MOSSADAMS

IT Auditing for the Non-IT Auditor

Chris Wetzel, Senior Manager
Financial Services Advisory

Learning Objectives

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

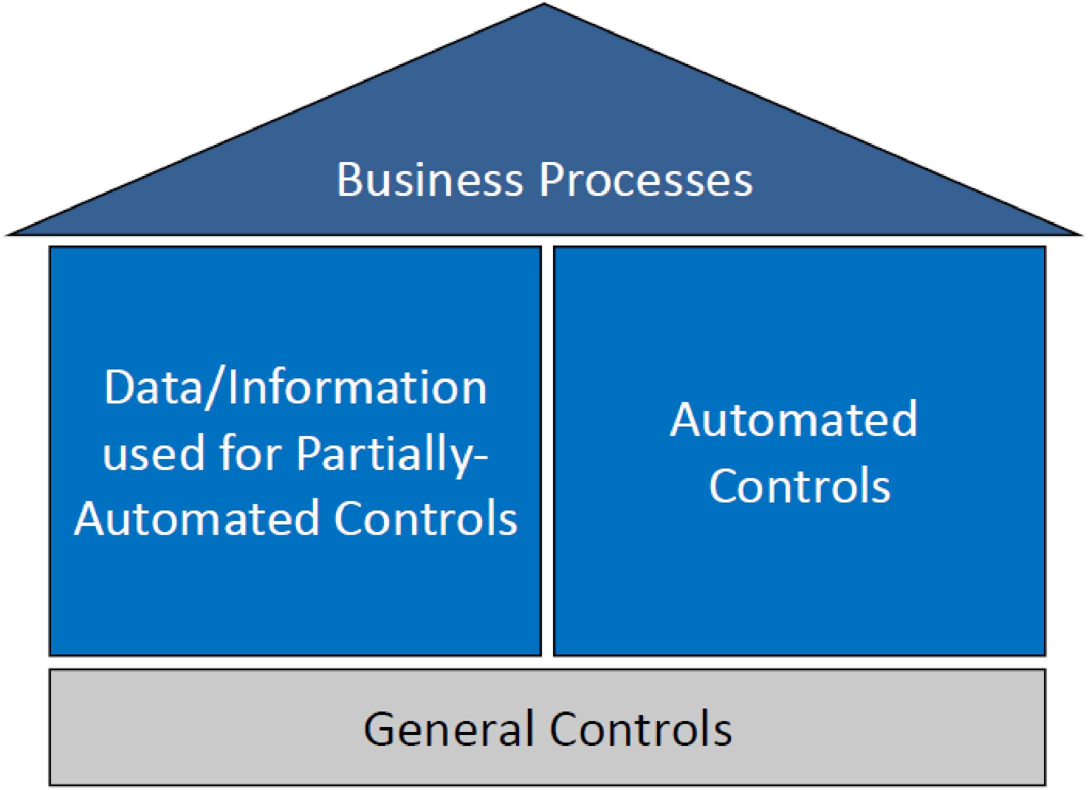
Today’s Lineup

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

Key IT Terms in Banking

- Core System
- E-Banking
- Outsourced vs. In-house (“On Prem”)
- The Cloud
- GLBA 501(b)
  (12 CFR Part 30 / 12 CFR Part 748)
- SOC Report
- Patch Management
- Logical Controls
- MFA – Multi-Factor Authentication
- SDLC – System Development Life Cycle

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 and environmental security controls
- System development life cycle controls

Check This Out – IIA IT General Controls

IT Control Reviews

- FFIEC IT Examination Handbook
- Regulatory Guidance
- 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

Test Your Knowledge

Which of the following would be the best password to use?

a) Password;-)

b) allmyexsliveintexas

c) asdfghjkl

d) $n00pD0ggyd0G

Cybersecurity Incidents

According to the Verizon 2020 Data Breach Investigation Report, in 2019 Financial Services industry was ranked 5th in reported incidents (1,509 – 62% increase) and 1st in confirmed breaches/data disclosure (448 – 116% increase).

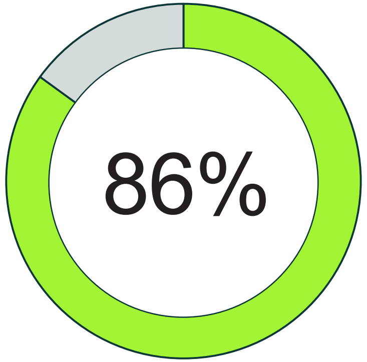
- Web application attacks were the most used attack pattern (over 30%)
- 77% of disclosures involved personal financial data
- 91% of attacks were financially motivated

State of Cybersecurity Today

It's no longer a question of whether a network will be compromised, but when a network will be compromised.

