

## IT Examination Handbook Presentation Operations Booklet

### Visual

### Narrative

1.

#### *IT Handbook Presentations*

#### *Operations*



The *Operations Booklet* is designed to assist with the evaluation of risk management practices within the technology environments of financial institutions.

2.

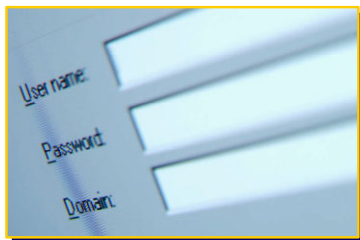
#### *Rescinds and Replaces*

- Chapter 13—Operations
- Chapter 17—Document Imaging

The booklet rescinds and replaces Chapters 13 “Operations” and 17 “Document Imaging” of the 1996 *FFIEC Information Systems Examination Handbook*.

3.

#### *Consistent Controls*



IT operations-related risk requires controls that are consistent with the nature and complexity of the specific technology environment. Thus, the booklet includes concepts and principles that can be applied to:

4.

#### *Consistent Controls*

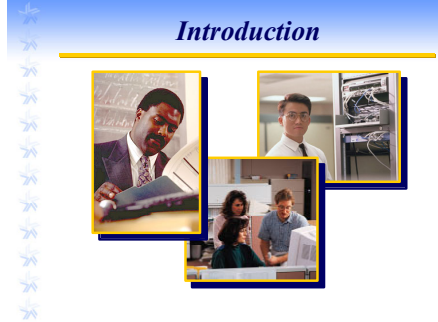
- Core operations
- Distributed operations
- Standalone microcomputers
- Support functions
- Affiliates

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

They are also applicable to smaller or less complex technology operations at community financial institutions.

**Visual****Narrative**

5.



The booklet introduction describes 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 an institution's information assets.

6.



In addition to specific content in the booklet itself, readers are encouraged to investigate other sources to find guidelines and best practices that might be helpful in either developing or reviewing their operational control needs. Although FFIEC does not endorse any specific resources, the booklet lists the following as resources that may be helpful:

- The National Institute of Standards and Technology,
- The International Organization for Standardization,
- The Information Systems Audit and Control Association's *Control Objectives for Information Technology (COBIT)*,
- The Institute of Internal Auditors, and
- The Committee of Sponsoring Organizations of the Treadway Commission.

7.



The booklet is divided into five sections:

- Roles and Responsibilities,
- Risk Identification,
- Risk Assessment,
- Risk Mitigation and Control Implementation, and
- Risk Monitoring and Reporting.

**Visual**

**Narrative**

8.

***Roles and Responsibilities***

The first section, Roles and Responsibilities, looks at the role of

9.

***Roles and Responsibilities***

- Boards of directors
- Senior management
- Operations management

boards of directors, senior management, and operations management, all of whom share in the responsibility of assuring a safe and sound operating environment.

This responsibility applies to both centralized and decentralized IT operations, and includes;

10.

***Roles and Responsibilities***

- Implementation
- Documentation
- Environmental controls
- Physical and logical security
- Operational continuity and resiliency
- Staffing and training
- External expertise

- Implementation,
- Documentation,
- Environmental controls,
- Physical and logical security,
- Operational continuity and resiliency,
- Adequate staffing and training, and
- Access to qualified external expertise.

11.

***Booklet Organization***

- Roles and Responsibilities
- Risk Identification
- Risk Assessment
- Risk Mitigation and Control Implementation
- Risk Monitoring and Reporting

The issue of risk identification, addressed in a separate section, emphasizes the need for management to have an in-depth understanding of the IT environments for which they are responsible.

**Visual**

**Narrative**

12.

**Risk**

- Environmental surveys
  - Resources
  - Physical locations
  - Hardware/Software configurations
  - Interfaces

Two risk management tools are discussed that can help management gain that understanding:

- Environmental surveys, which provide an enterprise-level view of resources, physical locations, hardware and software configurations, interfaces, and

13.

