iad INTERNAL AUDITORS DIVISION
An Affiliate of SIFMA

Internal Audit Guidelines
Data Center

November 2007

The Audit Guidelines (the "guidelines") are intended to provide members of the Internal Auditors Division (“IAD”), an affiliate of the Securities Industry and Financial Markets Association (“SIFMA”) with information for the purpose of developing or improving their approach towards auditing certain functions or products typically conducted by a registered broker-dealer. These guidelines do not represent a comprehensive list of all work steps or procedures that can be followed during the course of an audit and do not purport to be the official position or approach of any one group or organization, including IAD or any of its divisions or affiliates. Neither IAD, nor any of its divisions or affiliates, assumes any liability for errors or omissions resulting from the execution of any work steps within these guidelines or any other procedures derived from the reader's interpretation of such guidelines. In using these guidelines, member firms should consider the nature and context of their business and related risks to their organization and tailor the work steps accordingly. Internal auditors should always utilize professional judgment in determining appropriate work steps when executing an audit.

iad INTERNAL AUDITORS DIVISION
A Division of SIFMA

TABLE OF CONTENTS

iad INTERNAL AUDITORS DIVISION
A Division of SIFMA

I. Introduction and Background

I. INTRODUCTION AND BACKGROUND

A. Overview

A data center comprises the facilities (computers, storage and print facilities, networks (i.e., communications equipment), etc.) and premises (i.e., computer room, archives, offices, etc.). A data center may be manned continuously (with staff working shifts) or else at times when it is not manned there is an on-call service. Generally a company's data processing does not rely exclusively on the central information technology (IT) equipment in a computer center, but on a multitude of local IT systems that are connected to it. However, the concentration of IT equipment and data in a computer center means that the amount of potential damage that could occur is much greater than where data processing is decentralized.

In contrast to the protection requirement of a server room, many IT security measures are not simply optional for a computer operations center but mandatory. These include, for example, an appropriate alarm system and an alternative power supply. For such secure IT operations devices for the early detection of fires through monitoring of the hardware use and the raised floor is effective and economical. Automatic indoor fire extinguishing systems are primarily directed at the building itself.

The guidelines described in this document describe a practical approach to operational risk management that emphasizes the daily operations and the tactical activities associated with the overall capture, transmission, processing, and storing of a firm’s information assets at an IT data center. Information is one of the most important assets of a firm, and IT data center operations should process and store information in a timely, reliable, secure, and resilient manner.

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, 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.

An IT audit should cover the following data center environments:

- Complex core operations at centralized data center locations;
- Distributed data center operations at lines of business;
- Microcomputers used as standalone processors;
- Support functions; and
- Affiliates under the enterprise umbrella.

B. Examination Objective

An IT data center audit will assess the quality and effectiveness of the firm's IT data center operations and help disclose the adequacy of risk management of, and controls around, the firm's data center operations. IT data center operations-related risks require controls that are consistent with the nature and complexity of the specific technology environment. The objectives of the audit are to ensure that:

- Management has taken appropriate and timely action to address the deficiencies noted in prior audit and examination reports.
- Senior management develops and implements long- and short-range plans that fulfill the firm's mission and goals.
- Senior management has appointed a planning or steering committee to oversee the information services function and its activities.
- Segregation of duties is adequate.
- Management assumes full responsibility for formulating, developing, documenting, promulgating, and controlling policies, and that procedures are in place to determine that policies and procedures are being followed. This would include change management, scheduling, tape library, and other operations procedures.
- The firm is in compliance with external requirements (regulations, laws, etc.).
- Management of the IT function schedules routine and periodic hardware maintenance to reduce the frequency and impact of performance failures. Problems and incidents are resolved, and the cause investigated to prevent any recurrence.
- An uninterruptible power supply, batteries and generators are available to secure against power failures and fluctuations.
- Appropriate physical security and access control measures have been established.
- System security is adequate to safeguard information against unauthorized use, disclosure or modification, damage or loss.
- For each relationship with a third-party, hardware, and software provider, a formal contract is defined and agreed upon.
- Adequacy of insurance coverage for various aspects of the computer operations center. This would include employee fidelity, equipment and facilities, errors and omissions, extra expenses, etc.
- Staff skills and resources are maintained at adequate levels to fulfill their duties and obligations and to perform their responsibilities and the objectives described above.

C. Audit Scope

The scope of the audit will be established by focusing on those factors that present the greatest degree of risk to the firm's IT data center operations and at a minimum will include the following areas that are detailed in the next section, Audit Risks. Additionally the Audit Guidelines cover specific audit areas for each risk.

- Executive Sponsorship for Accountability, Ownership, and Awareness
- IT Business Plan
- Environmental Survey (a comprehensive understanding of the institution's operations universe)
- Asset Inventories
  - Hardware Inventory
  - Telecommunications Inventory
  - Software Inventory
  - Storage Media Assets and Data Content
- Risk Identification and Assessment
  - Review of Controls to Mitigate Risk
  - Risk Monitoring and Reporting
- Review of Specific Data Center Controls to Mitigate Risk
  - IT Data Center Business Continuity Plan
  - Data Center Security
  - Environmental Hazards
  - Equipment Maintenance
  - Data Center Staffing and Training
  - Data Center Operations Procedures
  - Program Change Controls and Procedures
  - Monitoring
  - Outsourced and Vendor Activities
  - Global, Federal, State and Local Regulations
  - Insurance
- Prior Audit Issues

D. Audit Risks

The following typical risks are assumed to be relevant to the audit of a data center:

Executive Sponsorship for Accountability, Ownership, and Awareness

A successful data center audit requires executive support of the audit process. As with any other firm initiative, if the ownership and accountability of the audit are not defined clearly from the beginning and communicated to appropriate staff, the audit may not operate as effectively as it could. Areas of concern include:

- Executive responsibility for the audit process
- Allocation of sufficient resources and budget for audits
- Awareness by data center personnel of management's role in the audit process

IT Business Plan

The audit process must always begin with the firm's IT business plan. This provides the framework for conducting an audit. An audit usually begins by reviewing the plan along with its associated policy, procedures, and standards for currency and relevance. If these are out-of-date, ensure that a new risk assessment is completed so the IT business plan can be updated appropriately. The IT business plan must also be consistent with and support the firm's overall business strategy and objectives. Failure to align IT strategy, resources, and support infrastructure with the business strategy may result in missed business objectives and lost opportunities for the firm.

Environmental Survey

The environmental survey, along with the technology asset inventory, provides the foundation for the risk identification and assessment processes and is the next critical building block in a successful data center audit. A comprehensive understanding of the institution's operations universe and technology environment includes documenting data center resources and physical locations along with the infrastructure (air conditioning, electricity, etc) needed to support physical locations. Environmental concerns are a high priority, with many firms evaluating data center management solutions on the ability to save space and power. A well maintained environmental survey can support the main business drivers of reducing costs and creating higher efficiency through better utilization of resources and more flexibility, and support for multiple applications. An environmental survey can achieve these objectives by reducing space requirements of servers, decreasing power consumption, and reducing cooling costs. The top three challenges associated with achieving these efficiencies through well planned management of the IT environment are lack of expertise, difficulty managing large number of servers, and multiple points of failure.

Asset Inventory

Alongside the environmental survey, management should also perform and maintain an inventory of specific information technology assets. The inventory should also track the capture, processing, flow, and storage of data and other business processes throughout the firm that are dependent upon data center assets that may be physically located outside of the data center. A well maintained asset inventory will allow IT data center management to control asset costs more effectively, manage hardware and software licensing and software upgrades, prevent theft and security breaches, reduce personal property taxes on assets, reduce risks of Sarbanes-Oxley non-compliance, increase profitability and shareholder value through improved asset inventory and better operational and capital spending decisions, and protect business investments by ensuring data accuracy in corporate databases.

The asset inventory includes:

- Hardware Inventory
- Telecommunications Inventory
- Software Inventory
- Storage Media Assets and Data Content

Risk Identification and Assessment

Based on the environmental survey and asset inventory firms should then conduct a risk identification and assessment against the physical locations, physical assets, and the business processes and procedures of the data center. The assessment should also include steps that can be taken to mitigate identified risks. Senior management can use risk assessment data to make informed risk management decisions based on a full understanding of the operational risks. Regardless of the level of complexity of an IT data center, the risk identification and assessment process should be formal and should adapt to changes in the IT environment. An audit of this process should measure the effectiveness of the process by evaluating management's understanding and awareness of risk, the adequacy of formal risk assessments, and the effectiveness of the resulting policies and internal controls. Failure to identify and address risks to IT operations could result in the loss of operational capabilities that may introduce subsequent financial and integrity risks to the firm.

Review of Specific Data Center Controls to Mitigate Risk

The following typical risks are assumed to be relevant to the IT protection of a data center:

IT Data Center Business Continuity Plan

An IT Data Center Business Continuity Plan ("BCP") enables a Firm and its employees to survive a disaster and to re-establish critical data center operations required to support the business within the timeframes set out by the business managers. A disaster could result in short-term or long-term delays in production processing. Both types of delays could result in different recovery methods (i.e., normal backup / recovery vs. invoking "hot-site" recovery).

A BCP should ensure:

- The development, implementation, testing and maintenance of an IT Data Center business continuity and emergency response plans that enables data center management to protect its assets and meet its business recovery objectives.

