



# Information Technology

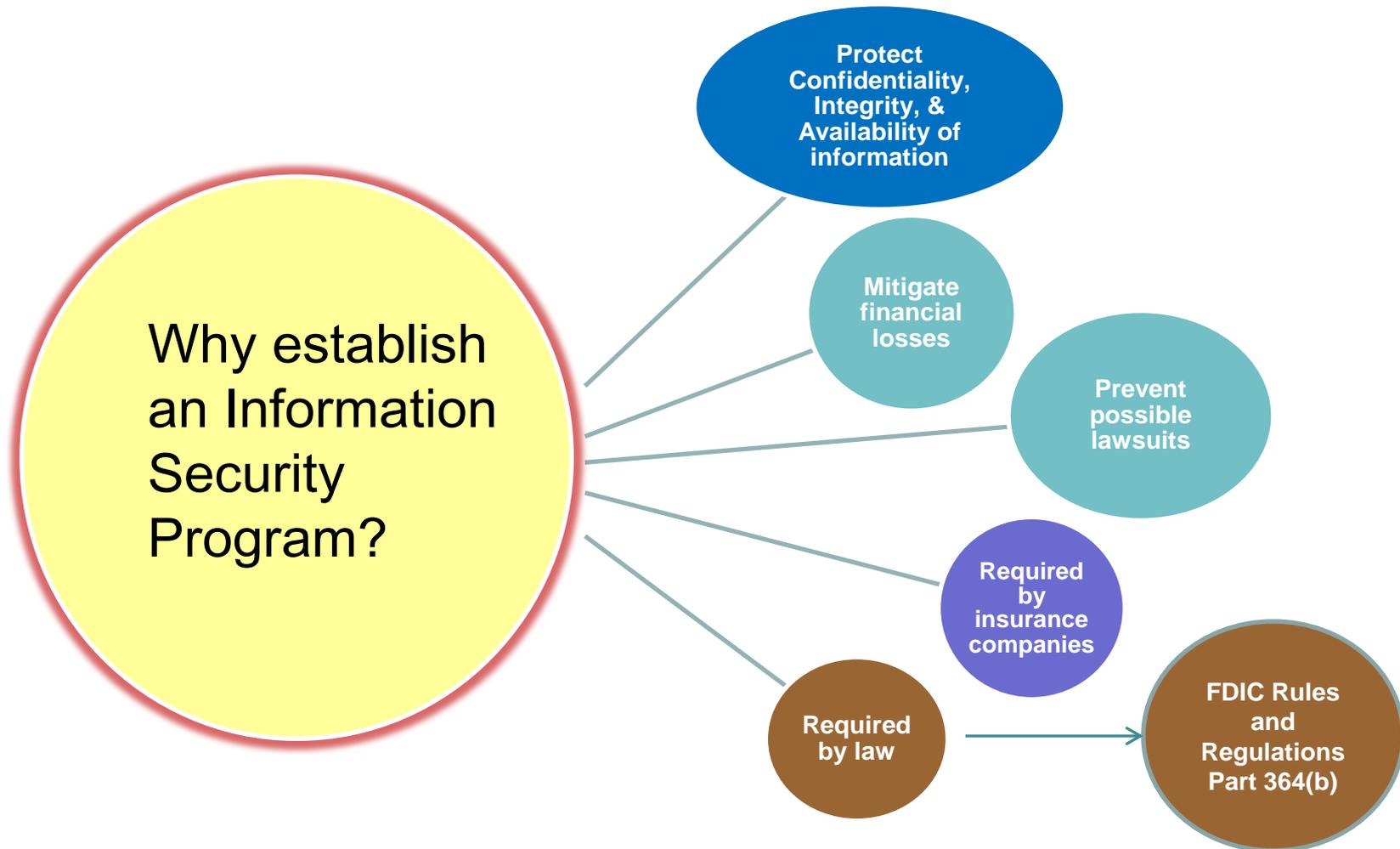
---

