point closer to the transaction initiator (i.e., customer). This trend changes item processing characteristics from a labor intensive process to a technology operations process. For example, on-line bill payment using ACH eliminates traditional item processing and emphasizes automated electronic capture techniques. The IT Handbook's "Retail Payment Systems Booklet" describes retail payment instruments; clearing and settlement processes; and risk management.

There are several different types of processing:

- Batch - In batch processing, various institution departments accumulate and process debits and credits through the proof and capture methods. Items are converted to electronic format through a reader/sorter or multi-pocket proof machine. Batch processing creates electronic batch files that are forwarded to the computer throughout the day, or at a minimum at the end of the day for creating a transaction file of the current day's activities. A new master file is created by updating the prior day's master file with the current day's transaction file.
- Real Time Data Entry - Unlike batch processing, this system permits the instantaneous updating of the master files or programs. An institution maintains a daily transaction file as back-up and a form of control. Thrift institutions and credit unions use real time systems most frequently.
- Memo Post - This system allows an institution to update information on transactions throughout the day, but still uses a batch system for actual posting. With this system institutions post transactions to a copy of the master file either individually or in batches, as deemed appropriate throughout the day, thus allowing a more accurate reflection of transactions and account balances. At the end of the day the memo-post file is deleted and actual posting occurs through normal batch processing.

PROOF OPERATIONS

Proof operations capture the transaction data in an electronic format for subsequent processing. Institutions proof work in batches as a control mechanism. Proof machines typically have built-in balancing features used during the encoding phase. The typical single pocket proof/reader/sorter operations workflow includes:

- The teller and departmental work is bundled in batches with a ticket showing the dollar total of all the items in the batch. Some financial institutions define batch processing based on a certain number of items rather than a specific time of day.
- Proof operators process the transactions. The item-processing center MICR encodes, proves, and balances the teller and departmental work before receipt by operations for batch processing.
- Proof operators consolidate batches into blocks and prepare block tickets for the total of all batches in the block.
- Proof operators process trays of block work through high-speed reader/sorters and the computer to capture the item information and transaction tickets. The reader/ sorter sorts the items and transaction tickets into different pockets based on the type of item it is.
- At the end of the workday, operations staff review financial and item capture report totals to ensure they balance and reconcile.
- All unprocessed items are returned to the originating branch or department for research and correction. Until corrected, return items are charged to a temporary control account (e.g., unposted debit/credit account, suspense items, etc.). Once the return item is corrected the temporary control entries are reversed and the item is posted to the proper customer or detail account. If systems automatically post to the general ledger, manual entry to control accounts should be restricted.
- When proof operations are complete, the transaction information in batches is transmitted directly or indirectly through magnetic media (i.e. disk or tape) to the computer for processing.

With multi-pocket proof machines, the steps may vary because multi-pocket proof machines encode, read, and sort, combining many of the steps required in single pocket proof operations into a more streamlined and simplified process.

Some institutions set up regional proof centers to reduce operating costs. These centers operate similarly to the proof department of a single branch, but perform the proof operation for many offices.

In small branches and departments lacking proof equipment, tellers or other branch personnel may develop batch control totals on transactions by running adding machine dollar totals. An independent person should review the batch totals and prepare control totals for all batches on a transmittal form. One method of establishing control in item capture is to limit the size of each batch of entries for data processing to no more than 150-300 items. For auditing purposes, small batches are easier to handle and reconcile.

PROOF MACHINES AND BATCH PROCESSING

Three basic machines are used in the proof area: the single pocket proof, the multi-pocket proof machine and the reader/sorter. Many aspects of the proof function are the same, regardless of which type of proof machine is used.