- Prevention and mitigation activities to reduce the likelihood and impact of a disruption.

- The IT Data Center business continuity and contingency plans (i.e., mainframe and distributed) support business recovery objectives.

- Addresses a process for reconstruction of physical data center location that will be needed to continue operations in the event that a primary location is destroyed or uninhabitable for a long period of time.

Data Center Security

Because of the capital invested in IT and because of its importance to the continued operation of any organization, IT facilities should be protected from most hazards. This is true of both the large mainframe installations where custom-built data centers are used and the newer client/server installations where server equipment is no less critical. The hazards we are protecting against are both accidental and deliberate. Accidental hazards include fire and flood, and the like. Deliberate hazards are the intentional acts of compromise.

Because the computing facilities of any organization represent a considerable investment and because their continued operation is often vital to the continued viability of the organization, all computing equipment should be protected against physical threats that could damage or destroy that equipment. In addition, as the computer center is a sensitive area, we should limit the number of people who have access to the building and to the computer facilities themselves.

Physical security is implemented using the concept of defense in depth. This organizes security in concentric layers from the outside to the inside. Physical protection of the facilities is achieved by the design of the facilities and physical access control.

<u>Unauthorized entry into a building</u> – A number of threats to IT systems, e.g. theft or tampering, could be caused by unauthorized entry into the data center. The objective of a break-in could be theft of IT components or other items that are easy to dispose of, but equally the intruder might be seeking to copy or tamper with data or IT systems. Tampering that it is not obvious can be far more harmful than direct acts of destruction. Damage to property can occur simply as the direct consequence of unauthorized entry, as windows and doors are opened by force and damaged, so that they have to be repaired or replaced.

<u>Unauthorized admission to specific rooms requiring protection</u> - If unauthorized persons enter protected rooms; hazards may be entailed not only by deliberate acts, but also by accidental acts. Disruption is caused merely by the fact that checks must be made for potential damage as a result of the unauthorized access.

<u>Theft</u> – Theft of IT equipment, accessories, software or data results not only in the expense of having to replace the equipment or to restore it to working order, but also in losses resulting from lack of availability. In addition, loss of confidential information and the results of this can be damaging. As well as expensive IT systems, mobile IT systems that are easy to transport inconspicuously are often targeted for theft.

<u>Attack</u> - There are multiple technical possibilities for carrying out an attack: throwing bricks; use of explosives; use of firearms; arson. Whether an IT operator will be exposed to the risk of attack,

and to what extent, will depend on the site and environment of the building and also, to a great extent, on his/her tasks and on the political/social climate. When assessing the risk of politically motivated attacks, advice can be obtained from the local criminal police office or from the federal criminal police office.

Environmental Hazards

Lightning – The occurrence of lightning during a thunderstorm is a major threat to a building and the IT facilities accommodated there. If a building is directly hit by lightning, damage will be caused by the lightning strike. This may include physical damage to the structure (roof and façade), damage caused by resultant fire, or over voltage damage to electric devices.

Fire - Apart from the direct damage caused by fire to a building or its equipment, there may be consequential damage, the impact of which can be disastrous, especially for IT systems. Factors that help fires to spread include:

- Wedging fire doors open
- Improper storage of combustible materials
- Failure to observe relevant standards and regulations
- Absence of fire detection devices
- Absence of hand fire extinguishers and automatic quenching systems
- Deficient fire prevention (e.g. lack of fire insulation along cable routes)

All computer installations should take adequate precautions to ensure that fire can be prevented, detected and extinguished. Many types of extinguishing systems will be encountered including Halon, CO_2 and water.

Flood and Water - There is a danger that water will damage supply facilities or IT components (e.g. short-circuit, mechanical damage, rust, etc.) or render them unserviceable. Where central supplies for the building (main power distributor, trunk distribution frame for telephone, data) are accommodated in basement rooms without automatic water removal, the ingress of water can cause major damage. The uncontrolled flow of water into buildings or rooms may, for instance, result from:

- Rain, floods, inundation
- Disruption of water supply and sewerage systems
- Defects in the heating installation
- Defects in air conditioning systems connected to the water supply
- Defects in sprinkler systems

Water detectors are essential in mainframe installations especially under raised floors. Care needs to be taken to ensure that water pipes are not routed across computer rooms within false ceilings.

Climate and Humidity - Every device has a temperature range within which its proper functioning is ensured. If the room temperature exceeds that range in either direction, the result may be a discontinuity of service and failure of devices. In a server room, if ventilation is insufficient, the admissible operating temperature of the devices may be exceeded.

Power Outage and Surges - Every device has an electrical tolerance within which its proper functioning is ensured. If the power supply allows electrical currents to exceed that range in either direction the device may fail resulting in an interruption of essential services. A steady and uninterruptible power supply must be maintained to the data center and all its components to insure continuity of service.

Equipment Maintenance

Equipment maintenance of computer, network, and telecommunications equipment is critical to the smooth running of data center operations. Performing regularly scheduled maintenance which includes cleaning, checks and updates on equipment will help prevent system problems instead of waiting until failures to occur. Risks mitigated by having a scheduled maintenance program for computer equipment include equipment outages, costly repairs, excessive down time, and loss of data that may all potentially impact business operations.

Failure of the IT system – Failure of a single component in an IT system can result in a failure of the entire IT operation. Such failures are especially likely to occur where faults develop in components that are central to the IT system. Failure of components of the technical infrastructure / environment, for example air conditioning or power supply facilities, can also help induce an IT system failure.

Disruption of power supply - However secure a power supply is, power failures could be a regular occurrence. In most cases of power failure, the power is down for less than a second so that it can escape unnoticed. Interruptions can also be caused by shutdowns for unannounced maintenance work or by cables damaged during underground engineering work by external service personnel. All infrastructure installations are either directly or indirectly dependent on electric power (e.g., air conditioning, alarm systems and telephone private branch exchanges).

Failure of existing safety devices - Technical defects or external factors (e.g., ageing, improper use, deficient maintenance, manipulation, power failure) can cause safety devices to fail, with the result that their protective effect is greatly reduced or entirely lost. For example: Door locks can become damaged due to age or improper use, fire extinguishers that are incorrectly serviced do not work properly, and dirty fire alarms fail to detect fires or are triggered unnecessarily.

Data Center Staffing and Training

Establishing standards and procedures alone does not guarantee the smooth flow of IT operations. Each individual in the organization must be aware of the rules and procedures that apply to him. The damage that can result from inadequate knowledge of existing standards and procedures could result in delays in computer processing or damage to critical hardware and/or software. Resources with the right mix of skill sets and periodic training programs are required to keep data center staff operating at maximum levels.

Organization and Management – For the most part, policies have been established and the organizational structure applies standards to implement the policies and manage the operation of the computer facilities. The management structure provides the desired degree of control.

Organization allows lines of reporting and responsibility and allows control systems to be implemented. Within this area, the organization of the IT department ensures that adequate division of duties exists, that recruitment and staff relations procedures are conducive to control, and that training is adequate.

One of the more important aspects of organization and management is the concept of segregation of duties. This is a sound principle of internal control and is applied within the computing area. Responsibility for all aspects of processing data does not rest with a single individual or department. The functions of initiating, authorizing, inputting, processing and checking of data are separated. This ensures that no one person has complete control over a particular function; therefore, abuse of that function (fraud, etc.) may not be possible without collusion between two or more individuals.

The primary division of duties is between operational and systems development sections. Operations are responsible for the running of production systems and have minimal contact with the development team. Similarly, systems development has little contact with production systems. Within each of the main divisions, further division of duties is evident such as the area of Technical Support and Security Administration among others.

Data Center Operation Procedures

There are many areas of control involved with the computer operations area. Many of these are concerned with maintaining controls over the day to day activities that occur. Firms should maintain a set of policies and procedures that document these controls.

In a traditional Data Center the main tasks of operators are to mount tapes / cartridges, feed paper to printers and generally be present in case any unusual event occurs. The level of involvement may vary from one Data Center location to another. Some activities maybe performed remotely in a centralized command center, or from the company’s various office locations. Minimum operator intervention is required for the running of systems. This will minimize the risk of the operators performing tasks incorrectly with disastrous results on the normal data processing and the company's operation. This is achieved by automatic job scheduling whereby all the production work is submitted for processing by the operating software. Procedures are set up which call particular programs in particular orders. Jobs with specific dependencies are not run until previous programs complete. There are a few circumstances in which operators are actually allowed to change any of the program parameters and influence the way in which jobs are run.

Media Management - While the majority of an organization's data will be held on direct access devices such as fixed disks, it’s not always feasible to have every piece of data online at all times, mainly for performance reasons. Less frequently accessed data may be archived to other storage media such as tapes, cartridges, diskettes or optical disks. Backups are also a critical component in protecting a firm’s data. Data is fast becoming one of the most valuable assets of any organization and must be protected.

Back-up and recovery procedures are a key component of any IT data center operation and plans should be in place to ensure that the company can recover from any form of failure, whether it is the loss of one record or the entire computing facility. The procedures for backup and recovery need to be reviewed from the standpoint of day-to-day backup and contingency planning. Although also covered in a Business Continuity Planning (the data center audit) the importance of backup and recovery plans makes it worthwhile to also include them in an IT data center audit.