**Risk Identification**

- Environmental surveys
- Technology inventories
  - Hardware
  - Software
  - Network components and topology
  - Media

Technology inventories, which provide a detailed record of an institution's technology resources, including:

- Hardware,
- Software,
- Network components and topology, and
- Media.

14.

**Booklet Organization**

- Roles and Responsibilities
- Risk Identification
- **Risk Assessment**
- Risk Mitigation and Control Implementation
- Risk Monitoring and Reporting

The assessment of operations related risk is accomplished by analyzing the results of the environmental survey and technology inventory.

15.

**Risk Assessment**



The risk assessment factors management may need to consider are numerous and varied, and the combination of factors considered should be appropriate to the size, scale, complexity, and nature of the institution being examined.

**Visual****Narrative**

16.

***Interdependency and Risk***

However, successfully assessing potential risks and vulnerabilities requires more than simply reviewing data gained from the environmental survey and technology inventory. Connectivity and interdependence among systems, processes, and various IT elements can introduce vulnerabilities and potentially compromise an institution's security controls.

17.

***Prioritizing Efforts***

- Probability of occurrence
- The potential impact

Once an institution identifies and analyzes its universe of risks, management should prioritize their risk mitigation actions based on the:

- Probability of occurrence, and
- The potential impact to the institution's financial, reputational, or legal standing.

18.

***Potential Impact***

- Lost revenue
- Loss of market share
- Insurance premiums
- Litigation and adverse judgments
- Data recovery and reconstruction

Management should prioritize the risk assessment results based on the importance of the associated systems to the business. Considerations should include issues such as:

- Lost revenue,
- Loss of market share,
- Increased cost of insurance premiums,
- Litigation and adverse judgment costs, and
- Data recovery and reconstruction expenses.

19.

***Booklet Organization***

- Roles and Responsibilities
- Risk Identification
- Risk Assessment
- Risk Mitigation and Control Implementation
- Risk Monitoring and Reporting

Reflecting the booklet's emphasis on the daily operations and tactical activities associated with operational-related risk; the bulk of the booklet content is presented in the fourth section, *Risk Mitigation and Control Implementation*.

**Visual**

**Narrative**

20.

**Subsections**

- Policies, Standards, and Procedures
- Controls Implementation

This discussion is divided into two subsections, one on implementing policies, standards, and procedures; the other on issues associated with the actual implementation of risk mitigation controls.

21.

**Policies and Procedures**

Policies and procedures are important tools for risk mitigation, and should be established with consideration of how issues such as:

22.

**Policies and Procedures**

Consider issues such as...

- Segregation of duties
- Data entry controls
- Quality assurance programs
- Industry certification
- Operating thresholds and parameters

- Segregation of duties,
  - Data entry controls,
  - Quality assurance programs,
  - Industry certifications, and
  - Operating thresholds and parameters
- can be most effectively implemented within the IT environment of a given institution.

23.

**Balance**

- Business requirements
- Cost
- Efficiency
- Effectiveness

Management should balance implementation of these types of controls against business requirements, cost, efficiency, and effectiveness.


**Visual**

**Narrative**

24.

**Standardization**

- Simplify surveys and inventories
- Improve performance
- Reduce IT costs
- Allow for resource leveraging
- Enhance reliability and predictability
- Improve interoperability/integration
- Reduce re-configuration time



Standardization of hardware and software within the operating environment is another policy-related method of controlling operational-related IT risk. In addition to minimizing the complexities involved with technology-related risk management, standards can also help management to:

- Simplify the survey and inventory process,
- Improve IT operations performance,
- Reduce IT costs,
- Allow for resource leveraging,
- Enhance reliability and predictability,
- Improve interoperability and integration, and
- Reduce re-configuration time.

25.

**Subsections**

- Policies, Standards, and Procedures
- Controls Implementation

Implementing risk mitigation controls to reduce internal and external threats in IT operations is a complex process that requires a multitude of strategies.

Let's take a brief look at each of the risk mitigation techniques discussed in the booklet.

26.

