

IT Examination Handbook Presentation Management

Visual

Narrative

1.

IT Handbook Presentations

Management



Open music

2.

IT Management



- Maximizing the effective use
- Minimizing universal risks

Effective management of information technology systems is critical. Information Technology, or IT management has the dual responsibility of maximizing the effective use of IT within its institution while controlling the risks associated with the implementation of that technology.

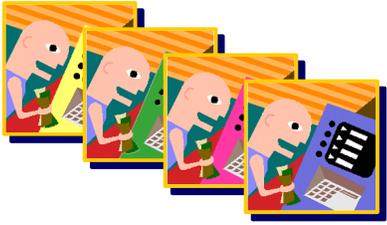
3.

Challenges

- Support across business units
- Increased interconnectivity
- Growing interdependence
- Need for larger budgets
- Increasing criticality of information
- Rapid changes in new technologies

Among the challenges faced by IT management in today's marketplace are:

- The demand for technology based solutions across all business units within an institution;
- The interconnection of multiple systems, operated not only by the institution, but also by third parties, and the public;
- A growing interdependence among infrastructure, applications, web content, and support functions;
- Increasing expenses for IT support and expansion;
- The criticality of providing timely and accurate information; and
- The rapid growth of technologies, which prompt increased investments in infrastructure, systems, and applications.

	Visual	Narrative
4.	<p style="text-align: center;">Unique Needs</p> 	<p>The unique characteristics of each financial institution define the technologies that will be most effective in supporting the needs, philosophies, and business lines of that institution. However, there are common risk factors associated with planning and managing virtually every IT solution.</p>
5.	<p style="text-align: center;">Organization</p> <ul style="list-style-type: none"> – Introduction – Risk Overview – Roles and Responsibilities – IT Risk Management Process – Management Considerations for Technology Service Providers 	<p>Hence, the Management Booklet is designed to provide guidance on the effective management of these common IT risk factors. The booklet looks at these issues in five sections:</p> <ul style="list-style-type: none"> ▪ Introduction, ▪ Risk Overview, ▪ Roles and Responsibilities, ▪ IT Risk Management Process, and ▪ Management Considerations for Technology Service Providers.
6.	<p style="text-align: center;">Management Booklet</p> 	<p>Although some issues are covered in other booklets in the <i>FFIEC IT Examination Handbook</i> series, this booklet looks at them from the perspective of IT management.</p>
7.	<p style="text-align: center;">Management Booklet</p>  <p style="margin-left: 20px;">– Chapter 9</p> <p style="margin-left: 20px;">– Chapter 11</p>	<p>This booklet replaces Chapter 9, <i>Management</i>, and Chapter 11, <i>Management Information Systems (MIS) Review of the 1996 FFIEC Information Systems Examination Handbook</i>.</p>

Visual

Narrative

8.

Integral to Operations



Over the past few years, IT has become such an integral part of the overall operations of every financial institution that the institution's IT functions can no longer be effectively managed in isolation.

9.

IT Support

- Internal data
- New products and services
- New electronic payment systems
- Different business lines

For example, IT now frequently supports not only the processing of internal data, but also:

- Provides avenues for new products and services,
- Enables new electronic payment systems, and
- Supports communications among different business lines within an institution.

With this new dependence on technology's support of multiple corporate goals, IT management has become an essential component of the overall management and operation in financial institutions.

10.

Organization

- Introduction
- Risk Overview
- Roles and Responsibilities
- IT Risk Management Process
- Management Considerations for Technology Service Providers

Having discussed the introduction section of the booklet, let's look at the information within each of the remaining sections that can support this increasing responsibility of IT management beginning with Risk Overview.

11.

Risk Overview



Operational Risk

Operational risk is the primary risk associated with information technology.