Scheduling - The operating system contains facilities that allow the system to build a queue of programs depending on predetermined sequences. Effectively, the operating system is presented with a list of programs to run and, at the required time, the system will load the program and run it. The scheduler can also be told what to do in the event that a program fails to complete satisfactorily (i.e., which jobs are dependent on successful running).

Many large mainframe operations use batch processing, despite the moves towards client/server type applications. Large volumes of data must be processed for settlement, producing confirmations / statements, or producing management reporting information. While most large batch processes will run overnight when online activity is minimized, computer resources are still finite and some form of batch job scheduling should be done to ensure the best use of computer resources. Management must look at the way jobs are scheduled to ensure that the most important jobs are given the highest priority.

Supervisor Privileges - In order to operate the operating system effectively, there is often the need to allow for a level of operation higher than that used for normal application programs. This level is often referred to as supervisor state (in the IBM world) or root privileges (in the UNIX world). This allows anyone who is allowed this privileged state to bypass most of the control and security mechanisms applied by the operating system over the application programs. While this is a necessary facility in order to keep the operating system running, it is a dangerous facility. Programs that acquire the privileged state can read and write data to areas of memory outside the ones in which they run. They can then interfere with the operation of other programs.

Program Change Control and Procedures

It’s never a good idea to install new or amended software or application programs directly into a production environment because they may not work as required and could have a detrimental effect on the organization's data and hence, business. In addition, they may conflict with other changes that are being made at the same time to related software or programs. There must be some form of process by which changes can be tested, approved and moved into production in a controlled manner.

This is where change management software comes in. Change management software associated with these processes can move both source and object code from development into production and maintain control over the contents of program libraries. The processes should not be too onerous, yet still provide assurance that only approved working changes are promoted. They’ll also want to verify that the change management software is sufficiently secure to ensure that the controls it provides cannot be bypassed.

Problem management is an earlier stage of this process. Problems will be logged and assigned a priority for fixing, resources will be allocated to do the work, and the resulting changes will be fed into the change management process.

Monitoring

Management oversight and monitoring of critical data center operations is essential. The lack of performance monitors and analysis for production hardware (computer/network devices) may result in inadequate support for production job processing. Lack of capacity planning and monitoring may result in inadequate space that is required by production systems. Computers and network performance should also be monitored and analyzed to ensure that they can support critical jobs and a regular analysis of performance metrics is required to identify bottlenecks and improve data center performance.

Outsourced and Vendor Activities

Outsourcing generally and offshore outsourcing in particular, continues to be a key part of many member firm's cost management strategy. The strategy has proven to be effective but brings with it significant risks that must be recognized and managed. In outsourcing, a firm is relying on someone else to run certain business functions. If not properly managed, outsourcing may negatively affect a firm's operations and clients. The product or service can be outsourced, but the risk cannot. Some of the potential negative outcomes may include;

- On-time delivery performance and end customer satisfaction levels may decline because of delays at third parties.
- Product or service quality may suffer.
- Schedules and budgets may not be achieved because of insufficient planning and/or resources.
- Suppliers may not be financially viable.

Increasingly, firms are also outsourcing technology applications to third-party vendors and application service providers. As a result, it is critical to clearly define the roles and responsibilities of those vendors and to manage the ongoing relationship between the bank and the vendor. More often than not, however, a firm's expectations of the relationship are not clearly defined. In fact, in many cases, management may not completely understand the obligations and commitments of a vendor. Therefore, firms can use service level agreements as a tool for managing the risks associated with technology outsourcing and to agree upon practices for managing, measuring, and monitoring vendor performance.

Global, Federal, State and Local Regulations

Failure to comply with Global, federal, state, and local regulations could cause a data center to be closed by regulators thereby impacting business operations. The design and operation of a large data center must comply with various state and federal workplace regulations such as OSHA. The implementation of the space itself, including raised floors, backup power, HVAC (Heating, Ventilation, and Air Conditioning), and network cabling are subject to common code requirements, including OSHA Regulations and potential requirements under the Americans with Disability Act (ADA) for access and moving about the data center such as how much space to leave between racks of equipment.

Additionally, Section 404 of the Sarbanes-Oxley Act of 2002 requires the CEO and CFO of publicly traded companies to certify the effectiveness of their organization's internal controls as they relate to the accuracy of financial information. The dependence on electronic information and IT systems is essential to support these critical business processes.

- SOX: Internal compliance and security technology Technical Paper
- Sarbanes-Oxley compliance and strong authentication Technical Paper
- SOX Compliance and Sidewinder SecurityReporter

Insurance

Inadequate or non-existent insurance coverage on computer equipment and the data center may subject a firm to financial loss through damaged or inoperable equipment. The time to replace damaged equipment is covered under the BCP however the money required should come from insurance policies that are updated regularly to reflect actual replacement value of all equipment and the construction costs associated with building a new data center.

Prior Audit Issues

An effective audit process includes a firm's commitment to addressing issues that arise out of prior IT data center audits and therefore all audits should include a review of these follow-up activities. An individual or small group should be designated with the authority and responsibility to follow up and report on progress towards implementing all prior audit recommendations through coordination with appropriate IT management. They should also fulfill the obligation to communicate the implementation status of prior audit recommendations to IT executive sponsors, IT management, and internal auditors. This individual or small group should also be accountable to ensure implementation efforts fully resolve audit issues or findings on a timely basis. Failure to follow-up and resolve prior audit issues may impair a firm's ability to resume IT operations in the event of a malfunction.

iad INTERNAL AUDITORS DIVISION

A Division of SIFMA

II. Audit Guidelines

II. AUDIT GUIDELINES

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
A. Executive Sponsorship for Accountability, Ownership, and Awareness		
Lack of awareness around factors that present the greatest degree of risk to the data center and lack of support for an audit process to mitigate those risks.	Determine examination scope and approach for the data center audit and to ensure management support for both daily operations and the audit.	• The scope, objectives, and approach will be discussed with management prior to commencing the review. • Interview management to review the management structure for running the data center. Review responsibilities of IT operations management is to ensure the firm'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. • Review executive support of and the firm's processes to support the audit process and ensure that: • An executive has responsibility for the audit process. • Sufficient resources and budget are allocated to audits. • Top-down support is present to ensure that compliance is treated as a corporate mandate versus a departmental challenge. • Support exists for the scope and objectives of individual audits by providing the audit team with a better understanding of the materiality and nature of the transactions being performed. • Support audit independence by ensuring that auditors have sufficient access to, and understanding of, key business information systems.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Interview management and review data center risks to identify: • Any significant changes in business strategy or activities that affect data center operations; • Any material changes in the audit program, scope, or schedules related to the IT data center audit; • Key management changes; • Information technology environments and changes to configuration or components; • Changes in key service providers (technology, communication, back-up/recovery, etc.) and software vendor listings; and • Any other internal or external factors that could affect the data center audit. • Determine management's consideration of newly identified threats and vulnerabilities to the organization's data center. Consider: • Technological and security vulnerabilities; • Internally identified threats; and • Externally identified threats (including known threats published by information sharing organizations). • All audit issues raised during the current examination will be discussed and approved with management and include responses prior to report issuance. • Review management's response to issues that rose 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.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
B. IT Business Plan		
Failure to align IT strategy with the business strategy, resulting in missed objectives, lost opportunities, and increased costs.	IT activity relating to operations and monitoring should be aligned to the strategies, goals and priorities of the firm.	• Verify that a formal IT Strategic Plan approved by IT senior management exists that clearly specifies the oversight and support provided by the board of directors and senior management. • Identify areas where the business strategy is critically dependent on IT and ensure that the IT business plan has adequately addressed those needs. • Review enterprise priorities and objectives to ensure that there is alignment between business and technology objectives and resources. • Obtain and review the IT Tactical Plan that is derived from the IT Strategic Plan and determine if it details the required IT data center related initiatives, resource requirements, and how the use of these resources and achievements will be actively monitored and managed to support the IT Strategic Plan. • Determine if a current technology infrastructure plan exists and is in accordance with IT Strategic and Tactical plans, and includes contingency arrangements and direction for acquisition of technology resources. Verify that senior IT management has approved the technology plan. • Determine if an Architecture Board or equivalent exists to: • Provide technology solutions, guidelines and advice on selection of new technologies. • Direct technology standards and best practices including compliance with external requirements. • Verify compliance with any regulatory requirements. • Verify the adequacy of the business / IT representation on

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		the architecture board. • Verify the frequency of their meetings and their escalation processes of issues by obtaining their minutes of meetings.
C. Environmental Survey		
Lack of a thorough understanding of the firm's IT operations environment may result in: • Inability to identify vulnerabilities; • Security breaches; • Equipment failure; and • Inability to continue operations during a disaster.	The environmental survey, along with the technology asset inventory, provides the foundation for the risk identification and assessment processes. The process should begin with a comprehensive survey of the institution's technology environment.	• Determine if the firm has created an environmental survey at an enterprise-level view that documents resources and physical locations of all data centers. The survey should also identify all resources (electric, heat, air conditioning, humidity control, etc) needed to support the physical locations. • Verify if physical maps exist for the data center layout, data center wiring, LAN/WAN topology maps, building wiring maps, telephone termination records. • Review floor space requirements with the respect to future growth or future decreases in the equipment (servers, media storage, etc) needed to support the firms data processing needs.
D. Asset Inventories		
Lack of a thorough understanding of a firm's IT assets and supporting documentation may results in: • Inability to identify vulnerabilities; • Redundancy; • Additional cost; • Missed upgrades; and • License violations.	Data center management maintains all technology assets (i.e., servers, databases, network devices) in use by the firm along with its key attributes (e.g., asset ids, location) in a central inventory database and keeps it up to date. A current configuration chart identifying all major	• Review the process to track and maintain datacenter IT asset inventory. • Determine that data center management has knowledge of what equipment, systems and programs are in its data center. • Obtain an inventory of computer equipment, programs and systems and test check a sample by verifying its existence in the data center. • Obtain a computer room floor plan with equipment, entrance and exits, storage, and fire protection equipment indicated on it and test check a sample.