SINGLE POCKET PROOF MACHINES

Using a single-pocket proof machine, proof operators encode the dollar amount (at minimum) and put credit and debit items into one pocket. The register locks in credit entries and then subtracts debit entries or vice versa. The user cannot enter additional credits until the preceding credits and debits net to zero. This method proves each transaction as well as creates an overall debit and credit total. The single-pocket machine also typically prints information about the institution related to "bank of first deposit" requirements described in Regulation CC. Some key features of a single pocket proof machine include the following:

- The machine has a ten key keyboard;
- Function keys permit the operator to enter information such as account number, ABA transit number, transaction code, dollar amount, etc.;
- A master tape lists the information encoded on the item and any other information entered through the keyboard;
- The machine may have a small screen that displays the MICR encoding and special messages;
- The machine may have a programmable capability that defines the functions to be performed and the sequence in which they are performed;
- The machine contains a single pocket to receive processed items. Items are stacked in the sequence they are processed in;
- The machine endorses each item as it is processed; and
- The machine has a zero-balance capability that enables the operator to know each individual transaction is in balance. Debits must equal credits, and therefore net to zero. If it is not in balance, the machine locks until corrections bring the transaction into balance.

High-speed document handlers or reader/sorters are used in conjunction with the single pocket proof machine. Some characteristics of a high-speed document handler include the following:

- The MICR read-head reads the MICR-encoded items and sorts items into predefined pocket;
- The machine may operate on-line with a computer when it is part of the item processing operation. In some operations the reader/sort may produce a file that is dumped or saved to disk or tape and then transferred to the computer for processing;
- The reader/sorter can be used to sort checks into account number sequence (fine sort);
- The machine has on-line data-capture capability under computer program control;

- The machine's feed rate ranges from 600 to 2400 documents per minute;
- The number of pockets items that are sorted into may range from 6 to 36 depending on vendor and model;
- An ink-jet sprayer or stamp prints the document identification number on the reverse side of the document;
- The machine may have a high-speed microfilm unit;
- The machine may have a high-speed endorsement capability; and
- A rack above the document handler pockets stores processed items as pockets fill up.

Upon receipt at item processing operations, personnel prepare the branch or department work for processing on high-speed MICR reader/sorter equipment. Each batch of debits and credits should contain a batch header or adding machine tape listing indicating the total dollar amount of the items included in the batch.

Usually, a clerk encodes a batch number on a batch header card or creates a batch header and assembles the batches into blocks of items. A header card is included with each block that contains a block number and the total dollar amount of all batches in the block. Using a standardized form to record the batch number and corresponding batch total is an effective control over batches of work. Additional data integrity processing controls include using hash totals, block and record counts, and cross footing balancing.

The reader/sorter, which is a high speed document handler, reads the MICR encoded information on documents and captures it in a form the computer will be able to understand and process. The reader/sorter also sorts the documents into groups based on the type of document.

MULTI-POCKET PROOF MACHINES

Multi-pocket proof machines encode and sort items and may be used in place of the single-pocket proof machine and reader/sorter. When operating a multi-pocket proof machine, the operator should encode the item, determine if it is a debit or credit and classify the transaction by type (on-us check, foreign check, cash-in or cash-out, general ledger, etc.). Each pocket creates a record for the dollar amount of each credit and debit sorted to it. Periodically, operators take each pocket's entries and sum-totals entries run to that pocket. Multi-pocket proof machines capture information in an electronic format, eliminating the need to run items through the reader/sorter. Electronic batch files may be forwarded to the mainframe throughout the day or held to the end of the day to complete the transaction processing.

- A multi-pocket proof machine has all the features and functions of a single pocket proof machine, but with the following additional features:
- The multi-pocket machine sorts items to multiple pockets, based on the type of item and disposition;

- The machine captures, records, and transmits data to the computer or onto magnetic media as items are processed;
- The machine has an ink jet sprayer or stamp that prints the document identification number on the reverse side of the document;
- The machine may have a high speed microfilm unit; and
- It can be used to sort checks into account number sequence (fine sort).

BATCH PROCESSING

Throughout the day, as the computer receives batches, it accumulates dollar totals for posting to the respective general ledger accounts. At the end of the day, after all batches have been received, the computer operator will proceed with processing the transaction. Processing involves posting all debits and credits to the specific accounts and developing new account balances. Rejected items are typically held overnight in general ledger suspense accounts and are resubmitted with the next day's work. At some point in item processing a picture of both the front and back of each item is captured. This may be done several ways. A stand-alone microfilmer, or a multi-pocket proof machine or reader/sorter with a microfilmer attached to it or other equipment designed specifically for the purpose of image capture may be used.

