MOSSADAMS

IT Control Reviews

Chris Wetzel, Senior Manager
Financial Services Consulting

Learning Objectives

- Increase understanding of IT Controls
- Learn how best to assess if controls are operating effectively
- Develop practical approaches to completing reviews

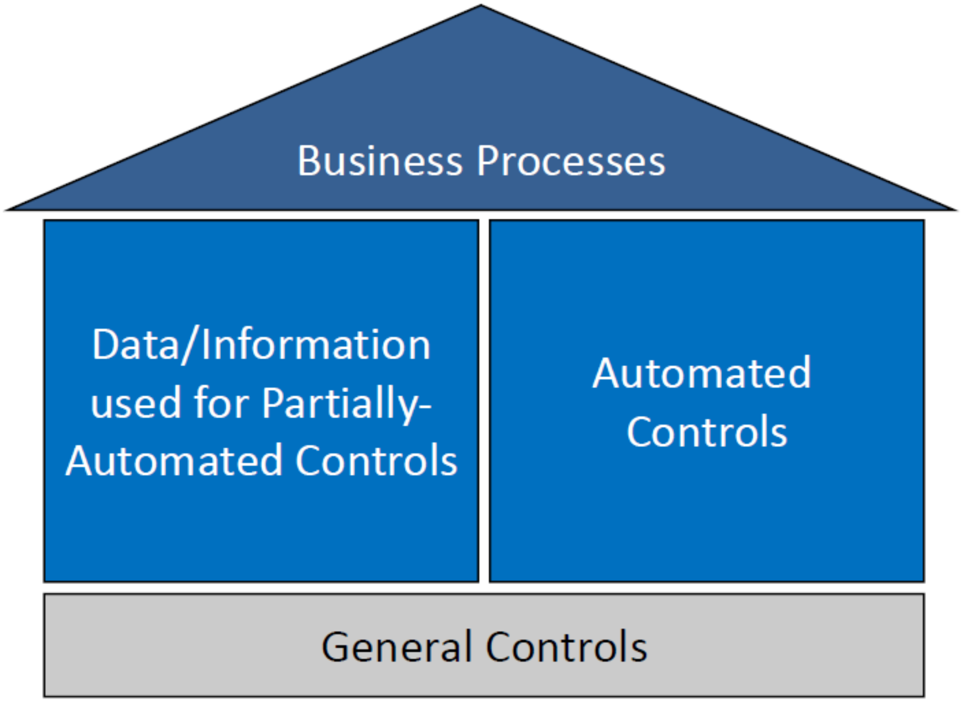
Today’s Lineup

- IT Level Set
- Cybersecurity
- Information Security
- Vendor Management
- Disaster Recovery and Business Continuity Planning

Key IT Terms in Banking

- Core Processor/Core System
- Item Processing
- Electronic Banking
- Outsourced vs. In-house
- GLBA 501(b)
  (12 CFR Part 30 / 12 CFR Part 748)
- SSAE 16, SSAE 18
- Patch Management
- Logical Controls
- Multi-Factor Authentication

Importance of IT General Controls



Common IT General Controls

- Organizational controls
- Logical access controls over applications, data and supporting infrastructure
- Change management controls
- Backup and recovery controls
- Computer operation controls
- Physical security controls
- System development life cycle controls

Check This Out – IIA IT General Controls

IT Control Reviews

- FFIEC IT Examination Handbook
- Regulatory Guidance
- FDIC/NCUA IT Examination Guide
- ISO 27002 Standard – Information Security Management
- NIST (National Institute of Standards and Technology) Standards
- CIS (Center for Internet Security) Critical Security Controls

Cybersecurity Threats

Looking back...

According to the Verizon 2016 Data Breach Investigation Report, in 2015 Financial Services was 3rd highest in reported incidents of all industry categories, and #1 in confirmed data loss.

Cybersecurity Threats

According to the Verizon 2017 Data Breach Investigation Report, in 2016 Financial Services was ranked 4th in reported incidents among all industry categories...and **still** ranked 1st in confirmed data disclosure/loss.

According to the Verizon 2018 DBIR, in 2017 Financial Services had 598 reported incidents resulting in 146 confirmed breaches...about a 25% success rate. (Or, should we say, failure rate?)