Management should be particularly aware of the implications of operational risk factors, such as:

	Visual	Narrative
12.	<p style="text-align: center;">Operational Risk</p> <hr/> <ul style="list-style-type: none"> - Liquidity, interest, and price risk 	<ul style="list-style-type: none"> ▪ The fact that reliance on technology to provide information on changes in credit, external markets, and information about specific customers, exposes an institution to increased liquidity, interest, and price risk.
13.	<p style="text-align: center;">Operational Risk</p> <hr/> <ul style="list-style-type: none"> - Liquidity, interest, and price risk - Reputation risk <ul style="list-style-type: none"> - Confidential customer information - Public website 	<ul style="list-style-type: none"> ▪ Reputation risk stems from errors, delays, or omissions in information that can result in potential loss of customers. IT increases an institution's vulnerability to this type risk in two significant areas—the potential for unauthorized access to, or the disclosure of, confidential customer information and the potential of external attacks on the institution's public website.
14.	<p style="text-align: center;">Operational Risk</p> <hr/> <ul style="list-style-type: none"> - Liquidity, interest, and price risk - Reputation risk - Strategic risk 	<ul style="list-style-type: none"> ▪ Strategic risk stems from the potential for management to use inaccurate information and inaccurate or incomplete analysis of data when making strategic decisions, thus increasing the likelihood that they will make strategic decisions that are detrimental to the institution's growth and prosperity. <p>Since it has become more and more common to base strategic decisions on information provided by an IT unit, IT has become a critical aspect of an organization's strategic risk.</p>
15.	<p style="text-align: center;">Operational Risk</p> <hr/> <ul style="list-style-type: none"> - Liquidity, interest, and price risk - Reputation risk - Strategic risk - Compliance risk 	<ul style="list-style-type: none"> ▪ Compliance, or legal, risk results from an institution's inability to meet the regulatory and legal requirements associated with its IT products and services. For example, unauthorized disclosure of confidential information can lead to civil or criminal liability.

	Visual	Narrative
16.	<p style="text-align: center;">Organization</p> <hr/> <ul style="list-style-type: none"> - Introduction - Risk Overview - Roles and Responsibilities - IT Risk Management Process - Management Considerations for Technology Service Providers 	<p>Controlling IT risks requires concentrated effort on the part of many individuals and units within an institution.</p>
17.	<p style="text-align: center;">Roles</p> <hr/> <ul style="list-style-type: none"> - Board of Directors / Steering Committee - Chief Information Officer / Chief Technology Officer - IT Line Management - Business Unit Management 	<p>Effective IT risk management starts with a Board that is aware of and involved in decisions relating to the IT activities within the organization, but it must also be firmly enforced by all levels of the organizations management, including:</p> <ul style="list-style-type: none"> ▪ The Chief Information or Technology Officer, ▪ All levels of IT line managers, and ▪ Business unit managers <p>After discussing the specific roles each of these management levels play in the overall IT program within an institution, the booklet looks at some of the individual responsibilities that need to be carried out.</p>
18.	<p style="text-align: center;">Responsibilities</p> <hr/> <ul style="list-style-type: none"> - Risk Management Areas - Project Management - Other IT Functions and Support Roles 	<p>These responsibilities are broken down into three categories:</p> <ul style="list-style-type: none"> ▪ Risk Management Areas, ▪ Project Management, and ▪ Other IT Functions and Support Roles.
19.	<p style="text-align: center;">Responsibilities</p> <hr/> <ul style="list-style-type: none"> - Risk Management Areas <ul style="list-style-type: none"> - Information security - Business continuity - IT audit - Insurance - Compliance with regulations 	<p>Management is responsible for assuring that adequate risk management functions exist within the organization. Management should establish controls in all areas where IT risks can potentially impact operations—areas such as information security, business continuity, IT audit, insurance, and compliance with regulations.</p>

	Visual	Narrative
20.	<p style="text-align: center;"><i>Multiple Approaches</i></p> 	<p>While some institutions have a separate risk management department that is responsible for overseeing the various areas of IT risk, other institutions establish a system where risk management responsibilities are shared among various operating units. Either way, risk management functions should play a key role in measuring, monitoring, and controlling risks within the institution.</p>
21.	<p style="text-align: center;"><i>Responsibilities</i></p> <ul style="list-style-type: none"> - Risk Management Areas - Project Management - Other IT Functions and Support Roles 	<p>Effective project management is key to the success of any internal business effort, and IT is no exception.</p>
22.	<p style="text-align: center;"><i>Effective Project Management</i></p> 	<p>A financial institution's ability to manage projects drives its ability to adapt to changes in its business requirements and to satisfy its strategic objectives.</p> <p>Sound project management techniques assist management to effectively control system acquisition and development projects, as well as other activities such as system conversions, product enhancements, infrastructure upgrades, and system maintenance.</p>
23.	<p style="text-align: center;"><i>Project Management</i></p> <ul style="list-style-type: none"> - Initiating - Planning - Executing - Controlling - Closing projects 	<p>Although the formality of project management practices will vary with the complexity of the project and the institution's business lines, generally, project management consists of initiating, planning, executing, controlling, and closing projects.</p>