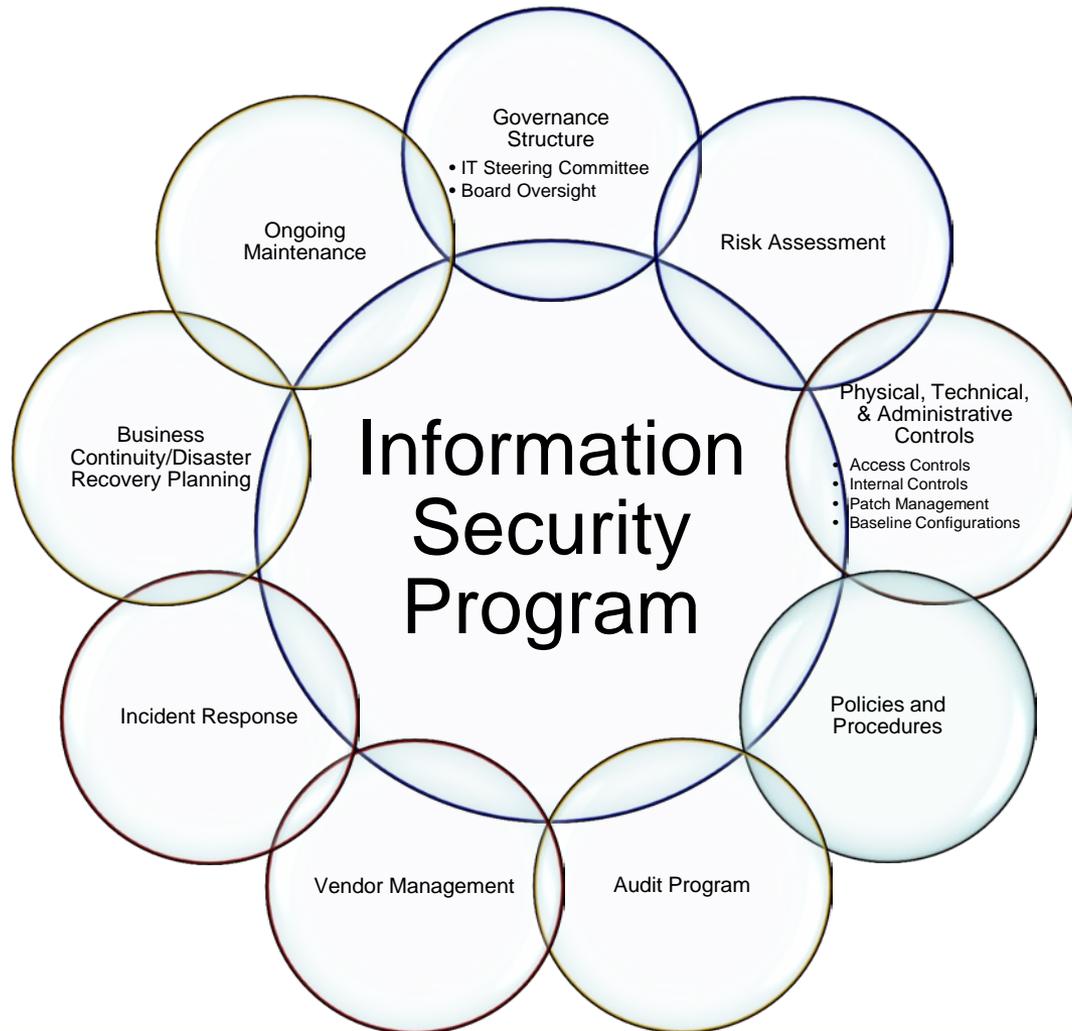
**A Current Perspective on Risk  
Management**