The Price of Cybersecurity Threats

- The Price of Data
  - Social Security Number: $3 - $5
  - Credit Card Number: $2 - $4 with full name, card type, expiration date and CCV
  - PayPal Account: $20 - $35
  - Medical Record: $50
- Cost of data breaches and cybercrime was estimated at over $530 billion in 2015
- By 2019, that number is expected to top an estimated $2.1 trillion
- In 2016, Financial Industry Avg. Cost of Data Breach = $264/record

Sources: “The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation,” Juniper Research (12/5/15); “2016 Data Breach Investigations Report,” Verizon (April 2016); “2016 Cost of Data Breach Study: United States,” Ponemon Institute (June 2016)

2016 Financial Sector Breaches

Company or Agency	State	# of Records Exposed
Southern Michigan Bank & Trust	MI	38,601
M Holdings Securities	OR	19,012
Primary Residential Mortgage	UT	2,889
Freddie Mac	VA	2,361
Rockland Trust	MA	2,182
QR Lending	FL	1,487
First Home Mortgage Corp.	MD	1,300
Nationwide Retirement Solutions	OH	457
Ash Brokerage Firm	IN	423
Ameriprise	MN	350

Source: Data Breach Reports: 2016 End of Year Report, Identity Theft Resource Center

Check This Out – https://www.idtheftcenter.org/2017-data-breaches

Cybersecurity and Internal Audit

It’s time to game plan…

- What can Internal Audit do to assist their organization’s cybersecurity efforts?

Cybersecurity Assessment Tool

May 31, 2017 – Press Release: FFIEC Release Update to Cybersecurity Assessment Tool

- Revised mapping in Appendix A of the FFIEC IT Examination Handbook to the updated Information Security and Management booklets.

- Additional response option for assessing maturity levels: “Yes with Compensating Controls” (allows management to include supplementary or complementary behaviors, practices and processes that support its cybersecurity activity assessment).

Cybersecurity Assessment Tool

Domain 1: Cyber Risk Management and Oversight

- Risk Management – Baseline **Audit** Controls
  - Independent audit or review evaluates policies, procedures, and controls across the institution for significant risks and control issues associated with the institution's operations, including risks in new products, emerging technologies, and information systems.
  - The independent audit function validates controls related to the storage or transmission of confidential data.
  - Logging practices are independently reviewed periodically to ensure appropriate log management (e.g., access controls, retention, and maintenance).
  - Issues and corrective actions from internal audits and independent testing/assessments are formally tracked to ensure procedures and control lapses are resolved in a timely manner.