COMPANIES
that experienced at least one cybersecurity incident.

Source: 2017/18 Kroll Annual Global Fraud and Risk Report



$7.91 million

Cost of the average data breach to a U.S. company – up from $5M in 2015

Source: Ponemon Institute's 2018 Cost of a Data Breach Study

5 billion

Total number of records breached

Source: 2018 Year End Data Breach QuickView Report by Risk Based Security

$3.86 million

Average world-wide cost a company pays for a data breach

Source: Ponemon Institute's 2018 Cost of a Data Breach Study

$6 trillion

Estimated cost of cyber crime by 2021. *More profitable than the trade of illegal drugs.*

Source: Cybersecurity Ventures 2017 Official Cybercrime Report

Cybersecurity and Internal Audit

It’s time to game plan…

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

Cybersecurity Assessment

FFIEC Cybersecurity Assessment Tool and NCUA ACET

- 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.

Cybersecurity Assessment Tool

Domain 1: Cyber Risk Management and Oversight

- Risk Management – Evolving **Audit** Controls
  - The independent audit function validates that the **risk management function** is commensurate with the institution’s risk and complexity.
  - The independent audit function validates that the institution’s **threat information sharing** is commensurate with the institution’s risk and complexity.
  - The independent audit function validates that the institution’s **cybersecurity controls function** is commensurate with the institution’s risk and complexity.
  - The independent audit function validates that the institution’s **third-party relationship management** is commensurate with the institution’s risk and complexity.
  - The independent audit function validates that the institution’s **incident response program and resilience** are commensurate with the institution’s risk and complexity.