# Topics Covered

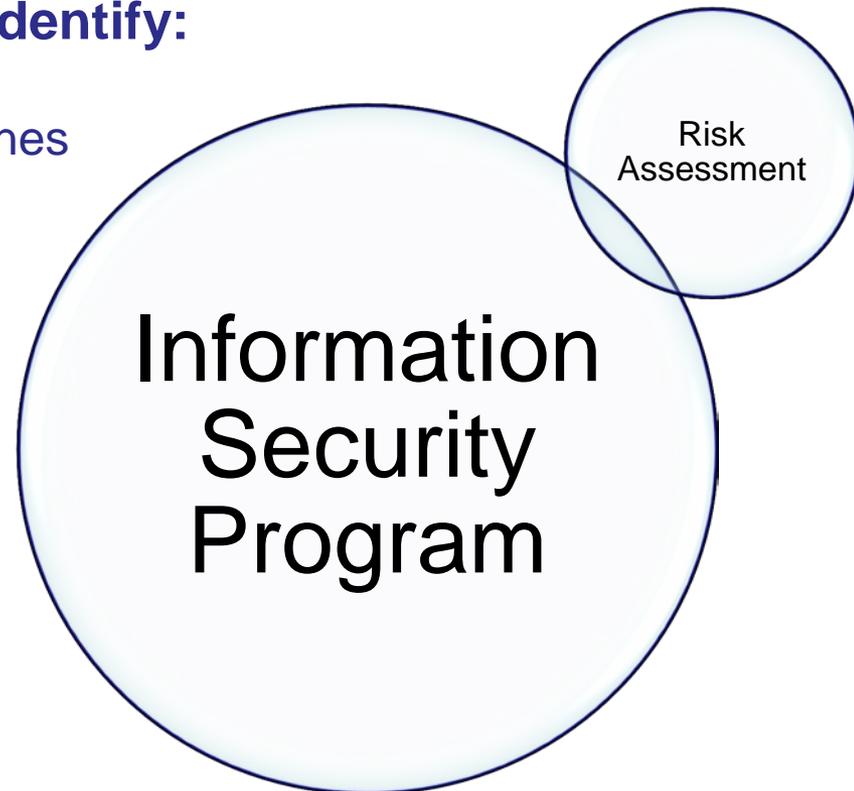
- **Information Security Program**
- **Common Examination Findings**
- **Existing and Emerging Risks**
  - ◆ ACH/Wire Fraud and Corporate Account Takeover
  - ◆ Distributed Denial of Service Attacks (DDoS)
  - ◆ Cloud/Hosting
  - ◆ Third-Party Payment Processing
- **Questions**





## Use the Risk Assessment to identify:

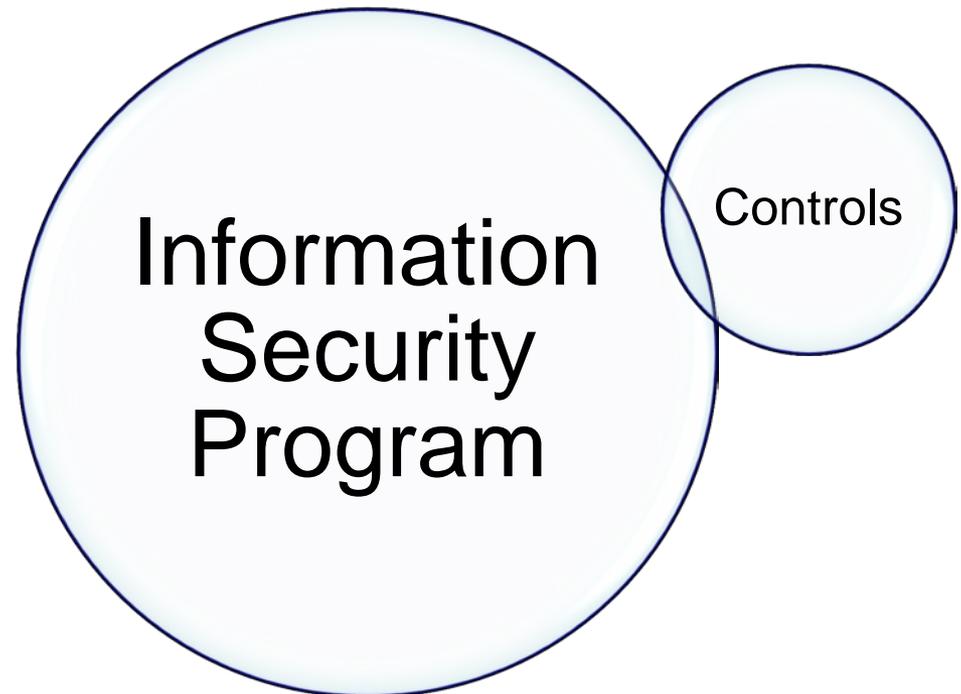
- Bank functionality and product lines
- IT systems and devices
- Data locations and uses
- Threats, risks, and controls