Risks to be Managed	**Types of Controls to Manage/Eliminate Risks**	**Potential Audit Work Steps**
	equipment utilized and controlled by the data center should be maintained.	• Verify system and network configuration diagrams and lists exist and that they define the purposes of hardware and software products.
D.1 Hardware Inventory		
Lack of a thorough understanding of the institution’s IT hardware assets and supporting documentation may results in; • Inability to identify vulnerabilities, • Redundancy, • Additional cost, • Missed upgrades, • License violations.	Data center management maintains an inventory of all hardware assets including computing devices, printers, tape drives, and media as well as supporting software.	• Determine if the firm has created a hardware inventory. 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. • Determine if the firm has complete documentation of storage media. This should complement hardware, network topologies and software inventories without being redundant. Descriptive information should identify: • The type, capacity, and location of the media. • The location, type, and classification (public, private, confidential, or other) of data stored on the media. • Determine if a periodic inventory has been taken of all hardware and

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		reconciled to the local fixed asset system. Are reconcilement's performed annually? Review prior two years. • Verify the local fixed asset system contains all equipment purchased leased or otherwise acquired. • Verify that hardware is being properly capitalized and tracked. • Verify that contracts for purchased/leased hardware exist and have been properly authorized.
D.2 Telecommunications Inventory		
Lack of a thorough understanding of the institution's IT network assets and supporting documentation may results in; • Inability to identify vulnerabilities, • Redundancy, • Additional cost, • Missed upgrades, • License violations.	Data center management maintains an inventory of all its telecommunication assets including hardware, telecommunications software, network components and topology.	• Determine if the firm has created a telecommunications inventory. 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: i. POTS – plain old telephone service; ii. SONET – synchronous optical network; iii. ISDN – integrated services digital network; iv. Frame relay; and v. Wireless. • Determine if the firm has created a network components and topology inventory. The firm management should fully document the network configuration. Depending on the size and complexity

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		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; • Verify that redundancy exists in telephone lines and that they are sourced from different hubs even if different carriers are providing service and; • Identify what information is available and where it resides.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
D.3 Software Inventory		
Lack of a thorough understanding of the institution's IT software assets and supporting documentation may result in; • Inability to identify vulnerabilities, • Redundancy, • Additional cost, • Missed upgrades, • License violations.	Data center management maintains an inventory of all its software assets including in-house applications, databases, third-party supplied software, and vendor application services.	• Determine if the firm has created a software inventory. There are at least three major categories of software that should be included 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, system, or application name (e.g. general ledger); • 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).
D.4 Storage Media Assets and Data Content		
Lack of a thorough understanding of a firm's data assets, storage	A media management plan must be in place in order to track the location of the	• Verify that the survey tracks the capture, processing, flow, and storage of data throughout the firm.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
needs, and backups may result in lost, damaged, or stolen data thereby resulting in a firm's inability to conduct business.	data, and to ensure that data is stored securely and can be found and restored when needed.	• Verify that a process is in place in order to track the location of data at all times and that only authorized jobs may access data. • Review media management processes and controls to ensure that data cannot be lost. • Review media security processes to ensure that only authorized staff have access to data and that all media are stored in a secure environment. • Verify that scheduled backups are performed and that data copies are stored off-site. Ensure that retrieval of backup copies can be performed in a timely manner.
E. Risk Identification and Assessment		
Lack of an identification of major threats and vulnerabilities to IT operations that could result in loss of operational capabilities that may introduce subsequent financial and integrity risks.	Management can employ a variety of techniques to identify and assess risks, including performing self-assessments.	• Determine if an objective for a self-assessment has been formally defined and documented. • Determine if the self assessment identifies risk in at least the following major areas: • Internal and external risks; • Risks associated with individual platforms, systems, or processes; • Risk associated with people; • Risks associated with environmental conditions; • Those of a systemic nature; and • The quality and quantity of controls to mitigate risk. • Confirm that there is a process in place to ensure that the risk assessments are reviewed on a regular basis and approved by a registered principal. Confirm when the assessment was last

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		reviewed and when the next review is scheduled. • Review management's understanding of the environmental and asset surveys in the following areas: • All technology assets are accounted for; • Periodic updates are scheduled to the inventory are scheduled; • Plans exist for upgrading hardware, software, and licenses; • Risks and threats for each asset are identified and mitigated; and • Plans exist to continue operations in the event of a loss of each asset.
E.1 Review of Controls to Mitigate Risk		
Lack of a plan to manage, control, and mitigate risks to IT operations could result in loss of operational capabilities that introduce subsequent financial and integrity risks.	Management can employ a variety of techniques to manage risk, including the identification of responsible staff and the creation of on-going programs.	• Determine that programs and controls exist for the following: • Vendor management; • Change and problem management; • Job scheduling; • Capacity planning; • Hardware / software requisition and maintenance; • Physical and logical security; and • Environments (e.g., uninterruptible power supply, fire suppression, air conditioning, etc.) • Verify that clear roles and responsibilities exist for managing each of the above programs.
E.2 Risk Monitoring and Reporting		
Lack of proper reporting mechanisms to senior management could result	Both data center and firm management are responsible for the	• Review documentation that describes how management assesses the performance of datacenter operations and facilities functions and related controls; or discuss with management.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
in plan gaps and/or ongoing problems that may disrupt operational capabilities.	performance and operations of the data center including the programs for mitigating risk and threats, and for regularly reporting of this performance to senior management.	• Review operations management reports used to monitor previously identified issues. Determine how frequently such a review takes place and that the right personnel are receiving such reports. • Determine if the frequency of monitoring is adequate. • Determine if corrective actions are addressed in a routine manner throughout the year to address the previously identified issues/risks. • Determine that data center and firm management is aware of the performance of: ◦ Computer equipment ◦ Systems / Software ◦ Data center environment ◦ Employees ◦ Vendors • Obtain a copy of the above performance reports and review and test some items on them to the available incident reports. • Determine that data center and firm management are aware of the performance of the following programs: ◦ Vendor Management ◦ Change and Problem Management ◦ Job Scheduling ◦ Capacity Planning ◦ Hardware / software requisition and maintenance ◦ Physical and logical security ◦ Environments (e.g., uninterruptible power supply, fire suppression, air conditioning, etc.) • Obtain a copy of the above performance reports and review and test

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		some items on them to the regularly scheduled management reviews of each program. • Determine that performance issues and problems are being addressed by management in a timely fashion.
F. Review of Specific Data Center Controls to Mitigate Risk		
F.1 IT Data Center Business Continuity Plan		
Lack of an IT data center BCP plan may result in • Increased inability to support the dependent applications. • Deterioration of performance and increased user discontent. • Expensive recovery costs. • Lack of information and knowledge to reestablish operations.	Determine if the information technology environment has a properly documented business continuity plan that complements the enterprise-wide and other departmental BCP's.	• Determine if the IT component of the BCP has a properly documented contingency plan. Verify that the IT contingency plan properly supports and reasonably reflects the goals and priorities found in the corporate contingency plan. • Obtain access to the disaster recovery procedures. Review the documented IT continuity plans to ensure they include all critical business units and that they identify their system and service requirements in a disaster situation. • Ensure appropriate policies, standards, and processes address business continuity planning issues including: ◦ Systems Development Life Cycle, including project management; ◦ The change control process; ◦ Data synchronization, back up, recovery; and ◦ Employee training and communication planning; • Review the written IT continuity plan(s) and determine if the plan(s) addresses the back-up of the systems and programming function (if applicable), including: ◦ Back-up of programming tools and software; and ◦ Off-site copies of program and system documentation.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Determine if there are plans in place that address the return to normal operations and original business locations once the situation has been resolved and permanent facilities are again available.
F.1a Hardware Backup and Recovery		
Loss or corruption of physical processing equipment and/or data center needed to support business operations.	Determine whether the data center audit(s) include(s) appropriate hardware backup and recovery.	• Obtain the backup and recovery procedure for the firm's hardware and alternate data center plans. • Determine if all critical resources and technologies are covered by the alternate data center, including voice and data communication networks, customer delivery channels, etc. • Determine if the alternate center includes the entire network and communication connections. • Determine the arrangements for alternative processing capability in the event any specific hardware, the data center, or any portion of the network becomes disabled or inaccessible, and determine if those arrangements are in writing. • Determine if telecommunications equipment (modem, lines, controllers) are duplicated to ensure continuous operation should an equipment failure occur. • Ensure that dial backup capabilities exist in case of leased line failure. • Verify that alternate power supplies exist at both the main site and the alternate data center site: • Uninterruptible power supplies (UPS); and • Back-up generators.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
F.1b Data Backup and Recovery		
Loss or corruption of data needed to support business operations.	Determine whether the business continuity process includes appropriate data backup and recovery. Understand the process for backing up data from the production site to the contingency site.	• Obtain the backup and recovery procedure for the firm's data. • Determine whether data is backed up real-time (i.e., via replication), daily, weekly, monthly, incrementally, etc. • Verify Off-site storage of: ◦ Back-up media; ◦ Supplies; and ◦ Documentation, e.g., the data center audit(s), operating and other procedures, inventory listings, etc. • Determine that the off-site vault is an environmentally secured facility. • Determine if data backups are available from both on and offsite locations and can be restored to primary and alternate processing locations. • Determine if backup media (disks or tapes) are rotated off-site according to a predefined schedule. • Review arrangements to secure backup media (disks or tapes) at the off-site facility, including encryption, to prevent unauthorized access and potential loss of data. • Determine if the off-site storage facility is: ◦ Sufficiently remote from the processing facility; and ◦ Accessible within a reasonable time frame, if backups are needed. • If media is stored offsite in a non-Corporate building, has an