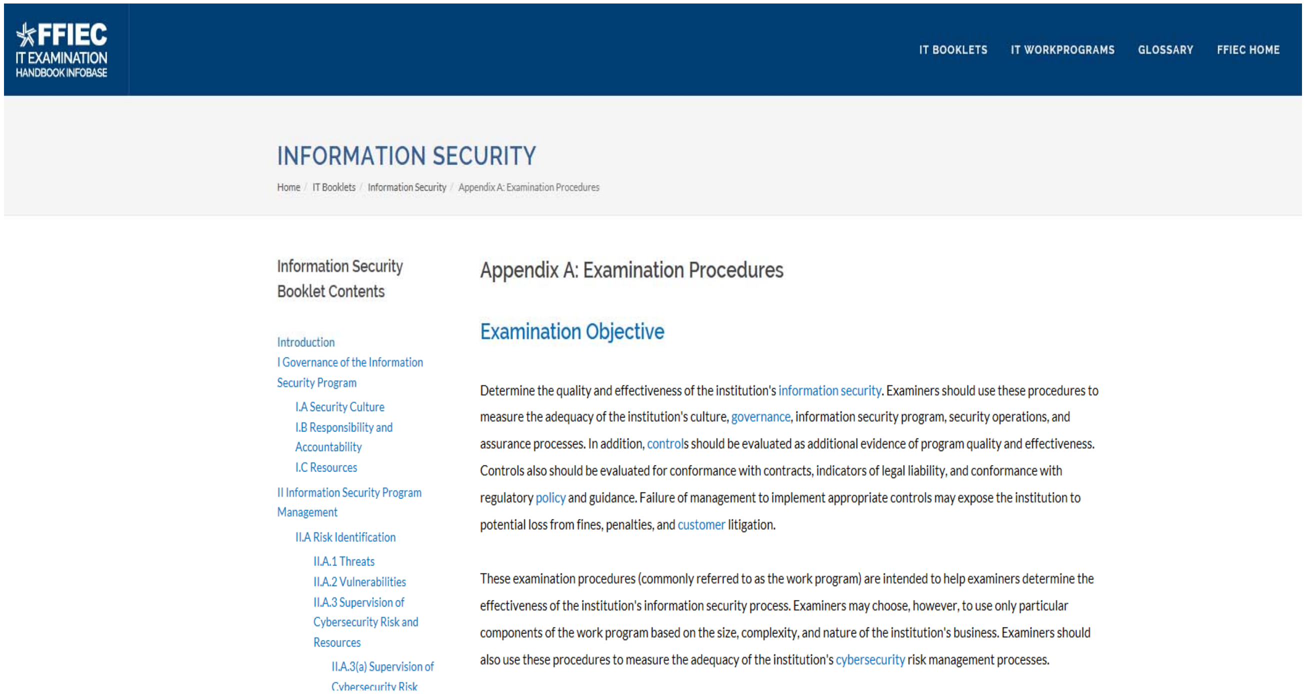
Information Security

Compliance with GLBA 501(b)

(12 CFR Part 30 / 12 CFR Part 748)

- Develop and implement a comprehensive written information security program
- Involve the Board of Directors
- Assess Risk
- Manage and Control Risk
- Oversee Service Provider Arrangements
- Adjust the Program
- Report to the Board

Information Security



INFORMATION SECURITY

Information Security Booklet Contents

Appendix A: Examination Procedures

Examination Objective

Determine the quality and effectiveness of the institution's information security. Examiners should use these procedures to measure the adequacy of the institution's culture, governance, information security program, security operations, and assurance processes. In addition, controls should be evaluated as additional evidence of program quality and effectiveness. Controls also should be evaluated for conformance with contracts, indicators of legal liability, and conformance with regulatory policy and guidance. Failure of management to implement appropriate controls may expose the institution to potential loss from fines, penalties, and customer litigation.

These examination procedures (commonly referred to as the work program) are intended to help examiners determine the effectiveness of the institution's information security process. Examiners may choose, however, to use only particular components of the work program based on the size, complexity, and nature of the institution's business. Examiners should also use these procedures to measure the adequacy of the institution's cybersecurity risk management processes.