## Types of Controls:

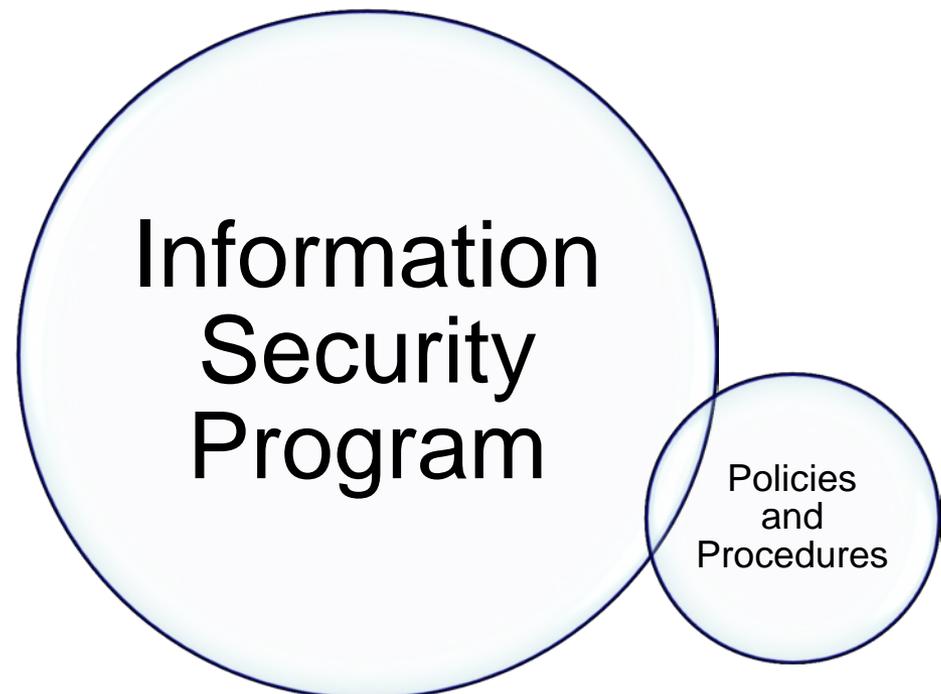
- Administrative
  - Policies
  - Procedures
- Physical
  - Secure areas
- Technical
  - System configurations
  - Patch management
  - Access rights

The control environment must continue to evolve with threats and risk.



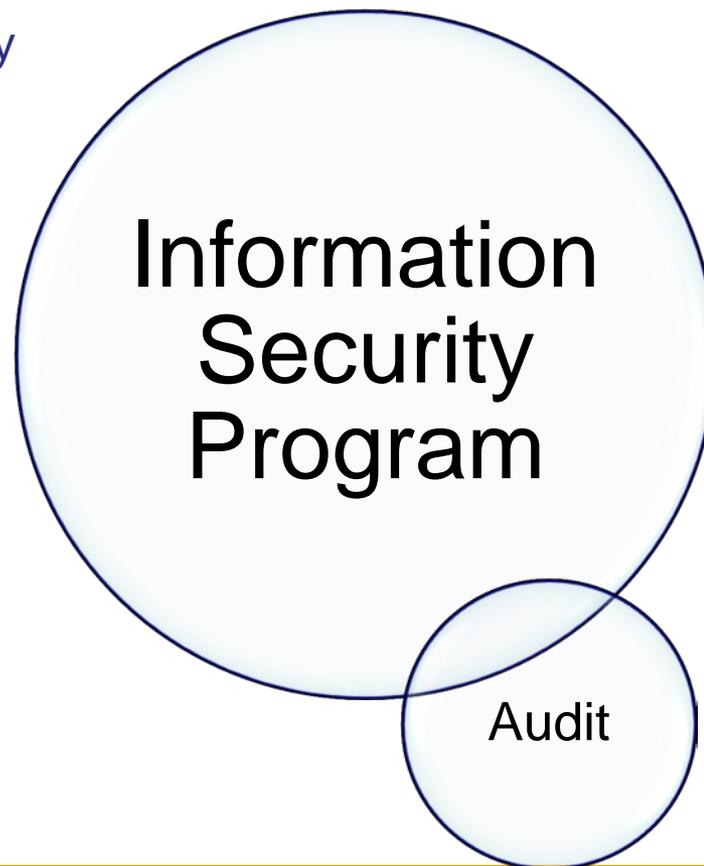
## Policies and Procedures:

- Set forth the standards for operations and performance
- Support consistency of operations
- Serve as the baseline for the audit program



## Audit

- Validates the information security program and control structure
- Consists of independent internal and external reviews
  - General controls audits
  - Vulnerability assessments
  - Penetration tests
- Driven by the risk assessment





# Information Security Program

## Vendor and Service Provider Oversight

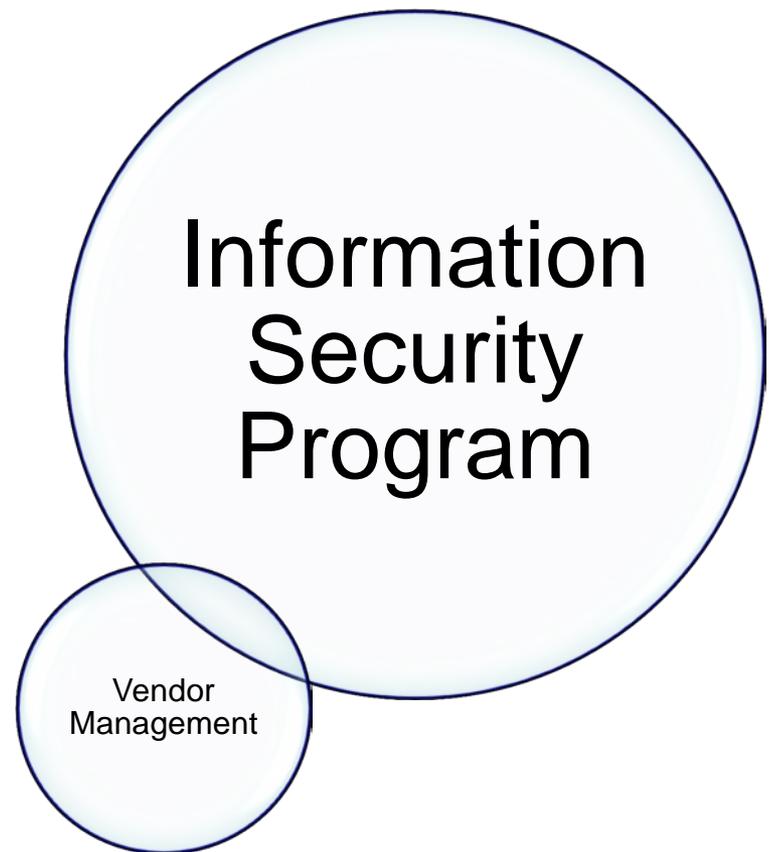
- Financial well-being
- Control structure
- Performance

## Technology Service Providers

- Regulatory Examinations
- Reports are available to serviced banks

## Report Requests:

- Name of provider/data center
- Types of services (e.g, core, Internet Banking, payment processing, etc.)
- Fax to: 816-234-8182

