TRAINA & ASSOCIATES

MVP managed vendor program

IT EXAMS

LOUISIANA BANKERS ASSOCIATION
TECHNOLOGY CONFERENCE 2015

@TrainaCPA

TOP 5 CITATIONS

Top 5 citations

1. Policy and Risk Assessment
2. ACH/CATO
3. Disaster planning
4. Audit
5. Oversight

1. POLICY AND RISK ASSESSMENT

- Risk assessments - internet banking, technology, application, new products, etc.
- Incident response plans
- Strategic planning

ISSUES

- Policies contain inaccurate and outdated information
- Lack of presentation to Board
- Training and testing for employees

2. ACH/CATO

- OFI & FDIC
- Managing risks
  - Layered controls
  - Out of bank authentication
  - Customer Review
- Response planning

AUTHENTICATION

- Security questions
- Out-of-band authentication

TRAINA & ASSOCIATES

MVP

OUT-OF-BAND AUTHENTICATION

- Delivery channels may not be different
  - Mobile, email, phone call, fax, etc.
- Dual control
- Customer education is key

TRAINA & ASSOCIATES

MVP

REVIEW OF ORIGINATORS

- Should be done annually
- Credit review
- System vs. documentation
- Board presentation

TRAINA & ASSOCIATES

MVP

TRAINING IS KEY!

- Education
  - Corporate customers and employees
  - Cannot be performed often enough
  - Atmosphere is changing almost daily
  - How are new employees educated?

TRAINA & ASSOCIATES

MVP

RESPONSE PLANNING

- CATO specific incident response plan
- Implementing respond recommendations
  - How is suspected fraud verified?
  - How are customer concerns/calls dealt with?
  - What are procedures for recovery?

TRAINA & ASSOCIATES

MVP

COMMON SHORTCOMINGS

- Address all recommendations
  - Missing specific products or updates
  - Response procedures

TRAINA & ASSOCIATES

MVP

WHAT BANKS ARE DOING RIGHT

- Most banks have good layered controls in place
- Risk assessments have been implemented and approved by BOD
- Better information provided through literature and online

TRAINA & ASSOCIATES

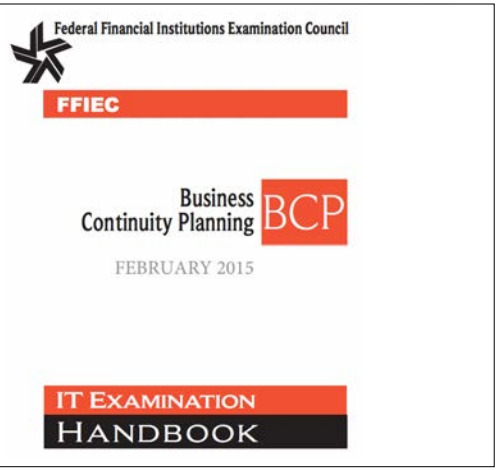
MVP

3. DISASTER PLANNING

- DR testing was the biggest focus last 12 months
- Appendix J emphasis expected in next 12 months

TRAINA & ASSOCIATES

MVP



APPENDIX J - COMPONENTS

Management

Capacity

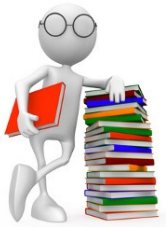
Testing

Cyber Resilience

HOW TO PREPARE FOR APPENDIX J

- Know your TSP's plans
- Participate in TSP testing
- Tabletop exercises
- Update your plans
- Address in vendor review

4. AUDIT



- Tracking and resolution
- Audit schedule
- Vulnerability assessments, patch reports, etc.
- Report to committee or Board

5. OVERSIGHT

- Management succession plans
- Separation of Information Security Officer from IT
- IT Committee
- Board of Directors

TRAINA & ASSOCIATES

MVP managed vendor program

CYBERSECURITY ASSESSMENTS

TRAINA & ASSOCIATES

MVP managed vendor program

Addressing the Need

- Banks have been effective with their own security, but have sustained losses as a result of issues with third parties
- Banks are increasingly recognizing that sharing information about IT issues is essential to protect themselves

TRAINA & ASSOCIATES

MVP managed vendor program

Cybersecurity Assessment

- Proactive approach to security and reporting
- Logging all significant cyber events that affect the FI
  - Ongoing reference document for future events

FFIEC Cybersecurity Assessment Tool

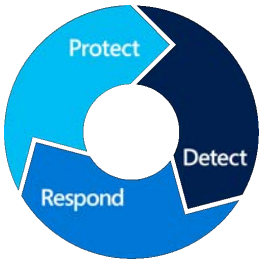
Objective

To help institutions identify their risks and determine their cybersecurity maturity.

The Assessment provides institutions with a repeatable and measureable process to inform management of their institution's risks and cybersecurity preparedness.