	Visual	Narrative
24.	<p style="text-align: center;">Responsibilities</p> <ul style="list-style-type: none"> - Risk Management Areas - Project Management - Other IT Functions and Support Roles <ul style="list-style-type: none"> - Human resource planning - Management information systems and reporting 	<p>The booklet also looks at two other types of responsibilities important in effectively managing IT risks: human resource planning and management information systems and reporting.</p>
25.	<p style="text-align: center;">Human Resource Planning</p> 	<p>The functionality and reliability of any IT system is only as good as the staff that installs, uses, and maintains it. The importance of human resource management is far too often overlooked as being a critical element in effective IT management.</p>
26.	<p style="text-align: center;">Human Resource Planning</p> 	<p>Human resource management must hire and maintain a competent and motivated workforce, and organizations should have an effective IT human resources management plan that meets the requirements for its particular IT systems and the business lines they support.</p>
27.	<p style="text-align: center;">Human Resource Planning</p> <ul style="list-style-type: none"> - Compensation planning - Performance reviews - Participation in industry forums - Knowledge transfer mechanisms - Training - Mentoring 	<p>The components of an effective IT human resources management process include:</p> <ul style="list-style-type: none"> ▪ Compensation planning, ▪ Performance reviews, ▪ Participation in industry forums, ▪ Knowledge transfer mechanisms, such as rotational assignments, ▪ Continued training, and ▪ Mentoring.

Visual

Narrative

28.

Incentive Programs



The board should also define and enforce incentive programs for IT management, similar to those available for other senior managers and put programs in place to ensure its IT staff has the current expertise necessary to achieve company goals and objectives.

29.

External Expertise



And, in some cases, institutions may need to look outside of the organization for expertise in specialized areas that require temporary or consulting support for the internal IT staff.

30.

Other Functions and Roles

- **Human resource planning**
- **Management information system and reporting**

The booklet also looks at the role management information systems, or MIS, plays in the overall success of an institution. MIS is a process that provides the information necessary to manage an organization effectively, and typically involves a substantial amount of computer-generated information. Therefore, MIS should be considered as an integral part of overall IT management and IT risk management.

31.

MIS Reporting



IT management is typically responsible for the policies, procedures, and controls that are necessary to effectively administer database management and report creation and ensure the effectiveness and usefulness of the organization's MIS reporting.

	Visual	Narrative
32.	<p style="text-align: center;">Organization</p> <hr/> <ul style="list-style-type: none"> - Introduction - Risk Overview - Roles and Responsibilities - IT Risk Management Process - Management Considerations for Technology Service Providers 	<p>The bulk of the booklet's content centers on the actual processes required to effectively manage IT risks. Central to all risk management is:</p>
33.	<p style="text-align: center;">IT Risk Management Process</p> <hr/> <ul style="list-style-type: none"> - Effective planning process - Ongoing risk assessment - Appropriate controls - Effective measurement and monitoring 	<ul style="list-style-type: none"> ▪ An effective planning process that aligns IT and business objectives; ▪ An ongoing risk assessment process that evaluates the environment and potential changes; ▪ Technology implementation procedures that include appropriate controls; and ▪ Measurement and monitoring efforts that effectively identify ways to manage risk exposure. <p>The booklet looks at each of the issues in four separate subsections.</p>
34.	<p style="text-align: center;">IT Risk Management Process</p> <hr/> <ul style="list-style-type: none"> - Planning IT Operations and Investment - Risk Identification and Assessment - IT Controls Implementation - Measure and Monitor 	<p>Let's take a brief look at each of these subsections, starting with Planning IT Operations and Investment.</p>
35.	<p style="text-align: center;">Operations/Investment Planning</p> <hr/> 	<p>Planning involves preparing for future activities by defining the specific goals and strategies needed to achieve them. The goals for IT operations and investment in IT should be consistent with the organization's operational planning.</p>