REJECTED ITEMS

The operations area should maintain a list of rejected items and send them to reconcilement clerks. This hard copy listing should contain the following:

- A batch number;
- A block number;
- An item capture number (each item is sequentially numbered on some systems for tracing purposes);
- An account number;
- The dollar amount of each item;
- Batch and block dollar control totals; and
- Out of balance dollar amounts.

The departments submitting work should list total dollar amounts on a transmittal form for all batches submitted. The transmittal form provides total batch debits and credits for each pocket. This control feature creates an audit trail to reconcile the general ledger and gives personnel dollar totals to balance the item processing capture runs. User departments and the proof areas should develop control totals since these amounts form the basis for all internal accounting controls (i.e., subsequent run-to-run totals and final output records).

OPERATING CONTROLS

Item processing controls are important because item processing involves source data, large dollar total amounts, and high volume activities. Item processing control weaknesses can lead to losses from unintentional errors, fraud, and poor business continuity planning. Institutions should recognize the risks and incorporate item processing technologies that result in improved efficiencies, better BCP, and reduced fraud losses. Management should address item processing controls during data capture, balancing, and reconcilement.

TRANSACTION CONTROLS

Important internal control considerations include the following:

- Segregation of duties;
- Appropriate oversight of transaction input, processing, and output functions;
- Well-defined standards for overnight control of dollar totals for rejects and holdover items;
- Appropriate reconcilement and balancing of work returned from processing to the previously established control totals;
- Expeditious clearing of exception items (exceptions are contrary to effective control and create potential risk to the financial institution); and
- Review exception reports by operations officers and supervisors.

Management should ensure segregation of duties to reduce potential fraud losses. Item processing automation and reduction in staff increases the importance of segregation of duties because critical functions are concentrated in fewer hands. Typically, departments achieve segregation of duties by ensuring an individual is not responsible for any two of the following:

- Input preparation and operating data input equipment;
- Operating computer equipment;
- Operating sorting equipment;
- Approving rejects for re-entry; and
- Reconciling output.

DIRECT ITEM ENTRY - CONTROLS

Direct item entry systems need enhanced controls to ensure data integrity because items are manually input for capture and processing without going through proof. Prompt input error notification can significantly reduce item rejects. The risk of fraud or error increases when operators convert data from source documents to electronic. Direct item entry software programs and system software can provide a high degree of error control by using the following techniques:

- Character/field count - A check of character and field count totals for comparison against original data entry totals.
- Checks for completeness - Ensuring users fill all entry fields using programmed checks.
- Check digits - The system performs an algorithmic operation on numeric fields and the results validate the account numbers.
- Dollar and item count totals - A necessary tool to balance dollar and non-dollar transactions to established control totals.
- Dual-field entry - When the same input appears twice, processes check to ensure both fields match.
- Reasonableness checks - Programmed comparisons of data entered to predetermined absolute values or relative limits of reasonableness.
- Sequence checks - Processes check key record fields for proper data entry sequence.
- Truncation fields - An automatic provision that provides round off or truncation rules for fields that exceed maximum length.
- Verification check - Systems query the user to validate the input data.

PROOF AND CAPTURE SORT CODES

Like mainframes, proof and capture machines require some programming to ensure items are properly handled. These are commonly referred to as proof and capture sort codes. These codes ensure the physical items are sorted to the appropriate pocket on the reader/sorter or multi-pocket proof machine. Items miscoded and thus sorted to the wrong pocket can affect balancing. These codes need to be backed up and included in disaster recovery procedures as they would need to be transferred to any new machine if the machines at the institution are unworkable or inaccessible. Additionally, it is important the institution use proper change control procedures, as described in the IT Handbook's "Development and Acquisition Booklet", when code changes are required.