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		agreement been signed to use the facility? • Access to data files should be logged in and out to prevent release to unauthorized individuals. A log of the contents, time of the backup and location of the off-site backups must be maintained and stored both locally and at the offsite location. • Determine whether a tape management system is in place and ascertain that reels of tapes and cartridges sent off site are logged and externally marked with proper identification. • Verify that the tape library (used for on-site storage) is a sufficient distance from the computer room and adequately protected to ensure that if a disaster befell the computer room, the tape library would be able to service, and vice versa.
F.1c Software Backup and Recovery		
Loss or corruption of mission critical software needed to support business operations.	Determine whether the business continuity process includes appropriate software backup and recovery.	• Obtain the backup and recovery procedure for the firm's software. • Review the written procedures and determine if the plan addresses the back-up of the systems and programming function (if applicable), including: • Back-up of programming tools and software; and • Off-site copies of program and system documentation. • Verify that regular back-ups of the following software occurs: • Operating systems; • Applications; • Utility programs; and • Telecommunication software. • Determine if software programs are available from both on and

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		offsite locations and can be run at both the primary and alternate data centers. • Determine if the plan establishes processing priorities to be followed in the event not all applications can be processed. • If the organization is relying on in-house systems at separate physical locations for recovery, verify if the equipment is capable of independently processing all critical applications.
F.1d Alternate Data Center		
Alternate data center is unable to support running of mission critical applications due to lack of backed up data, required applications, or type and size of equipment needed.	Data center management should maintain arrangements to provide an alternate data center; and periodically check that operations can be moved from the primary site to the alternate site in a timely manner, and that recovery processes will work as intended.	• Describe arrangements for alternate processing capability in the event the data center or any portion of the work environment becomes disabled. • Determine that there is a designated back-up computer hardware system, and that it is a practical site for back-up operations until current equipment can be repaired or a new computer can be installed. • Determine if the outside facilities used for recovery: • Have the ability to process the required volume. • Provides sufficient processing time for the anticipated workload based on emergency priorities. • Determine if the alternate data center allows the organization to use the facility until it achieves a full recovery from the disaster and resumes activity at the organization’s own facilities. • Determine how customers would be accommodated if simultaneous disaster conditions were to occur to several customers of the backup facility provider.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Determine whether the firm is kept informed of any changes at the recovery site (e.g., hardware or software upgrades or modifications) that might require adjustments to the firm's software or to the recovery plan. • Determine if the plan provides physical security at the recovery site. Determine whether there is a guard present and a sign in/out log for all visitors. • Determine the extent of vendor arrangements in the event of an emergency. • Review the contract between applicable parties, such as recovery vendors. • Determine how the recovery facility’s customers would be accommodated if simultaneous disaster conditions were to occur to several customers during the same period of time. • Determine whether the organization ensures that when any changes (e.g., hardware or software upgrades or modifications) in the production environment occur there is a process is in place to make or verify a similar change in each alternate recovery location. • Determine whether the organization is kept informed of any changes at the recovery site that might require adjustments to the organization’s software or its recovery plan(s). • Determine if the alternate data center addresses communications and connectivity with technical service providers in the event of a disruption at the primary site.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Determine if: • Duplicates of the operating systems are available both on- and off-site; • Duplicates of the production programs are available both on- and off-site, including both source (if applicable) and object versions; • All programming and system software changes are included in the back up; • Back-up media is stored off-site in a place from which it can be retrieved quickly at any time; • Frequency and number of back-up generations is adequate in view of the volume of transactions being processed and the frequency of system updates; • Duplicates of transaction files are maintained on- and off-site; and • Data file back-ups are taken off-site in a timely manner and not brought back until a more current back-up is off-site. • Determine if there are documented procedures in place with technology service providers (TSPs), correspondents, affiliates and other service providers, for accessing, downloading, and uploading information from primary and recovery locations, in the event of a disruption. • Determine if the firm has a copy of the TSPs BCP and incorporates it, as appropriate, into their plans. • When testing with the critical service providers, determine whether management considered testing: • From the institution’s primary location to the TSPs’ alternative location;

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• From the institution's alternative location to the TSPs' primary location; and • From the institution's alternative location to the TSPs' alternative location. • Determine if institution management has assessed the adequacy of the TSP's business continuity program through their vendor management program (e.g., contract requirements, SAS 70 reviews).
F.2 Data Center Security		
Lack of appropriate physical security at either primary or alternate site causes disruptions in or loss of ability to conduct business operations.	Physical access to all data centers should be documented and restricted to authorized individuals.	• Determine that there are adequate controls implemented to protect the data center from loss due to unauthorized access. • Ascertain that the computer room, tape library and the DASD area are restricted from access by individuals who have no need to enter these areas. • Determine whether adequate physical security and access controls exist over data back-ups and program libraries throughout their life cycle, including when they are created, transmitted/delivered to storage, stored, retrieved and loaded, and destroyed. • Determine if appropriate physical and logical access controls have been considered and planned for the inactive production system when processing is temporarily transferred to an alternate facility. • Determine if the intrusion detection and incident response plan considers resource availability, and facility and systems changes that may exist when alternate facilities are placed in use. • Note and evaluate the existence of the following physical security concerns for the primary and alternate datacenters as well as any

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		supporting rooms storing support systems such as UPS and Power generators etc; • Verify if physical barriers are used to prevent unauthorized access. Have additional devices (turnstiles, man traps) been installed to prevent "piggybacking" into the facility? . • Verify physical security barriers and perimeters are free of physical gaps and weaknesses. • Review physical access controls in place for server cabinets. Check that server cabinets are locked and that access to keys is controlled and allocated following a formal access control procedure. • Do emergency exits prevent entry from outside and, upon opening, sound off with an alarm? • Note and evaluate the existence of the following control procedures for the primary and alternate datacenters as well as any supporting rooms storing support systems such as UPS and Power generators etc; • Are badges displayed to a Security Guard and logged upon entering the computer room? • Are card keys and card key readers utilized to log, control and restrict access? • Are the card key listing and log reviewed periodically by management and access changed on a regular basis? • Are access cards or codes removed upon employee termination? • Review access to backup tape rooms. • Depending on the type of computer room access security system used, what would happen to this system in the event of a power failure?

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Note and evaluate the existence of the following CCTV plans for the primary and alternate datacenters as well as any supporting rooms storing support systems such as UPS and Power generators etc; ◦ Are closed circuit TV monitors used to monitor data center entrances? ◦ Review placement of security cameras. Verify if cameras are strategically positioned inside and outside the data center to track entrance, exit, and all activity within a datacenter. ◦ Review the central video management system. ◦ Review retention process, and period for CCTV recordings. • Determine if the methods by which personnel are granted temporary access (physical and logical) during continuity planning implementation periods are reasonable. • Evaluate the extent to which back-up personnel have been reassigned different responsibilities and tasks when business continuity planning scenarios are in effect and if these changes require a revision to the levels of systems, operational, data, and facilities access. • Review the assignment of authentication and authorization credentials to determine if they are based upon primary job responsibilities and if they also include business continuity planning responsibilities. • Obtain a list of individuals who may enter the computer room and evaluate some individual's need for having such ability. Review if entitlements granted are commensurate with job functions. • Is a sign-in log maintained to record data center access by