	Visual	Narrative
36.	<p style="text-align: center;">Essential Criteria</p> <ul style="list-style-type: none"> - Align IT with strategic plan - Align IT with business units - Support current and planned business operations - Integrate IT spending and weigh benefits - Ensure consideration of risks in new IT investments 	<p>IT operations and IT investment planning should:</p> <ul style="list-style-type: none"> ▪ Align IT with the corporate-wide strategic plan; ▪ Align IT strategically and operationally with business units; ▪ Maintain an IT infrastructure to support current and planned business operations; ▪ Integrate IT spending into the budgeting process and weigh direct and indirect benefits against the Total Cost of Ownership of the technology; and ▪ Ensure potential risks are identified and assessed before changes or new investments in technology.
37.	<p style="text-align: center;">IT Risk Management Process</p> <ul style="list-style-type: none"> - Planning IT Operations and Investment - Risk Identification and Assessment - IT Controls Implementation - Measure and Monitor 	<p>Institutions with less complex systems may have a more simplified risk-assessment process. However, all institutions should have a formal process that assists management in adapting to the continual changes inherent in IT environments.</p>
38.	<p style="text-align: center;">Process Effectiveness</p> 	<p>Examiners should measure the effectiveness of the institution's risk-assessment 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.</p>
39.	<p style="text-align: center;">Four Critical Steps</p> <ul style="list-style-type: none"> - Ongoing data collection - Risk analysis - Prioritization - Ongoing monitoring 	<p>Effective risk-assessment processes involve four critical steps:</p> <ul style="list-style-type: none"> ▪ Ongoing data collection from new initiatives or monitoring of existing activities, ▪ Risk analysis regarding the potential impact of the risks, ▪ Prioritization of controls and mitigating actions, and ▪ Ongoing monitoring of risk mitigation activities.

Visual

Narrative

40.

IT Risk Management Process

- Planning IT Operations and Investment
- Risk Identification and Assessment
- **IT Controls Implementation**
- Measure and Monitor

In addition to identifying and assessing potential IT risks, management must also implement satisfactory control practices as part of its overall IT risk mitigation strategy. The third section of the booklet provides a set of guidelines for establishing these controls, which are applicable both to the institution's in-house IT activities and to all external service providers that the institution uses for IT functions.

41.

IT Control Areas

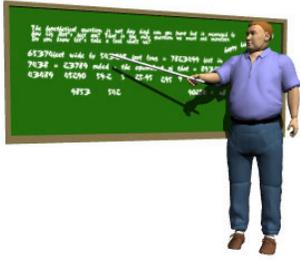
- Policies, Standards, and Procedures
- Internal Controls
- Personnel
- Insurance
- Information Security
- Business Continuity
- Software Development and Acquisition
- Operations
- Outsourcing Risk Management

This section discusses nine areas for control implementation:

- Adoption and enforcement of IT Policies, Standards, and Procedures;
- Internal Controls, that effectively mitigate the identified risks associated with IT processes;
- Personnel, where standards for hiring, changing duties, and terminating IT personnel should be established for internal staff, consultants, temporary employees, and other external parties;
- Insurance coverage and needs, which should be reviewed annually;
- Information Security, as the unauthorized loss, destruction, or disclosure of confidential information can adversely affect a financial institution's earnings and capital;
- Formal Business Continuity plans for each critical area of operation;
- Software Development and Acquisition;
- Operations, for all IT groups within the organization; and
- Outsourcing Risk Management, including oversight and management of third-party relationships.

42.

Training



Many of these control areas require not only detailed planning and oversight, but also sufficient staff training to ensure their accurate and continued implementation. For example, an organization's policies, standards, and procedures are only effective if the staff fully understands and implements them. Training and awareness programs are needed to promote understanding and increase individual accountability