HOLDOVERS

Holdover transactions occur when an institution is unable to process the volume of items, usually checks, within the date received. This may occur when a customer brings in a

large volume of checks to be credited to his or her account before the close of business, and the institution does not have time to process all the items. If this is allowed, the deposit ticket is processed on the date received with an offsetting debit posted to a holdover account. The actual offsetting items (checks) are secured for processing the next day. The next day the checks are processed (debits) with the credit going to the holdover account to zero out the debit there. If this occurs on a regular basis, an institution should have an agreement with the customer spelling out the conditions, especially if the transaction is out of balance with the deposit slip, when the checks are processed the following day. If this occurs on an infrequent basis, the institution should instruct the customer that the deposit will be posted the following day and not allow a holdover to occur. Of note, holdovers should only be performed for customers with good credit relationships. If examiners see this occur during an examination, they should ensure the items held over are processed the next day, that the holdover account is regularly balanced, and no balances are maintained in the holdover account for more then one business day.

BALANCING AND RECONCILEMENT

The balancing and reconcilement process ensures captured item data is accurate and reliable. These are also critical phases in item processing to identify exceptions and potential losses caused by damaged items, input error, and fraud.

BALANCING RECONCILEMENT

Reconcilement clerks balance each batch of debits and credits to the batch capture reports using a reconcilement form. The reconcilement clerk collects rejected entries (i.e., items not captured) as he or she balances each batch. Additionally, the item processing systems generate rejected entry reports with each item's dollar amount. The department that handles a rejected item researches, corrects, and then resubmits each item with the normal processing work. The reconcilement clerks complete final balancing processes and return unprocessed items to the user department for additional research and correction.

Personnel should segregate or identify all rejected, unread, unposted, and uncaptured items. The review clerk either corrects the item for resubmission and posting or returns it to the user area for disposition. The department manager or supervisor should review all reject re-entry items to ensure proper correction. This control environment prevents unprocessed items from reappearing for extended periods.

OCRR AND CONTROLS

Reader/sorter operators or other personnel have an opportunity to repair rejected items before they get to a reconcilement clerk. Most reader/sorters will allow for on-line correction, repair, and re-entry (OCRR) of unreadable or missing items from the MICR line. A list of the rejected items is presented on a CRT screen. The operator can then provide the missing or inaccurate information. After repairing a batch, the operator should forward the data for supervisory review prior to resubmission. Most software limits correction to the problem fields, but some do not. Management should require audit logs that identify the operator name, time of entry, and a list of repairs to mitigate error or fraud.

GENERAL LEDGER RECONCILEMENT AND FINAL REVIEW

The general ledger reconcilement process involves reconciling final daily item processing entry totals to the respective general ledger control account. Personnel should make

adjustments for missing entries, extra entries, and rejected or non-posted items. Key controls aspects include the following:

- Reconciling transactions against source documents;
- Reviewing the transaction reconcilement form for accuracy;
- Completing an additional reconcilement form for balancing the trial balance and other report totals to the general ledger;
- Maintaining adequate suspense account, rejected, and holdover item control processes;
- Reviewing exception reports (e.g., overdraft, large item, stop/hold, uncollected funds, kiting suspects);
- Comparing larger dollar items to the daily posting journal and signature card;
- Returning forged, dishonored, or otherwise invalid items within time limits specified by the Uniform Commercial Code, clearing house associations, and federal rules and regulations; and
- Auditing to ensure the control environment remains effective and appropriate.

MANAGEMENT REPORTS

Management should identify reports that facilitate item processing management. Management performance monitoring and control reports can include the following:

- Item processing volumes;
- Item processing systems capacity;
- Processing efficiencies (e.g., items per hour, items per employee);
- Courtesy Amount Recognition/Legal Amount Recognition (CAR/LAR) rejection rates;
- CAR/LAR false acceptance rates (i.e., processed items subsequently returned due to errors missed using automated solutions);
- Error rates;
- Reject volumes; and
- Exception reports

BUSINESS CONTINUITY PLANNING

Item processing business continuity planning should consider item handling from the transaction initiation point through final general ledger reconciliation. Item processing

often involves moving and handling large amounts of information. Consequently, if a disruption or disaster occurs, management may have a difficult task restoring items in process. Management should assess the risk involved in each item processing area and develop appropriate continuity plans. Senior management should understand the risks involved in areas where the institution does not have or cannot create reference copies to recreate transactions.