**Environmental Controls**



Management should carefully assess the IT operations environment and implement relevant controls, such as backup power sources and alternative utility and telecommunication feeds from different vendors. In addition, institutions should test and be prepared to switch to these alternate resources rapidly.

27.

**Environmental Controls**

- Fire
- Floods
- Humidity



Controls should also be implemented to mitigate the impact of potential risks, such as fire, floods, and humidity to the physical environment.

**Visual**

**Narrative**

28.

*Preventive Maintenance*

---



Preventive maintenance plays an important role in controlling risk—minimizing potential equipment or systems failures that can negatively impact an institution’s ability to conduct critical business activities.

29.

*Security*

---



The security subsection discusses requirements for both physical and logical security controls.

30.

*Security*

---



- Gates
- Fences
- Alarms
- Armed guards
- Inventory labels
- Bar codes
- Logging procedures


Physical controls might include such things as video surveillance, gates, fences, alarms, armed guards, inventory labels, bar codes, or logging procedures.

31.

*Security*

---

- Preventive
- Detective
- Corrective



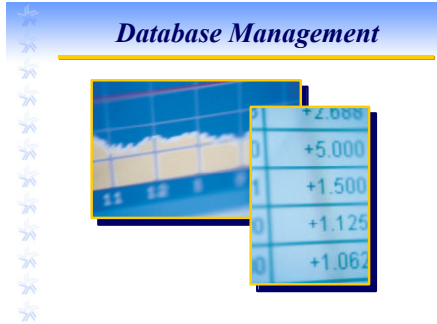
Logical controls should be based on the principle of "least privilege," and include preventive, or access, controls; detective controls, such as logging and sign in sheets; and corrective controls, including incident response procedures.



**Visual**

**Narrative**

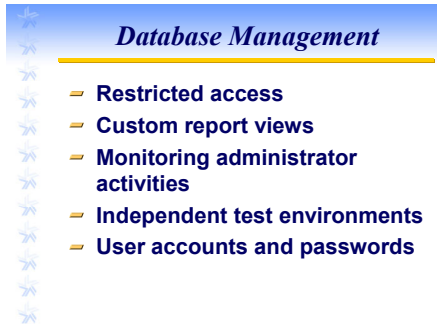
32.



Databases are repositories for some of a financial institution’s most critical information, and as such pose unique risks. Because databases often contain sensitive information, they are also often the targets of malicious activity from both internal and external sources.

Management's failure to adequately manage and secure databases can lead to the unintentional modification, loss, or disclosure of sensitive information.

33.



Risk mitigation of data base management should include consideration of activities such as:

- Restricted access
- Custom report views
- Monitoring administrator activities
- Independent test environments
- User accounts and passwords

- Restricting the use of and access to database systems,
- Creating custom views of database information, based on the unique work requirements of different users,
- Closely monitoring the activities of database administrators,
- Maintaining independent test environments to protect the integrity of actual production data, and
- Implementing user account and password authentication for access to database information.

34.



IT operations consist of more than technology and processes. The safety and soundness of an operation also requires appropriate and skilled personnel.

35.



Risk mitigation in the human resource area involves activities associated with the recruitment, hiring, training, placement, screening, and background checks of officers and staff.

- Recruitment
- Hiring
- Training
- Placement
- Screening
- Background checks

**Visual**

**Narrative**

36.

**Personnel Controls**

- Internal control procedures
  - Dual controls
  - Rotation of duties
  - Separation of duties

Furthermore, institutions should consider personnel policies that reference internal control procedures including dual controls, rotation of duties, and adequate separation of duties.

37.

**Personnel Controls**



In general, management should organize functional duties so that no one person performs a transactional process from beginning to end or checks the accuracy of his or her own work.

38.

**Change**



IT operations are dynamic, and, as such, undergo constant changes in technology, staff, and functions. Risk mitigation therefore requires that management have processes, procedures, and controls in place to manage change.

39.

**Change Management**

- Change Control
- Patch Management
- Conversions

The booklet discusses three facets of risk mitigation in the area of change management:

- Change Control,
- Patch Management, and
- Conversions.