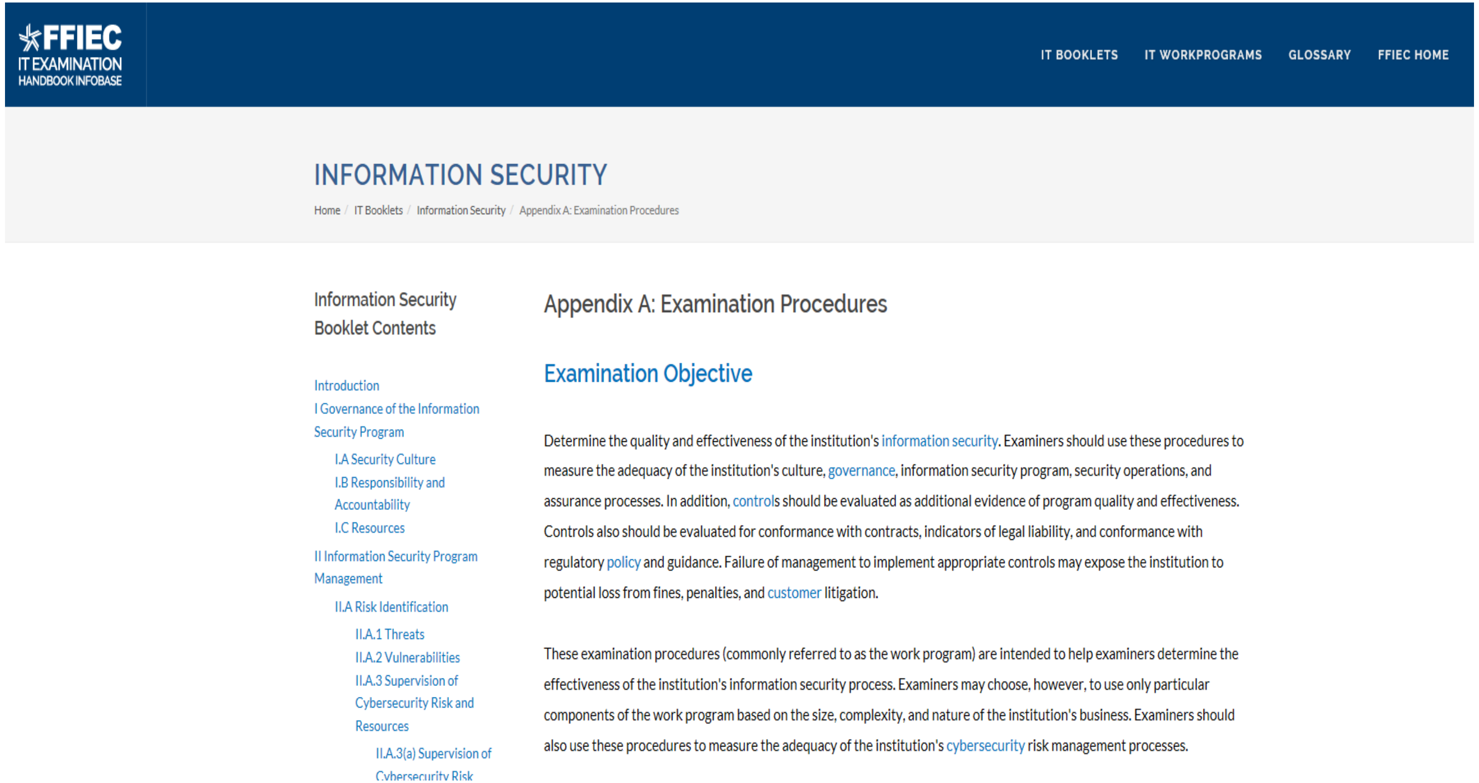
Information Security

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.

Test Your Knowledge

If your tablet or smartphone is lost or stolen, which of the following precautions would NOT be an effective way to restrict access to your device and the data on it?

a) Use a password/passcode or biometrics to restrict access.

b) Enable an "auto lock" feature that secures the device when it is left unused for a certain number of minutes.

c) Add a GPS tracking system for locating your mobile device.

d) Install an app that enables you to remotely wipe data from the device.

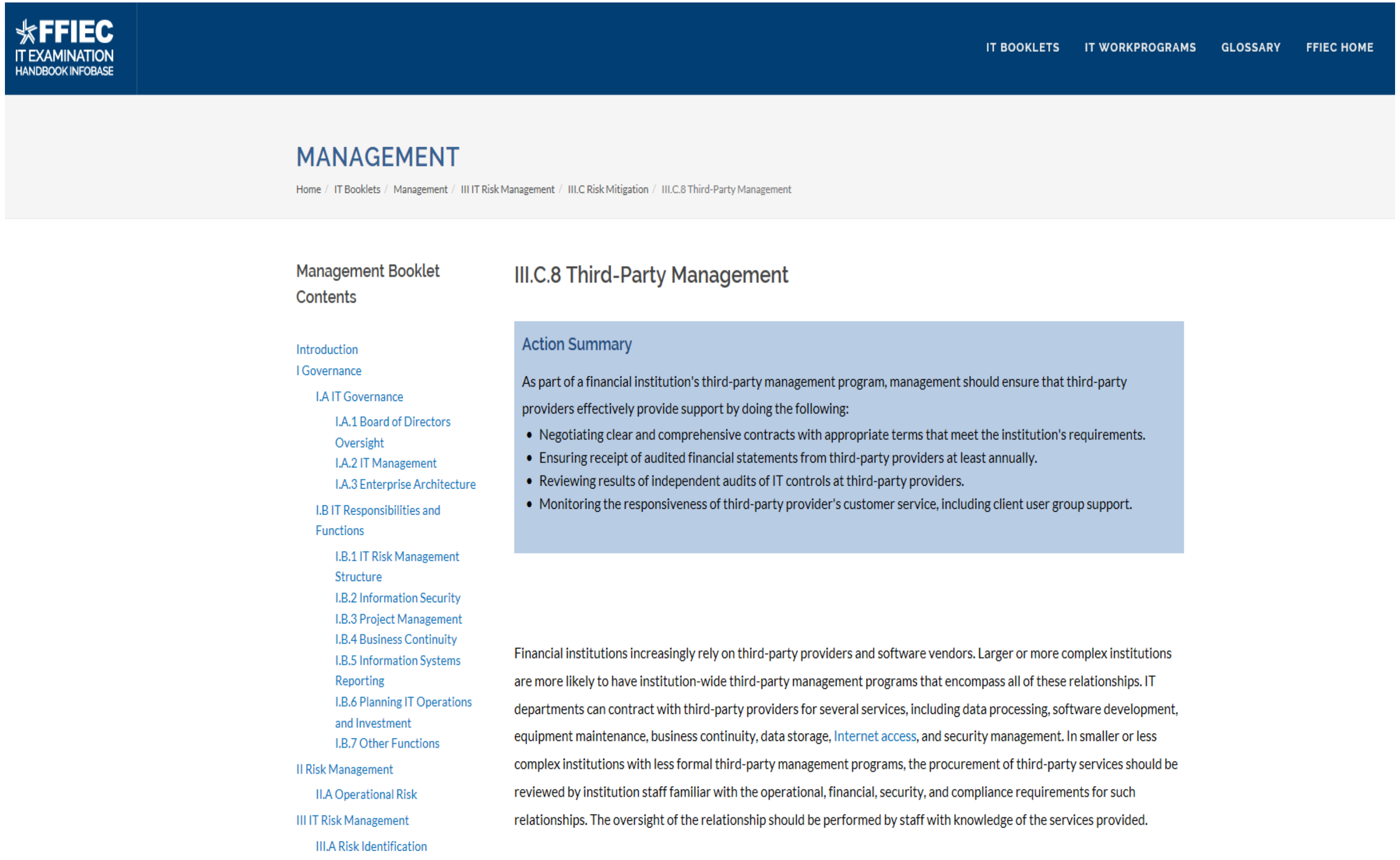
Vendor Management

- 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 SOC 1 / SOC 2 reports, including User Control Considerations
  - Review of financial statements
  - Review of service 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.