Appendix D: Advanced Data Storage Solutions

In the past, when the processing of all institution data was primarily in the mainframe environment, all data was stored centrally within the IT operations center on magnetic media (tapes and disks) directly connected to the processor. The introduction of PCs and LANs into the processing environment effectively decentralized information systems processing, bringing the computing power and data storage closer to the end user. With the subsequent proliferation of LANs and WANs, management of the increasing volume of data and the associated storage resources has become more challenging. Nevertheless, small, noncomplex institutions can still satisfactorily store data locally at the PC, network server, mid-range or mainframe level, with oversight responsibility assigned to local users, administrators, or operations personnel. Common storage solutions include the following:

- PC, server, and midrange: hard drive, floppy discs, compact discs (CDs), and digital video discs (DVDs); and
- Archival systems: computer output to laser disk (COLD), digital audio tape (DAT), and digital linear tape (DLT).

Within the traditional data center environment using mainframe or mid-range computers, data storage options include arrays of direct access storage devices (DASD), which are large drives of stacked magnetic disks. Other storage options include magnetic tape cartridge devices, automated tape library (ATL), and "jukeboxes". An ATL is a storage unit that contains one or more tape drives, a robotic arm, and a shelf of tapes. The ATL, also called a tape silo, is able to load and unload tapes into the tape drive from the shelf without operator intervention. More sophisticated tape libraries are able to identify each tape; for example, the robotic arm can use a bar-code reader to scan each tape's barcode and identify it. Jukeboxes, containing a series of optical disks, are conceptually similar to ATL units.

Larger, more complex institutions are turning to newer automated data storage solutions to meet their needs. Decision factors motivating the selection of automated storage solutions include:

- Significant growth in the volume of data (particularly mission critical data);
- The need to have data continuously available, and the resultant shrinking timeframe available for data back-up;
- The need for scalability to very large sizes; and
- The need to facilitate data back-up for business continuity purposes.

Storage Area Network

A storage area network (SAN) is a collection of interconnected storage devices, ultimately connected to host systems over a high-speed optical network. SANs allow institutions to centralize data and connect servers across the network to that data. SANs provide the ability to incorporate multiple storage solutions with different performance characteristics into a single storage pool. Management can map application requirements to the most appropriate storage option. Applications that are throughput-intensive may benefit from one configuration, while applications that are update-intensive may benefit from another configuration. SAN administrators should manage storage from the perspective of the individual applications, so storage monitoring and problem resolution can appropriately address the unique issues of the specific business lines. SANs support disk mirroring, back-up and restoration capabilities, archiving and retrieval of data, data migration from one storage device to another, and data sharing among servers within a network.

Many large institutions can benefit financially from the deployment of a SAN. SANs have a very high return on investment, which makes the total cost of ownership less. The operational benefits of SANs include:

- Greater speed and performance through Fibre Channel protocol;
- Increased disk utilization (multiple servers access the same physical disk resulting in more effective allocation of free space);
- Higher availability of storage through multiple access paths (multiple physical connections from multiple servers);
- More efficient staff utilization (enabling fewer people to manage more data);
- Enhanced data recovery capabilities (mirroring capabilities);
- Improved reliability through clustering (using shared drives, if one storage device fails, another takes over); and
- Non-disruptive scalability (storage devices can be added to a SAN without affecting other network devices).

A SAN has three physical layers. The top layer, or host layer, consists of the servers. The major components of the host layer are the host bus adapter (HBA) or I/O adapter card, through which the server connects to the SAN and the fiber optic cables. The middle layer is the fabric layer, which includes hubs, switches, and additional cabling. A hub is a device that physically connects cables. A switch also physically connects cables, but has the additional functionality of being able to intelligently route data from the host layer to the storage layer. The third layer is the storage layer where all the storage devices and data are located.