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		individuals (guests) not on the authorized listing (e.g., vendors or maintenance personnel)? • Is there a 7 by 24 Security Guard and are there approved Security Guard Procedures? • Determine if there is a silent police alarm. • Are all server and equipment cabinets locked and who has copies of keys or access codes? • Can the location of the data center be determined by unauthorized individuals (e.g. is it listed on the building directory)?
F.2a System Access by Users		
Individuals with technology knowledge within the firm access sensitive information or make unauthorized changes to the data center environment causing disruptions to the business.	The audit identifies whether procedures followed and the security system used adequately protects application programs and data files from unauthorized access. User access to all system resources should be properly defined and controlled.	• Verify that data center management establishes, communicates, and enforces policies and procedures surrounding data center system access. • Determine if a security software package is in place to ensure access to system data and software is adequately controlled and monitored. • Determine whether an external security system, if used, adequately protects application programs and data files from unauthorized access. • Verify that each system user is positively accountable for his/her actions by means of a unique user identification code. • Verify that each user must provide some mechanism of validating his/her identification (e.g. passwords). Do password controls adhere to the firm's Information Security Policy as follows: • A minimum of "n" characters. • Must be stored in encrypted form.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		◦ Must expire after "n" number of days. ◦ Should not be a commonly associated name. ◦ Access must be temporarily revoked after a number of unsuccessful logon attempts. ◦ Attempted violations of identification or authentication must be logged and reported to management. • Verify that there are adequate procedures for the review of patterns and trends of unsuccessful logon attempts. • Verify that the authorization of each consultant and/or temporary employee to access information must be for a limited time. • Ensure that access privileges granted to individuals who are terminated or whose responsibilities change must be promptly revoked. • Verify that information access is temporarily suspended after a certain period of inactivity. • Verify that the operating and/or security system: ◦ Defines authority and enforces access control to data within the system (e.g. files and programs). ◦ Is capable of specifying for each source (e.g. data file) a list of named individuals or a list of groups of named individuals with their respective mode of access. ◦ Users must be limited to a profile of transactions required to perform their needed tasks.
F.2b System Resource Administrators		
Unauthorized access to system data and software that results in loss, corruption, or damage.	The computer systems group must support an independent security administration function for	• Verify that the system support separate operator and security administrator functions. • Identify what functions the security administrators are authorized to

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
	controlling user access to system resources.	perform. • Verify that the security administrator is limited to those functions essential to performing the security administration role. • Verify that security administrators cannot or are not required to perform business transactions. • Determine if audit logs are maintained for all actions performed by security administrators.
F.3 Environmental Hazards		
Loss and damage of data center equipment, production systems and networks software, or media due to environmental hazards such as flooding, loss of air conditioning, power outages, intruders, humidity or fire.	Adequate physical safeguards and maintenance controls must be in place to protect computer equipment from loss and damage due to environmental hazards. Data center management must also test and review the results of the safeguard systems against pre-defined system capacity criteria.	• Determine if activation of fire, water, humidity, or temperature alarms will cause certain areas to be notified (e.g., building facilities management, local fire department, police, etc.). • Determine if documented procedures for employees to follow in the event of a computer room emergency exist. Through interviews, determine whether employees, especially supervisors, are familiar with these procedures. Verify that there two entries to the data center location and into the facility and that there are plans with local authorities to gain access during an evacuation of the local geographic area. • Determine if the data center facility can withstand earthquakes. Verify that the facility is built on stabilizers, all the equipment is racked and stacked securely, and that all overhead material is secured to prevent falling debris? • Determine if the data center facility's exterior walls and roof are built to withstand high winds from storms and that any windows or doors facing the exterior can withstand high winds as well.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Determine if emergency telephone numbers are posted for easy access. These numbers include outside police and fire departments, emergency response groups, and organization guards. In the event of a crisis, emergency personnel, i.e., firefighters and law enforcement officers can gain access to the facility without delay. • Determine if general computer housekeeping rules exist by noting and evaluating the following: • No smoking, eating or drinking is allowed inside the computer room. Display of these signs is also evident. • Excessive or flammable supplies are not stored in the computer room. • Raised floor is free of debris. • Floor tiles are properly maintained, they are not broken or missing and floor pullers are available. • Determine if there are procedures for daily or weekly cleaning of the information processing facility. • Determine if there are procedures or contracts for regular cleaning under the raised computer room floor. • Determine if there are procedures or contracts for regular computer equipment cleaning. • The hardware components are covered with dust covers when not in use.
F.3a Lightning		
Data center and power supply damage due to lightning during a thunderstorm entering the facility that houses the data center.	A risk assessment should be performed for determining lightning loss and damage for all types of structures, power, telephone, and internet connections required to	• Determine if the building housing the data center has a Lightning Protection System that complies with current nationally recognized codes. Lightning protection systems consist of air terminals (lightning rods) and associated fittings connected by heavy cables to grounding equipment, providing a path for lightning current to travel safely to ground.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
	support data center operations.	• Determine if UL Listed surge arresters are installed at for service and telephone equipment to prevent surges from entering building over power or telephone lines. Surges should diverted to the ground, and both wiring and appliances should be protected. • Determine if transient voltage surge suppressors are installed in primary and backup power supplies as well as receptacles to which computers and other electronic equipment are connected in order to limit the voltage to 11/2 times the normal (maximum for solid state devices).
F.3b Fire		
Production systems and networks are damaged by fire.	Building Operations inspects fire suppression system in office buildings and data centers for degradation and upgrade.	• Review the type of smoke detection, and fire suppression systems deployed at each of the datacenters reviewed, including co-location facilities. • Review the fire suppression unit. If a gas system is used: • Check for emergency hold-off buttons such as FM-200 abort button; and • Warning signage is located throughout the facility. • Determine if fire extinguishers are placed in strategic locations, marked in red for easy accessibility and periodically inspected. • Determine if automatic fire-fighting equipment such as dry-pipe water sprinklers, halon system, etc. exist and are regularly tested. • Determine if smoke detection devices are located above the ceiling and below the raised floor. • Review the maintenance process and reports for fire suppression systems, including fire extinguishers. • Is there evidence that fire drills are conducted regularly and that

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		staff have individual responsibilities in case of fire or other emergencies?
F.3c Flooding and Water Damage		
Production systems and networks are damaged by flooding.	Adequate physical safeguards and maintenance controls must be in place to detect flooding and unusual water levels in the data center to protect computer and network equipment from damage.	• The data center should have a raised floor to protect against the risk of flooding/ water leakage installed with water detectors to alert staff in the event of flooding. • Determine if water detectors exist under raised floors and if water covers are present for all equipment. Are there water detectors located under the AC? • Determine if water detection systems are in place or will provide alerts for flooding from water lines located above or on floors above the data center.
F.3d Climate & Humidity		
Production systems and networks are damaged due to high temperatures or humidity.	Adequate maintenance controls and alarms must be in place to monitor and report temperature and humidity levels throughout the data center.	• Review adequacy of temperature and humidity control systems. • Check if CRAC and Chiller units are in a redundant configuration. • Check if current cooling capacity exceeds current cooling loads. • Review datacenter cooling/ air management design. • Check for hot/cold aisle rack layout .i.e. check if data center equipment is laid out in rows of racks with alternating cold (rack air intake side) and hot (rack air heat exhaust side) aisles between them. • Check for raised flooring with perforated tiles. • Observe for any obstructions to HVAC ducts supplying cold air to the aisle. • Review maintenance contracts and reports for CRAC and chiller

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		units. • Review the system in place for monitoring the health of environmental control systems i.e. chillers and CRAC systems. Review sample reports. • Verify that temperature and humidity measuring devices exist and are working to keep equipment within manufactures specs. • Are there Emergency Shutoff controls for, electricity heating, ventilation, and air-conditioning?
F.3e Power Outages		
Production systems and networks are damaged by loss of power or electrical surges.	Adequate physical safeguards and maintenance controls must be in place to monitor power supplies, suppress surges, and raise alarms for potentially damaging conditions.	• Verify that there is a battery powered emergency lighting throughout the data center. • Determine if there is an UPS system and that it is maintained and tested and if the backup power supply system can be relied upon to: • Keep the processors running for a short period of time, until the system can be brought down easily, without causing damage to the computer equipment or data (UPS backup)? • Keep the processors running indefinitely during an extended power outage (Generators)? • Review the process for maintenance and monitoring of the emergency/backup power supply systems. • Verify change management processes are followed during the planning and execution of data center power downs. Obtain evidence of planning, execution and issue tracking related to power downs. • Determine if both the primary power supply and the backup power supply have surge and lightning protection.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Determine if is there a remote Building Management System (BMS) to control the power and cooling during facility evacuations. • Verify that redundancy exists in power lines and that they are sourced from different sub-stations even if different utilities are providing service.
F.4 Equipment Maintenance		
Equipment outages due to improperly maintained equipment that results in loss of data center operations and subsequent financial risk to the firm.	Preventive maintenance should be performed for all hardware, equipment, environmental controls, and alarm and detection systems.	• Determine if service contracts exist for all hardware, computer, and network equipment identified in the asset inventory. • Determine if service contracts exist for all environmental controls and alarm and detection systems. • Ensure that records are maintained for equipment servicing due to hardware malfunctions and for preventive maintenance. • Review a sample of preventive maintenance contracts for coverage and cost. • Verify that downtime logs are maintained and contain adequate/necessary information of problem. • Verify that downtime logs are reviewed and necessary action is taken to ensure non-recurrence of problem. • Determine if an inventory system is used to record hardware purchase, distribution, and disposal. Assess its adequacy by comparing to the physical inventory. • Confirm that procedures for hardware moves, additions and changes are adequate. Requisitions follow a centralized procedure and data center management approves and oversees all relevant changes.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Determine if procedures exist to destroy data from computer hard-disk prior to disposal. • Determine if all software (whether purchased or developed in-house) is accounted for through an inventory system and assess its adequacy.
F.4a Network Equipments Installation and Cabling		
Cabling installed does not meet standards required for data transmission (e.g., the standard named "ANSI/TIA/EIA-568-A 1995" which specifies categories that can support certain bandwidth requirements). Cabling used for data transmission or power distribution is not securely mounted and protected from damage caused by personnel working in the data center. Cable lengths exceed maximum recommended by standards.	Information Technology relies upon standards that specify cabling required for network connections. Cabling is selected to connect specific devices based upon requirements specified for such devices. Individuals who perform work that physically connects computer hardware use correct cable as determined by standards and requirements. data center personnel responsible for installation of cabling used for data transmission or power distribution have utilize methods for ensuring that cabling used for data	• Interview data center personnel responsible for management of cabling and review relevant documentation to determine whether standards are utilized to specify cabling requirements for network connections. • If standards are used, obtain understanding of process for selecting cable that meets requirements for network connections. • Select a sample of physical cables used to connect computer hardware to network and determine whether these meet standards. • Verify that cabling is neatly and clearly routed, via secure fire-proof conduits where necessary. Cabling allows sufficient free space under-floor for circulation of air. • Interview data center personnel responsible for installation of cabling used for data transmission or power distribution and determine methods used for ensuring that cabling used for data transmission or power distribution is not securely mounted and protected from damage caused by personnel working in the data center. • Observe cabling in data center and evaluate whether it is securely mounted and protected from damage caused be personnel working in data center.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
	transmission or power distribution is not securely mounted and protected from damage caused by personnel working in the data center.	• Ensure that cables are laid out in a manner that does not make them susceptible to physical strains (cables enclosed, fire and water resistant, resistant to extreme temperatures and sturdy). • Determine if cable condition checks are conducted once every two to five years according to the firm's policy. • Verify that there are Inventory controls in place to prevent loss of and damage to cabling equipment. Such as: • Are there extra cables stored on-site (CAT5, etc.)? • Who has access to extras? How is access controlled? • How many are there? • What condition are they in? • Determine if cables are properly labeled and if a cable map exists. • Determine if the cable map is public knowledge or only accessible to a limited number of people who need the information. Repair personnel should have knowledge of cable mapping. • Determine if cabling is heavily protected between floors traveling from floor to floor through the center of the building. (The outer parts of the building are more susceptible to weather damage.)
F.5 Data Center Staffing and Training		
Data center management systems may be ineffective and inefficient due to misalignment with their mission and not capable of meeting the business objectives.	Current job descriptions/ responsibilities of all members of the data center team are defined in a manner that prevents violation of segregation of duties requirements.	• Obtain an organization chart of the data center and review the chart for adequacy of reporting lines and staffing requirements. • Determine whether the policies are outlining the supervision and assignment of responsibilities to groups and related individuals should be documented, communicated, and enforced. • Discuss individual responsibilities within the organization chart and