**Visual**

**Narrative**

40.

**Change Management**

- Management Booklet
- Development and Acquisition Booklet

Institutional policies, procedures, and processes for implementing change are discussed more fully in the IT Handbook's *Management Booklet* and *Development and Acquisition Booklet*.

41.

**Distribution and Transmission**

- Output
- Transmission

Risk controls should address not only the IT operating environment, but also how information is distributed and transmitted. This includes system output of electronic and hard copy reports and the inbound and outbound transmission of information.

42.

**Storage and Backup**



Storage and backup are another critical area of risk mitigation. Financial institutions store vast amounts of data, the integrity and availability of which are critical to ongoing business operations.

43.

**Storage and Backup**



- Written standards
- Off-site storage

Institutions should:

- Have written standards that document back-up methodologies, delineate responsibilities, and ensure uniform performance throughout the institution; and
- Maintain off-site storage for data and program files in a secure location to assure recoverability in case production data is lost.

**Visual**

**Narrative**

44.

**Disposal of Media**



The media on which institutional data has been stored, paper, tapes, or CD-ROMs for example, should be disposed of in a manner that assures confidential information on them is destroyed.

45.

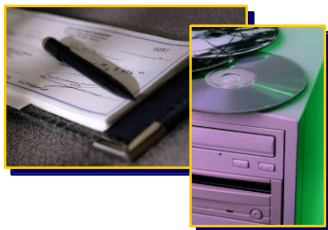
**Disposal of Media**



For example, when an institution is disposing of magnetic media, simply deleting files is not sufficient—procedures may include degaussing and other types of destruction that ensures no information remaining on the media is recoverable.

46.

**Imaging**



Imaging, or converting paper documents into electronic files, introduces yet another risk area for IT operations in contemporary financial institutions. The importance of adequately controlling such practices is demonstrated in recent legislation, The Check Clearing for the 21st Century Act addresses one particular application of this technology—that of capturing negotiable items such as checks as images.

47.

**Imaging**

- Capture
- Indexing
- Security
- Training
- Audit
- Back-up and recovery
- Legal issues

Management should ensure there are adequate controls to protect imaging processes, as many of the traditional controls, for paper-based systems, may not be effective. Considerations should include:

- Capture,
- Indexing,
- Security,
- Training,
- Audit,
- Back-up and recovery, and
- Legal issues.

**Visual****Narrative**

48.

***Event/Problem Management***

Effective event/problem management ensures appropriate controls are in place to identify, log, track, analyze, and resolve problems that occur during day-to-day operations.

49.

***Possible Events/Problems***

- Production program failure
- Out-of-balance conditions
- Different parties performing operational tasks
- Logging issues
- Network outages
- Termination of operations personnel
- Run time anomalies

Events or problems might include occurrences such as:

- Production program failure,
- Out-of-balance conditions,
- Different parties performing operational tasks,
- Logging issues,
- Network outages,
- Termination of personnel, or
- Run time anomalies.

50.

***Event/Problem Management***

- Identification
- Severity rating
- Impact and root cause analysis
- Documentation and tracking
- Contact and communication information
- Escalation process
- Resolution
- Management reporting

Event/problem-management plans should cover hardware, operating systems, applications, and security services and, at a minimum, should address:

- Problem identification,
- Rating of severity based on risk,
- Impact and root cause analysis,
- Documentation and tracking of the status of identified problems,
- Contact and communication information, including names or position titles, current phone numbers, and organizations that should be notified and the circumstances under which such notification should occur,
- The process for escalation,
- Resolution, and
- Management reporting.

**Visual**

**Narrative**

51.

**User Support**

An institution's support function should ensure that end users have continual access to the resources and services they need to perform their jobs in an efficient and effective manner.

Financial institutions that outsource any of their IT operations may themselves be end users, requiring user support such as help desks. Thus, controls in this area should address both internal support functions and those of third-party service providers.

52.