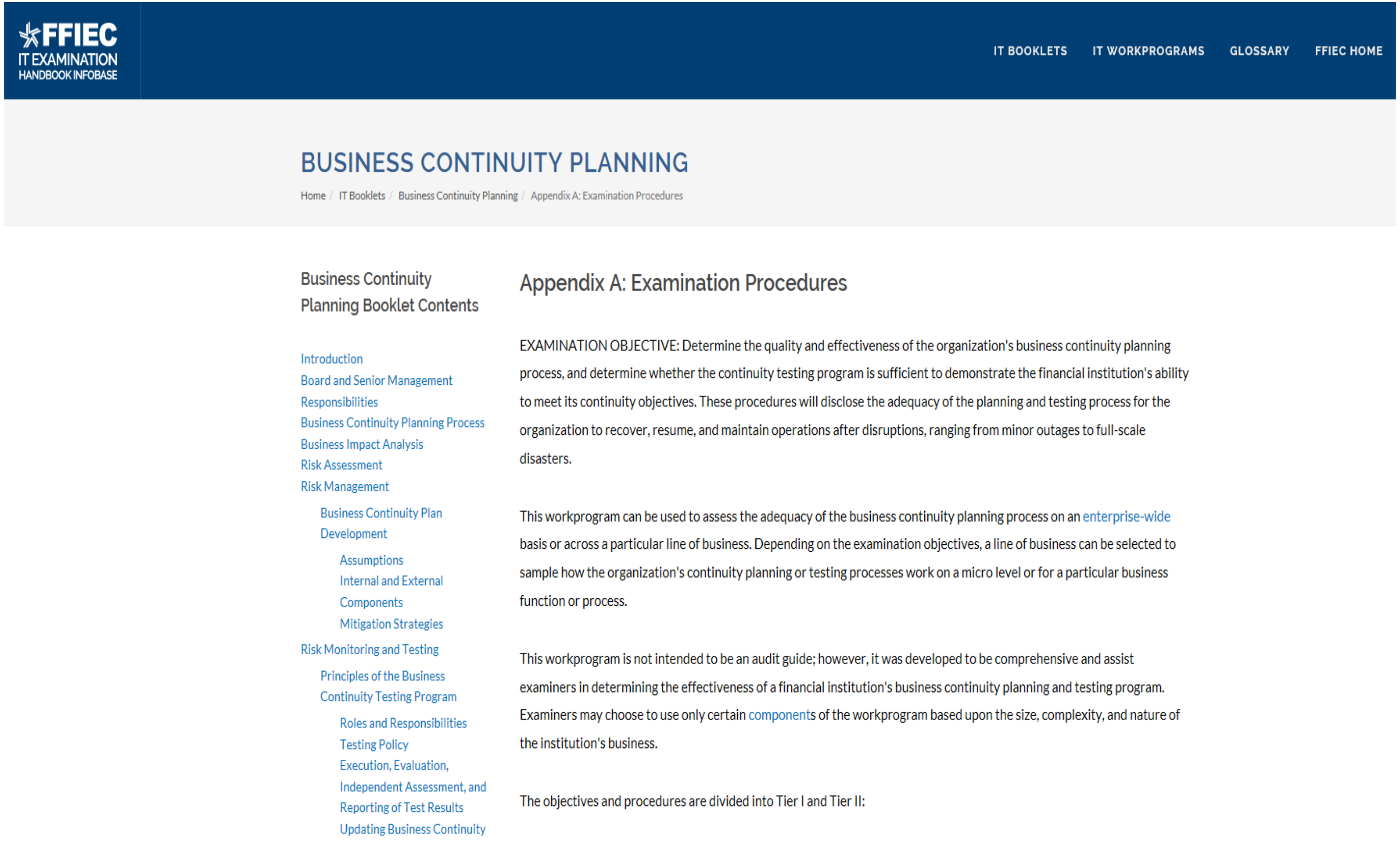
Disaster Recovery and Business Continuity Planning

- 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



BUSINESS CONTINUITY PLANNING

Home / IT Booklets / Business Continuity Planning / Appendix A: Examination Procedures

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 Advisory
chris.wetzel@mossadams.com

THANK YOU

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.