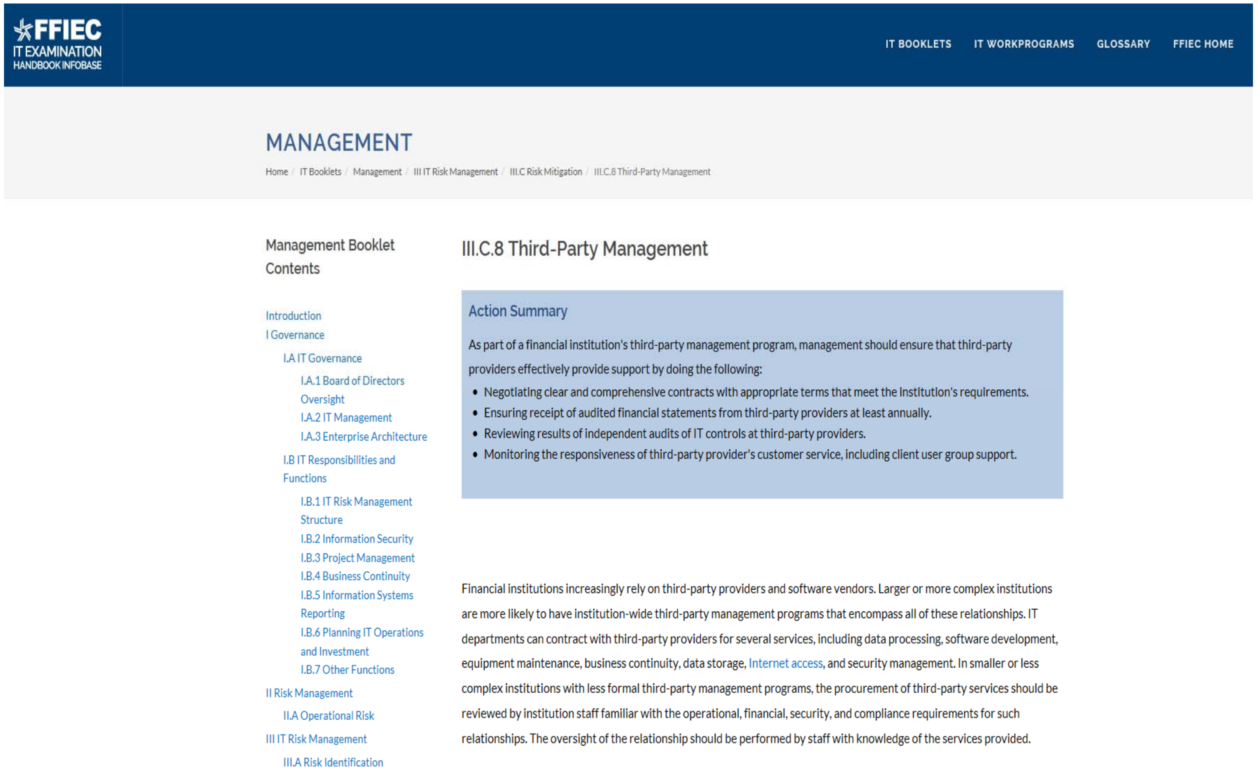
Vendor Management

- Governance
- Compliance
- Architecture/Software Scalability
- Access Management
- Data Protection and Security
- Availability and Recovery
- Incident Response

Vendor Management

- Review and Test
    - Contracts and Service Level Agreements
    - Vendor risk assessment
    - Review of SSAE 16/SSAE 18 reports
    - Review of financial statements
    - Review of performance
    - Review of access events / logging

Vendor Management



MANAGEMENT

Home / IT Booklets / Management / III IT Risk Management / III.C Risk Mitigation / III.C.8 Third-Party Management

Management Booklet Contents

III.C.8 Third-Party Management

Action Summary

As part of a financial institution's third-party management program, management should ensure that third-party providers effectively provide support by doing the following:

- Negotiating clear and comprehensive contracts with appropriate terms that meet the institution's requirements.
- Ensuring receipt of audited financial statements from third-party providers at least annually.
- Reviewing results of independent audits of IT controls at third-party providers.
- Monitoring the responsiveness of third-party provider's customer service, including client user group support.

Financial institutions increasingly rely on third-party providers and software vendors. Larger or more complex institutions are more likely to have institution-wide third-party management programs that encompass all of these relationships. IT departments can contract with third-party providers for several services, including data processing, software development, equipment maintenance, business continuity, data storage, Internet access, and security management. In smaller or less complex institutions with less formal third-party management programs, the procurement of third-party services should be reviewed by institution staff familiar with the operational, financial, security, and compliance requirements for such relationships. The oversight of the relationship should be performed by staff with knowledge of the services provided.

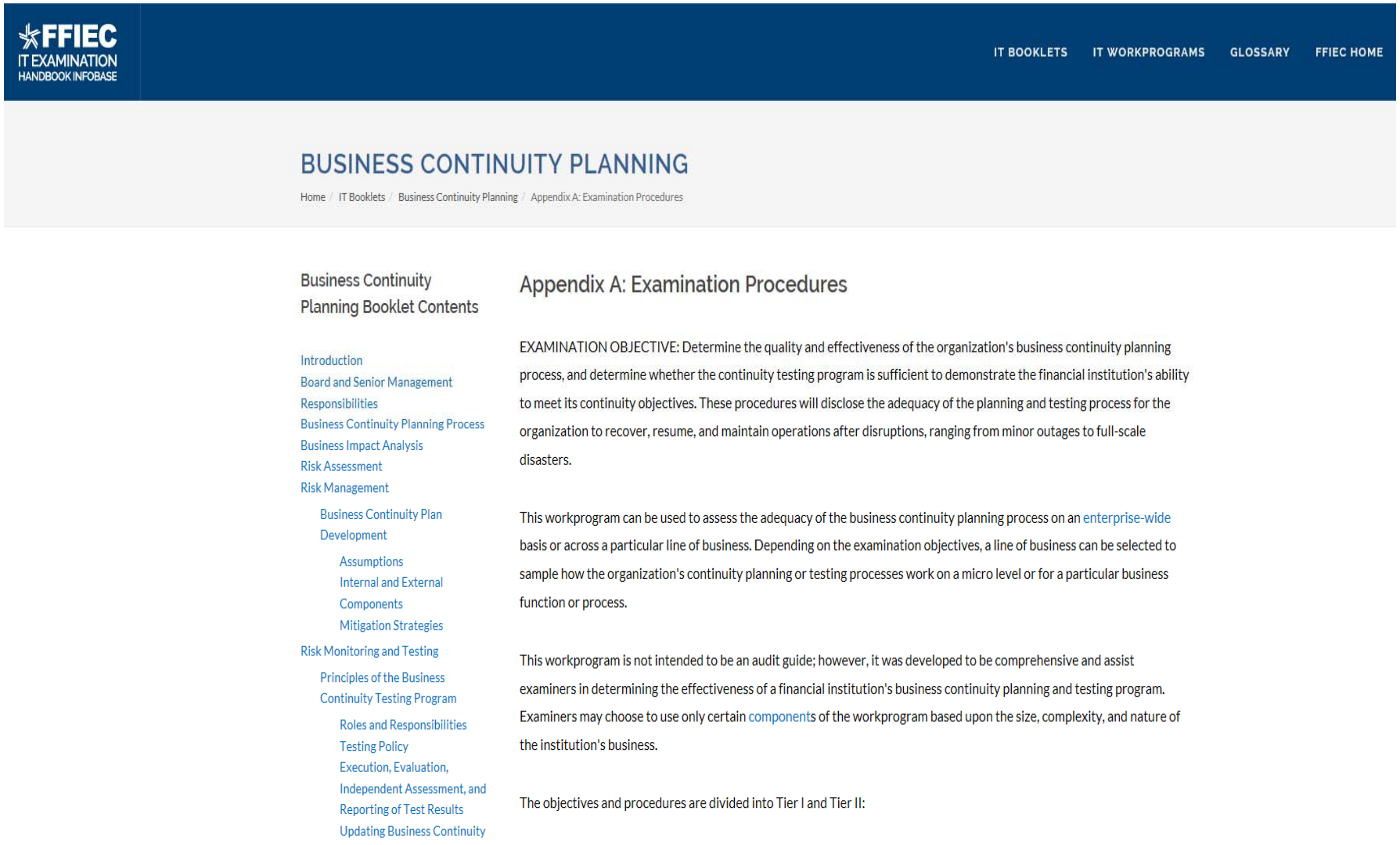
Disaster Recovery and Business Continuity Planning