**Other Controls**

- Scheduling
- Negotiable instruments

The Risk Mitigation and Control Implementation section also offers a brief look at two additional areas that require special consideration as management implements operation-related risk controls:

- Scheduling, which can help prevent degraded processing performance and should include procedures for creating and changing job schedules with greater efficiency, and
- Negotiable instruments, which require specific controls to prevent financial loss.

53.

**Booklet Organization**

- Roles and Responsibilities
- Risk Identification
- Risk Assessment
- Risk Mitigation and Control Implementation
- Risk Monitoring and Reporting

The final section of the booklet looks at risk monitoring and reporting requirements.

54.

**Risk Monitoring and Reporting**

- Performance monitoring
- Capacity planning
- Control self-assessments

This section looks at three functions that can be used to support effective risk monitoring and reporting:

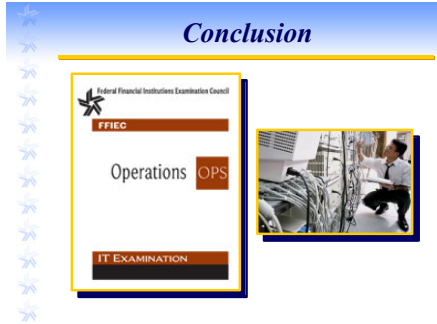
- Performance monitoring, which can provide assessment of IT operations efficiency relative to the institutional controls,
- Capacity planning, which involves using baseline performance data to model and project future needs, and
- Control self-assessments to validate the adequacy and effectiveness of the control environment.

	<b>Visual</b>	<b>Narrative</b>
55.	<p style="text-align: center;"><b><i>Booklet Organization</i></b></p> <ul style="list-style-type: none"> <li>– Appendix A: Examination Procedures</li> <li>– Appendix B: Glossary</li> </ul>	The booklet provides the standard examination and glossary appendices.
56.	<p style="text-align: center;"><b><i>Booklet Organization</i></b></p> <ul style="list-style-type: none"> <li>– Appendix A: Examination Procedures</li> <li>– Appendix B: Glossary</li> <li>– <b>Appendix C: Item Processing</b> <ul style="list-style-type: none"> <li>– Item processing overview</li> <li>– Proof operations</li> <li>– Magnetic ink character recognition</li> <li>– Optical character recognition</li> <li>– Balancing and reconciling</li> </ul> </li> </ul>	<p>Additionally, Appendix C provides information on item processing, including:</p> <ul style="list-style-type: none"> <li>▪ Item processing overview,</li> <li>▪ Proof operations,</li> <li>▪ Magnetic ink character recognition,</li> <li>▪ Optical character recognition, and</li> <li>▪ Balancing and reconciling.</li> </ul>
57.	<p style="text-align: center;"><b><i>Booklet Organization</i></b></p> <ul style="list-style-type: none"> <li>– Appendix A: Examination Procedures</li> <li>– Appendix B: Glossary</li> <li>– Appendix C: Item Processing</li> <li>– <b>Appendix D: Advanced Data Storage Solutions</b></li> </ul>	Appendix D provides information on advanced data storage options that may be appropriate for larger and complex operations.
58.	<p style="text-align: center;"><b><i>Advanced Data Storage Solutions</i></b></p> <ul style="list-style-type: none"> <li>– Storage area networks</li> <li>– Redundant array of independent disks</li> <li>– Network attached storage</li> <li>– Storage virtualization</li> </ul>	<p>Topics in this resource include:</p> <ul style="list-style-type: none"> <li>▪ Storage area networks, or SANs;</li> <li>▪ Redundant array of independent disks, or RAID;</li> <li>▪ Network attached storage, or NAS; and</li> <li>▪ Storage virtualization.</li> </ul>

**Visual**

**Narrative**

59.



Readers will find that the *Operations Booklet* provides a good overall assessment of the complex issues involved in management of operation-related risk.

60.



The booklet represents a valuable tool for examiners and institutional managers alike to identify sound risk management techniques that are appropriate for the nature and complexity of specific IT operating environments.