Several protocols are used in SANs. Protocols enable computer systems to communicate with other devices. Protocols are divided into layers and logically sequenced into a stack. Each layer provides different functionality. The bottom layer is the physical layer, which includes all hardware (cabling, hubs, and switches). The software layers of the protocol stack lie on top of the physical layer. The primary SAN protocol is Fibre Channel, since it supports both peripheral interfaces and network

interfaces. Fibre Channel protocol actually includes two protocols: Fibre Channel Arbitrated Loop (FC-AL), which works with hubs; and Fibre Channel Switched (FC-SW), which works with switches. Fibre Channel is the foundational protocol in SANs, as other protocols such as small computer system interface (SCSI) run on top of it. SCSI allows computer applications to talk to storage devices.

Fibre Channel SANs employ fiber optic cables, which use pulses of light to transmit data. Due to the fast speeds, this is the ideal medium for data communications. (In a vacuum, light travels approximately 300,000 kilometers per second. A strand of fiber optic cable, whose core consists of tiny strands of glass, slows the speed to about 200,000 kilometers per second due to the impurities of the glass.) The movement of data from server to the data storage device requires significant bandwidth. SANs generally operate within the 1-2 gigabyte per second bandwidth, although faster speeds are being introduced.

Another performance consideration in SANs is latency, which is the time needed for data to travel from one point to another. Latency can be caused by too much distance between the server and the storage device or by too many hops between the servers and the storage device. Each hop adds approximately a one-millisecond delay. Proper planning and design of a SAN is essential to minimize the number of hops. One or two hops are normal. Additional hops add latency and degrade performance.

In order to reduce the risk of major system problems, redundancy is an important consideration in designing SANs. A SAN should have at least two separate fabrics (cabling, hubs and switches), redundant HBAs in each server, and fail-over and/or load balancing software on the servers for the HBAs.

Redundant Array of Independent Disks

Redundant Array of Independent Disks (RAID) configurations are often incorporated into SANs. RAID refers to multiple individual physical hard drives that are combined to form one bigger drive, known as a RAID set. The RAID set represents all the smaller physical drives as one logical disk to the server. The logical drive is a Logical Unit Number (LUN). RAID configurations typically use many small capacity disks to store large amounts of data in order to provide increased reliability and redundancy. RAID is another form of DASD. It offers improved performance because the server has more disks to read from when data is accessed. Availability is increased because the RAID controller can recreate lost data from a failed drive by using parity information from the surviving disks, which is created when the data is initially written to the disk. Management can use a variety of different storage techniques (RAID types) to achieve different levels of redundancy, error recovery, and performance.

Network Attached Storage

Another concept in data storage is Network Attached Storage (NAS). NAS enables server connections and the movement of data between servers over a standard Internet Protocol network. A NAS usually resides on a LAN, while a SAN is its own network. Institutions can use NAS as primary or secondary storage within a network. The strength of NAS is its ease of installation as another node on the network. However, introducing an additional network node may reduce performance. An alternative approach to NAS uses Internet Small Computer Storage Interface (iSCSI) protocol, which connects servers to storage devices using a standard TCP/IP network adapter. iSCSI encapsulates standard SCSI storage blocks into the IP protocol, allowing the transmission of block-based SCSI data to storage devices using a standard IP network. The advantages of iSCSI include ease of deployment, the ability to leverage existing

knowledge of IP networking, and reduced cost as opposed to a Fibre Channel SAN.

Storage Virtualization

As large institutions wrestle with growing volumes of data, the concept of storage virtualization is gaining prominence. Storage virtualization takes many different physical storage networks and devices and makes them appear as one entity. This offers institutions the ability to centralize and streamline storage services, thereby providing an efficient means of managing enterprise-wide storage across multiple platforms. Storage virtualization adds additional staff efficiencies by allowing fewer people the ability to manage more data. Storage virtualization is merely a part of the network virtualization concept, in which storage and computing capacity are centralized into a single virtual location so that processing capacity and other network administration tasks can be managed more effectively.