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
Organizational structure may be inappropriate for achieving business objectives. Lack of accountability could also lead to improper segregation of duties. Improperly or untrained data operations staff may cause operational errors that result in financial risk to the firm.	Data center staffs have a minimum level of experience and there are ongoing training plans in place to ensure that all staff has the requisite skill set. Data center management must maintain a high standard for personnel, constantly challenge them, adequately reward them and train them and always motivate them.	validate that there are no segregation of duties conflicts. • Identify those positions responsible for maintaining the programs, backing-up the system / data files, and using the various computer center systems. If necessary, review the written job descriptions for each functional duty described in the organization chart. • Determine whether provisions are made for backup personnel in key positions? • Obtain a listing of terminated personnel over the past year and verify whether personnel turnover over the past year has been significant and determine reasons why. • Determine if data center staffs are adequate in number and are technically competent to accomplish its mission; specifically: • Discuss with data center management the current skill sets and background of all personnel within data center. • Review the experience levels of Computer Operations personnel and determine if data center personnel have sufficient skill sets to execute their roles, responsibilities and key operations procedures. • Obtain training/development plan for the data center. Review the training provided Computer Operations personnel. • Identify strategy and procedures for cross-training and second-level support, if applicable. • Determine if training is provided to data center personnel regarding; • The firm’s compliance guidelines and regulations. • Security and confidentiality of information and copyright laws, guidelines and regulations. • Verify that all data center personnel have attended

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		mandatory compliance and professional conduct training; and that exceptions have been appropriately addressed. Specifically, obtain and review the record of attendees from the Compliance department. • Determine that job descriptions have been developed for all Computer Operations personnel and that they are regularly reviewed and revised. • Verify the existence of simulations and desktop exercises to test various threat scenarios. Scenarios should include: • Equipment failure • Environmental damage • Unauthorized access and sabotage • Loss of key personnel
F.6 Data Center Operations Procedures		
Failure to establish and ensure adherence to documented procedures may interrupt the continuous processing of data and the confidentiality of business information.	Data center management must document and maintain computer operating procedures and ensure that they are followed.	• Determine if management has documented, approved and signed off on policies, procedures and controls covering the following: • Preventative Maintenance of Hardware • Monitoring of IT Infrastructure and Related Events • Physical Safeguards of the facility and its assets • Handling of sensitive documents and output devices • Determine if management has approved and documented policies and procedures for support of capital expenditure. • Determine if management has updated the above policies and procedures to reflect changes in the technology environment over the past year. • Identify the number of operating shifts and the hours of operation of each shift. Are there appropriate staff and supervisory personnel

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		assigned for each shift? • Obtain and review key Support Documentation such as Operation Procedures, Data Center Operation Program change management, Job Scheduling (e.g. Control-M) Procedures, etc. • Determine if a problem management process is in place to handle and resolve all hardware, network, system, and application related processing problems. • Determine if support personnel for all major components of the data center (hardware, network, OS, and application software) have been identified and contact information is present for each. • Determine if an escalation procedure is documented and followed for hardware or software malfunction. • Verify if trouble incident reports are completed for every hardware or software malfunction? • Determine that a process is in place for the orderly and timely scheduling and execution of production jobs. • Verify that actual processing agrees with pre-established schedules and user requirements. • Are there procedures to ensure that all jobs scheduled have been run (e.g. automated Job Scheduling and Check Files). • Does the schedule include: on-line functions, jobs run daily, weekly and monthly and special request jobs? • Are all jobs authorized by data processing management and appropriate user groups? • Verify that a set of startup instructions/procedures exist for data center personnel to enable on-line user access to

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		applications. • Verify that run books contain all the information necessary to perform processing. • Are all jobs documented to the extent that operators can perform recovery procedures when necessary? • Are procedures established that ensure successful completion of all jobs? • Verify that processing can be successfully reconstructed when operational problems have occurred. • Verify, on a sample basis, that all output is complete and distributed in a timely/accurate manner to appropriate areas and/or individuals. • Determine if a shift turnover report is prepared which contains information on problems, system status, and any other types of information needed for efficient shift transactions? • Is the turnover report signed by both the outgoing and incoming shifts? • Are turnover reports reviewed by management and analyzed for trends? Are they maintained for at least 30 days? • Review the operator's procedures manual used by computer operators. Determine whether, according to those procedures and in practice, operator duties are properly segregated? • Identify what prevents the mounting and use of the wrong tape. • Identify what prevents the inadvertent use of an active tape as a scratch tape.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Review the console/control log. Determine whether it is reviewed by supervisory personnel and retained for a reasonable time? • Verify sufficient written procedures exist for the operation of all major equipment in the data center. List all major equipment and indicate what procedures are documented. • Evaluate telecommunications monitoring capabilities (response times, number of malfunctions). • Identify the data flow in the telecommunications network. Determine input/output line sources, protocols and configuration.
F.7 Program Change Controls and Procedures		
Data center disruptions caused by unauthorized or defective software changes.	To ensure that the implementation of new production application and operating system programs and modifications to existing programs are properly performed and are authorized by management. There should be a formal change management process in place and adequate documented procedures for controlling the migration of software into the production environment.	• Verify the existence of application and operating system software change control procedures. • Review a Flow diagram showing the program change management process. Highlight the existence or lack of control points. • Ascertain the existence of a formal list of application programming and management personnel who may authorize modifications to production programs. • Identify the individuals that have update access to production libraries (only appropriate data center production turnover personnel should have update capabilities). • Determine that manual and/or automated procedures are used to ensure that all corresponding production source and executable programs are always in agreement. • Determine if there is a process in place for handling software

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		changes to the production environment in emergency situations. • Determine if there is a process in place for maintaining the integrity of installed code within the production environment and that unauthorized access is logged and monitored. • Verify that systems purchased from outside vendors follow the same change control procedures applied to internal software modifications. • On a sample basis, determine that these procedures are satisfactorily documented and are being adhered to. • Determine that both Production and Quality Assurance libraries where user acceptance testing is performed are secured from unauthorized modification. • Determine that the following requirements are satisfied before application and operating system changes are put into production libraries. • Application programming or system support IT department approval is obtained. • Unit, integration, quality assurance (QA), and user acceptance tests (UAT) are performed. • User department signs off on test results. • Preparation of appropriate computer operating system instructions and restart/recovery procedures.
F.8 Monitoring		
Ineffective management of data center Operations activity leads to business disruption due to poor	A monitor system and capacity planning process should be in place to monitor batch job and all	• Confirm ongoing performance monitoring of batch jobs and equipments is occurring, reported upon and issues are addressed by management. Obtain a copy of the most recent reports. They should include:

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
problem management, failed batch jobs, system outages etc.	equipments, including PC, Networks devices, and other devices that are housed in the data to ensure that they can support critical jobs and to provide adequate capacity for production systems.	◦ Response times ◦ Frequency and maximum duration of outages ◦ Proportion, types, and causes of job failures ◦ Computer system peak and average utilization and trends • Examine utilization reports and determine the times of peak resource demand within the processing day. Determine how Computer Center management reacts to equipment utilization information. • Determine whether system downtime is recorded or tracked, include: ◦ Metrics defined and tools in place for application availability and load monitoring, and collection of application vital statistics. ◦ Regular reporting of application availability and performance. ◦ Active (automated) notification of application failures. Interface to problem management system. • Confirm that workload forecasting includes input from users on changing demands and takes into account new technology or current product enhancements. • Inquire of and determine the quality of processes or programs that monitor capacity for the production systems. • Confirm existing systems provide adequate capacity for anticipated network growth. • Determine whether capacity planning (processor, memory, channels, disk, etc.) performed, is consistent with, and integrated into strategic long-range plans.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Review the capacity threshold and determine whether such thresholds are adequate to give enough time to fix the capacity problem.
F.9 Outsourced and Vendor Activities		
The businesses use unreliable 3rd party production systems and mission critical outsourced activities fail to run during a disaster or suffer a disaster in their own right. Vendor SLA insolvency leads to inability to support the production application. Vendor contracts are not legally binding.	Determine whether data center management addresses the risks associated with critical outsourced activities and monitor the performance of 3rd party vendors.	• Verify that a procedure is in place to ensure that vendor services meet business requirements, an appropriate request for proposal (RFP) and bidding process is in place, that contract are formalized and retained, and that a legal should review is performed prior to the contract signing. • Determine that there are Service Level Agreements with performance and reporting standard. • Review a sample of the 3rd party data center contracts. Check that the contract includes, at a minimum, performance requirement, penalty clauses, right to audit clauses, confidentiality requirement etc. • Review if the co-location vendors performances fall short of the expected SLA and that technology management escalate the matter as documented in the contract. • For each relationship with a third-party hardware/software provider, confirm a formal contract is in place. Contracts with third parties should include: • Formal management and legal approval • Definition of services/spares to be provided • Cost of services / “out of contract” items • Quantifiable minimum service level • Content and frequency of performance reporting • Penalties for non-performance

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		- Problem resolution process - Agreement modification/dissolution process - Duration of contract and renewal/review procedures - Security requirements and non-disclosure guarantees • Determine if a designated body within the data center or a Vendor Management Office is in place to exercise on-going oversight of the service providers and / or vendors. If so, determine what reports and tools are used to execute this oversight.
F.10 Global, Federal, State and Local Regulations		
The data center violates State, Federal, or environmental regulations.	Data center management monitors and maintains compliance with state and federal environmental regulations and permits.	• Review the compliance of data center operations with state and federal workplace regulations such as OSHA. • Review the effectiveness of the firm's internal controls as they relate to the accuracy of financial information with respect to the Sarbanes-Oxley act of 2002.
F.11 Insurance		
Financial loss due to equipment damage.	The data center has adequate insurance coverage.	• Verify that the data center has insurance coverage protecting itself from financial loss due to equipment damage caused by a fire, water leakage, etc. (e.g. EDP equipment coverage). • Determine if an insurance questionnaire exists and is updated annually and submitted to the Corporate Insurance Department that includes all assets listed in the hardware inventory including replacement value. • Review the adequacy of insurance coverage (where applicable) for IT equipment and facilities in the data center. If the insurance policy requires that specific equipment be listed for coverage, determine that the current listing is accurate.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
G. Prior Audit Issues		
Prior and/or ongoing issues that impair a firm from resuming business operations in the event of a disaster.	Review of prior issues, resolution, and meeting of previously established target dates.	• Obtain prior the data center audit issues that related to this review and perform issue follow-up to ensure that actions are adequately resolved. • Review past reports for outstanding issues or previous problems. Consider: • Regulatory reports of examination; • Internal and external audit reports, including SAS 70 reports; • Business continuity test results; and • Organization's overall risk assessment and profile. • Review management's response to issues raised since the last examination. Consider: • Adequacy and timing of corrective action; • Resolution of root causes rather than just specific issues; and • Existence of any outstanding issues.
H. Conclusions and Action Plan		
Failure to address the data center audit gaps that impair a firm from maintaining data center operations and resuming them in the event of a disaster.	Discuss corrective action and communicate findings.	• Identify gaps in the data center audit. • Determine actions needed to close gaps. • Assign responsibility to action items. • Determine target date for each action. • Ensure review of action items becomes part of next audit.

iad INTERNAL AUDITORS DIVISION
A Division of SIFMA

III. Glossaries

III. GLOSSARIES

The definitions in this section shall apply to the terms used in the guideline. Where terms are not defined in this section or within another chapter, they shall be defined using their ordinarily accepted meanings within the context in which they are used.

Asset Inventory- A review of all the physical assets that comprise a functional data center. These include but are not limited to the primary and back-up computers, servers, media devices, network devices, routers, printers, monitors, and telecommunications infrastructure.

Approved- Acceptable to the authority having jurisdiction.

Authority Having Jurisdiction (AHJ)- An organization, office, or individual responsible for enforcing the requirements of a code or standard, or for approving equipment, materials, an installation, or a procedure.

Business Continuity- An ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies, recovery plans, and continuity of services.

Data- Information processed or stored by a computer. This information may be in the form of text documents, images, audio clips, software programs, or other types of data. Computer data may be processed by the computer's CPU and is stored in files and folders on the computer's hard disk or other external media storage devices.

Data Center- A facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (air conditioning, fire suppression, etc.), and special security devices.

Damage Assessment- An appraisal or determination of the effects of the disaster on human, physical, economic, and natural resources.

Disaster/Emergency Management- An ongoing process to prevent, mitigate, prepare for, respond to, and recover from an incident that threatens life, property, operations, or the environment.

Emergency Management Program- A program that implements the mission, vision, and strategic goals and objectives as well as the management framework of the program and organization.

Environmental Survey- A review of all the physical structures needed to house, support, and run a data center. These include but are not limited to a computer room, media storage, air-conditioning, heating, humidity control, water and flood monitoring, security and alarms, and fully redundant subsystems.

Exercise- Tabletop exercises, walkthrough evaluations, and other simulations that recreate various disaster scenarios and the actions needed to resume data center operations.

Hardware- The equipment and devices capable of accepting and storing computer data, executing a systematic sequence of operations on computer data, or producing control outputs. Such devices can perform substantial interpretation, computation, communication, control, or functions including managing network traffic, telecommunications interfaces, and providing services to remote computers. A complete list of a data center's hardware can be found in the asset inventory.

Impact Analysis [Business Impact Analysis (BIA)]- Analysis that identifies the impacts of losing the firm's resources.

Incident Action Plan- A verbal plan, written plan, or combination of both, that is updated throughout the incident and reflects the overall incident strategy, tactics, risk management, and member safety that are developed by the incident commander.

Incident Management System (IMS)- The combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in the management of resources during incidents.

Mitigation- Activities taken to reduce the severity or consequences of an emergency.

Mutual Aid/Assistance Agreement- A prearranged agreement between two or more firms to share resources in response to an incident.

Preparedness- Activities, tasks, programs, and systems developed and implemented prior to an emergency that are used to support the prevention of, mitigation of, response to, and recovery from emergencies.

Prevention- Activities to avoid an incident or to stop an emergency from occurring.

Recovery- Activities and programs designed to return conditions to a level that is acceptable to the firm and the conduct of its business.

Resource Management- A system for identifying available resources to enable timely and unimpeded access to resources needed to prevent, mitigate, prepare for, respond to, or recover from an incident.

Response- Immediate and ongoing activities, tasks, programs, and systems to manage the effects of an incident that threatens life, property, operations, or the environment.

Risk Assessment- Business processes and the business impact analysis assumptions are stress tested with various threat scenarios. The result is an assessment of the impact each may have on the organization's ability to continue to deliver its normal business services.

Situation Analysis- The process of evaluating the severity and consequences of an incident and communicating the results.

Software- A collection of instructions that describes a task, or set of tasks, to be carried out by a computer. More formally, it can be described as an expression of a computational method written in a computer language. Functional categories include application software, operating systems, video games, and compilers, among others. Computer programs embedded in hardware devices are called firmware. The formal expression of these computational methods in a human-readable computer language is often referred to as source code, while the machine-executable expressions of computational methods are commonly referred to as executables, object code, or binaries. A complete list of a data center's software can be found in the asset inventory and will include in-house applications, databases, third party supplied software, and vendor application services.

Stakeholder- Any individual, group, or organization that might affect, be affected by, or perceive itself to be affected by the emergency.

Standard- A document, the main text of which contains only mandatory provisions using the word "shall" to indicate requirements and which is in a form generally suitable for common reference by member firms.

The Audit Guidelines (the "guidelines") are intended to provide members of the Internal Auditors Division ("IAD"), an affiliate of the Securities Industry and Financial Markets Association ("SIFMA") with information for the purpose of developing or improving their approach towards auditing certain functions or products typically conducted by a registered broker-dealer. These guidelines do not represent a comprehensive list of all work steps or procedures that can be followed during the course of an audit and do not purport to be the official position or approach of any one group or organization, including IAD or any of its divisions or affiliates. Neither IAD, nor any of its divisions or affiliates, assumes any liability for errors or omissions resulting from the execution of any work steps within these guidelines or any other procedures derived from the reader's interpretation of such guidelines. In using these guidelines, member firms should consider the nature and context of their business and related risks to their organization and tailor the work steps accordingly. Internal auditors should always utilize professional judgment in determining appropriate work steps when executing an audit.