Cybersecurity Assessment

- Updated approach to existing framework
  - Identify
  - Protect, Detect, Respond
  - Recover



FFIEC Cybersecurity Priorities

- Cybersecurity Assessment Tool
- Incident Analysis
- Crisis Management
- Training
- Policy Development
- TSP Strategy
- Law Enforcement Collaboration

TRAINA & ASSOCIATES

MVP

FFIEC Cybersecurity Assessment Tool

Consistent with the principles in

- *FFIEC Information Technology Examination Handbook (IT Handbook)*
- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Industry accepted cybersecurity practices

FFIEC Cybersecurity Assessment Tool

Consists of two parts

Part One: Inherent Risk Profile

Part Two: Cybersecurity Maturity

FFIEC Cybersecurity Assessment Tool

Inherent Risk Profile Excerpt

Activity, Service or Product

Risk Levels

Category: Technologies and Connection Types	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Total number of internet service provider (ISP) connections (including branch connections)	No connections	Minimal complexity (1–20 connections)	Moderate complexity (21–100 connections)	Significant complexity (101–200 connections)	Substantial complexity (>200 connections)
Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)	None	Few instances of unsecured connections (1–5)	Several instances of unsecured connections (6–10)	Significant instances of unsecured connections (11–25)	Substantial instances of unsecured connections (>25)

FFIEC Cybersecurity Assessment Tool

Cybersecurity Maturity

- Cyber Risk Management and Oversight
- Threat Intelligence and Collaboration
- Cybersecurity Controls
- External Dependency Management
- Cyber Incident Management and Response

FFIEC Cybersecurity Assessment Tool

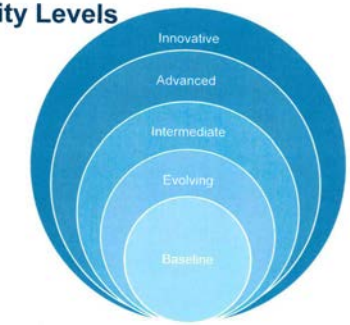
Cybersecurity Maturity

- Domains
  - Assessment Factors
    - Components
      - Declarative Statements

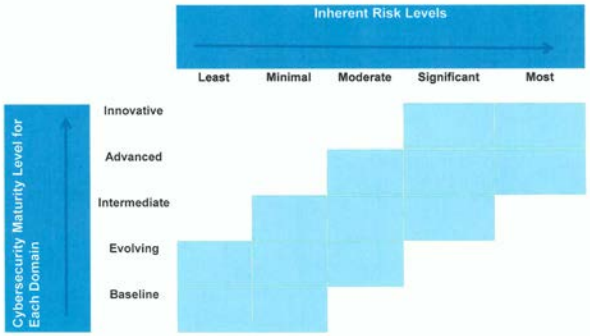
(495 Statements)

FFIEC Cybersecurity Assessment Tool

Maturity Levels



FFIEC Cybersecurity Assessment Tool



CYBER SECURITY & INCIDENT RESPONSE

Incident Response

- Response and recovery are becoming much more important to regulators
- Incident Response <—> Disaster Recovery
- The issue should be addressed in both plans

Cyber Attacks & Incident Response

- Risk Assessments should identify vulnerabilities and guide strategies
- Detection and recovery procedures needed, including customer notification when applicable
- Should be included in disaster recovery testing

Cyber Attacks & Incident Response

- **Examiners expect familiarity & planning for both incidents and zero-day vulnerabilities**
- How are you addressing the issues?

THIRD PARTY RISK MANAGEMENT

TRAINA & ASSOCIATES

MVP managed vendor program

DO YOU HAVE A VENDOR RISK ASSESSMENT?

TRAINA & ASSOCIATES

MVP managed vendor program

Common Shortcomings

- No review is performed, or review is incomplete
- No follow-up for missing documentation or review of received documents
- Information is reviewed, but not by appropriate parties
- No recommendation for evaluation of the relationship

TRAINA & ASSOCIATES

MVP managed vendor program

Common Shortcomings

- Certain vendors not designated as significant so no review is done
  - Website host vendor
  - Online backup host vendor
- New vendor notification not provided to FDIC

TRAINA & ASSOCIATES

MVP

Common Shortcomings

- Some areas not addressed in reviews
  - Incident response planning
  - Vulnerability scanning
  - Complementary controls

TRAINA & ASSOCIATES

MVP

DOES THE VENDOR REVIEW ITS VENDORS?

TRAINA & ASSOCIATES

MVP

Cloud Vendors

- Normal vendor due diligence process should be completed AND additional considerations apply
- FFIEC - July 2012 - Outsourced Cloud Computing

Cloud Vendors

- Contracts should address:
  - Encryption of data transmitted
  - Storage of data
  - Defining if FI data shares commingles with other data
  - Adequate disaster recovery plan of provider

Outsourcing Vendor Review

- Provider can supply necessary information to make an informed decision
- Decision to keep the vendor is up to the FI

LAST MINUTE TIPS

TRAINA & ASSOCIATES

MVP managed vendor program

LAST MINUTE TIPS

- Make sure you have provided all requested info
- Are policies updated?
- Check status of audit items
- What is status of annual requirements?
  - ISP report to Board
  - IS and DR training

TRAINA & ASSOCIATES

MVP managed vendor program

COMING SOON

TRAINA & ASSOCIATES

MVP managed vendor program

EMV

TRAINA & ASSOCIATES

MVP managed vendor program

TRAINA & ASSOCIATES

TRAINA & ASSOCIATES

MVP managed vendor program

QUESTIONS

@TrainaCPA