- Business Impact Assessment (BIA)
  - Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
  - Ensure business units have articulated critical processes
- DR/BCP documentation
- Training – Key recovery team personnel and individual business units
- Testing – Internal and external; frequency
- Reporting to senior management and the Board

Key DR/BCP Questions

- Does the plan cover all business units and critical operations and processes?
- Is senior management's involvement and oversight sufficient?
- Are testing activities balanced with walk-through exercises and functional recovery of critical infrastructure?
- Is the institution's level of dependence on external third parties appropriate?

DR/BCP Review


FFIEC
IT EXAMINATION
HANDBOOK INFOBASE
IT BOOKLETS
IT WORKPROGRAMS
GLOSSARY
FFIEC HOME
Home / IT Booklets / Business Continuity Planning / Appendix A: Examination Procedures

BUSINESS CONTINUITY PLANNING

Business Continuity Planning Booklet Contents

Appendix A: Examination Procedures

EXAMINATION OBJECTIVE: Determine the quality and effectiveness of the organization's business continuity planning process, and determine whether the continuity testing program is sufficient to demonstrate the financial institution's ability to meet its continuity objectives. These procedures will disclose the adequacy of the planning and testing process for the organization to recover, resume, and maintain operations after disruptions, ranging from minor outages to full-scale disasters.

This workprogram can be used to assess the adequacy of the business continuity planning process on an enterprise-wide basis or across a particular line of business. Depending on the examination objectives, a line of business can be selected to sample how the organization's continuity planning or testing processes work on a micro level or for a particular business function or process.

This workprogram is not intended to be an audit guide; however, it was developed to be comprehensive and assist examiners in determining the effectiveness of a financial institution's business continuity planning and testing program. Examiners may choose to use only certain components of the workprogram based upon the size, complexity, and nature of the institution's business.

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

MOSSADAMS

Questions?

Chris Wetzel, Senior Manager
Financial Services Consulting
chris.wetzel@mossadams.com

The material appearing in this presentation is for informational purposes only and should not be construed as advice of any kind, including, without limitation, legal, accounting, or investment advice. This information is not intended to create, and receipt does not constitute, a legal relationship, including, but nor limited to, an accountant-client relationship. Although this information may have been prepared by professionals, it should not be used as a substitute for professional services. If legal, accounting, investment, or other professional advice is required, the services of a professional should be sought.

Assurance, tax, and consulting offered through Moss Adams LLP. Wealth management offered through Moss Adams Wealth Advisors LLC. Investment banking offered through Moss Adams Capital LLC.

THANK
YOU