	Visual	Narrative																																				
43.	<p><i>IT Risk Management Process</i></p> <ul style="list-style-type: none"> - Planning IT Operations and Investment - Risk Identification and Assessment - IT Controls Implementation - Measure and Monitor 	<p>The final process discussed is measuring and monitoring.</p> <p>In order to be successful, IT risk management must be a dynamic process—keeping up with changes in business lines, technology, software, outsourcing relationships, and the sophistication of potential attackers.</p>																																				
44.	<p><i>Measure and Monitor</i></p> <ul style="list-style-type: none"> - Business plans - Plan to actual outcome comparisons - Performance benchmarks - Service level agreements - Quality assurance and control - Policy compliance 	<p>Institutions should establish measuring and monitoring programs that include strategies such as:</p> <ul style="list-style-type: none"> ▪ Routine review of business plans as they relate to information technology, ▪ Measuring actual outcomes against planned results, ▪ Establishing performance benchmarks, ▪ Periodic review of service level agreements, ▪ Integration of quality assurance and quality control programs, and ▪ Organizational compliance with established policies. 																																				
45.	<p><i>Metrics</i></p> <table border="1"> <caption>Approximate data from the 'Metrics' chart</caption> <thead> <tr> <th>Period</th> <th>Outcome (Yellow)</th> <th>Plan (Blue)</th> <th>Total</th> </tr> </thead> <tbody> <tr><td>1</td><td>100</td><td>100</td><td>200</td></tr> <tr><td>2</td><td>200</td><td>100</td><td>300</td></tr> <tr><td>3</td><td>300</td><td>100</td><td>400</td></tr> <tr><td>4</td><td>400</td><td>900</td><td>1300</td></tr> <tr><td>5</td><td>300</td><td>500</td><td>800</td></tr> <tr><td>6</td><td>400</td><td>400</td><td>800</td></tr> <tr><td>7</td><td>600</td><td>800</td><td>1400</td></tr> <tr><td>8</td><td>500</td><td>400</td><td>900</td></tr> </tbody> </table>	Period	Outcome (Yellow)	Plan (Blue)	Total	1	100	100	200	2	200	100	300	3	300	100	400	4	400	900	1300	5	300	500	800	6	400	400	800	7	600	800	1400	8	500	400	900	<p>Using metrics as part of the monitoring process will aid management in assessing their overall IT mitigation program. The nature and frequency of metric reports will depend upon the makeup of the institution's IT environment.</p>
Period	Outcome (Yellow)	Plan (Blue)	Total																																			
1	100	100	200																																			
2	200	100	300																																			
3	300	100	400																																			
4	400	900	1300																																			
5	300	500	800																																			
6	400	400	800																																			
7	600	800	1400																																			
8	500	400	900																																			
46.	<p><i>Organization</i></p> <ul style="list-style-type: none"> - Introduction - Risk Overview - Roles and Responsibilities - IT Risk Management Process - Management Considerations for Technology Service Providers 	<p>The final section of this booklet looks at IT risk management responsibilities as they specifically relate to technology service providers, or TSPs.</p>																																				

	Visual	Narrative
47.	<p style="text-align: center;">Outsourcing Resources</p> 	<p>Although the Outsourcing Technology Services Booklet provides detailed guidance on this topic, this section in the Management Booklet focuses on additional management considerations that TSPs should address in order to appropriately support financial institution customers in meeting safety and soundness and consumer compliance obligations.</p>
48.		
49.	<p style="text-align: center;">TSP Oversight</p> <ul style="list-style-type: none"> - Quality of service - Financial condition - Control environment 	<p>Management of financial institutions using TSPs for IT-related services is responsible for overseeing the quality of service and financial condition of the TSP, and the TSP's control environment. Financial institutions should expect TSP support at a level consistent with the criticality of the services being provided.</p>
50.	<p style="text-align: center;">TSP Support</p> <ul style="list-style-type: none"> - Audited financial statements - Clear contracts - Independent audit programs - Responsive customer service 	<p>TSPs should support their customer institution's by:</p> <ul style="list-style-type: none"> ▪ Providing audited financial statements at least annually; ▪ Negotiating clear contracts with appropriate language; ▪ Implementing independent audit programs governing TSP controls and reporting findings to customers; and ▪ Providing responsive customer service including user group support.
51.	<p style="text-align: center;">Organization</p> <ul style="list-style-type: none"> - Introduction - Risk Overview - Roles and Responsibilities - IT Risk Management Process - Management Considerations for Technology Service Providers - Examination Procedures - Laws, Regulations, and Guidance 	<p>In addition to the five sections in the body of the booklet, the booklet appendices contain a set of examination procedures and a list of references relating to the management of IT in financial institutions.</p>

Visual

Narrative

52.

Conclusion

Sound management of technology involves more than containing costs and controlling operational risks. An institution that is capable of aligning its IT infrastructure to support its business strategy adds value to its organization and positions itself for sustained success. The Board and executive management must understand and take responsibility for IT management as a critical component of their overall corporate governance efforts.