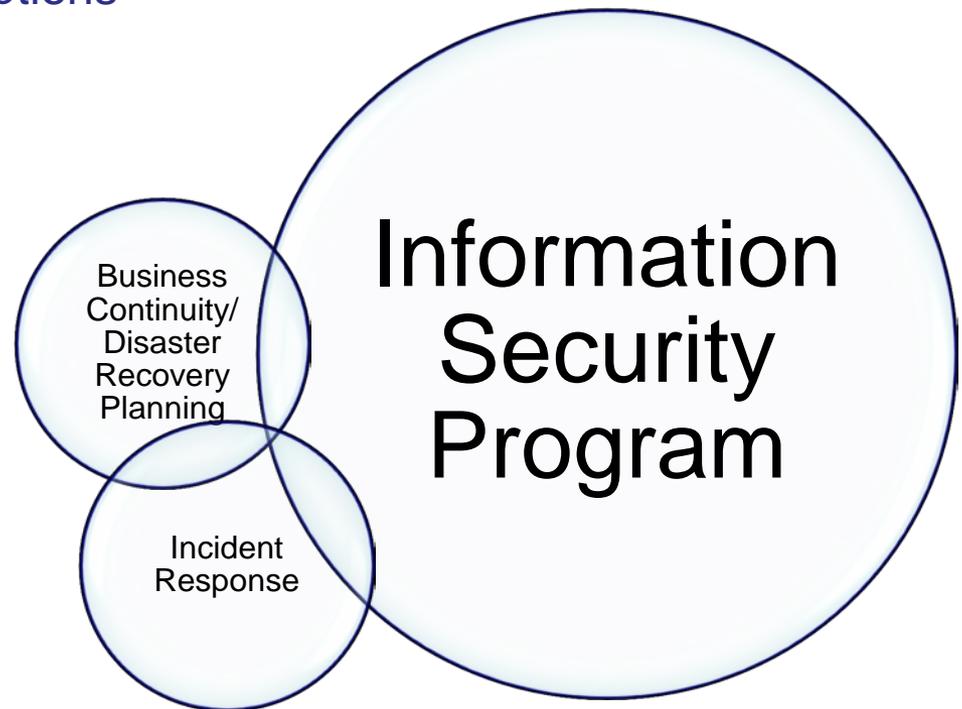


## Business Continuity/Disaster Recovery

- Plan for short and long term disruptions

## Incident Response

- Determine what happened
- Control and respond
- File a SAR if necessary
- Provide customer notice if misuse of data is possible or takes place
- Notify the FDIC
  - Debit/Credit card exception



FIL-27-2005 “Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice”





## Risk Assessment

- **Underutilized**
- **Use as a proactive risk identification process**
  - ◆ New technologies
  - ◆ New business lines
  - ◆ New risks
- **Drives control structure**



## Patch Management

- **Core and networked systems**
  - ◆ Servers, workstations, firewalls, routers, etc.
- **Microsoft and non-Microsoft systems**
  - ◆ Adobe, Java, QuickTime, Firefox, Oracle, etc.
- **Firmware updates**
- **Outsourcing arrangements**



# Common Examination Findings

## **\*\*\*Windows XP support ends April 8, 2014\*\*\***

- **Migrate to a supported operating system**
- **Implement risk mitigation strategies**
  - ◆ Increased monitoring
  - ◆ System isolation/protection from threat sources
- **Ensure senior management and Board awareness**

FFIEC Joint Statement on End of Support for Windows XP Operating System

<http://ithandbook.ffiec.gov/reference-materials.aspx>

Federal Reserve Board Article: Risk Related to End of Support for Microsoft Windows XP

<http://www.communitybankingconnections.org/articles/2013/Q4/Community-Bank-Operations.cfm>



## Configuration Standards

- **Capture servers, workstations, and network devices**
- **Develop baseline standards**
  - ◆ Disable unnecessary/risky services
  - ◆ Expand configuration from baseline as needed
- **Apply standards to new equipment**



## **Business Continuity/Disaster Recovery Planning**

- **Assess all business critical systems, operations, and product lines**
- **Look beyond core and include network-based installations**
- **Broaden planning and testing strategies as needed**

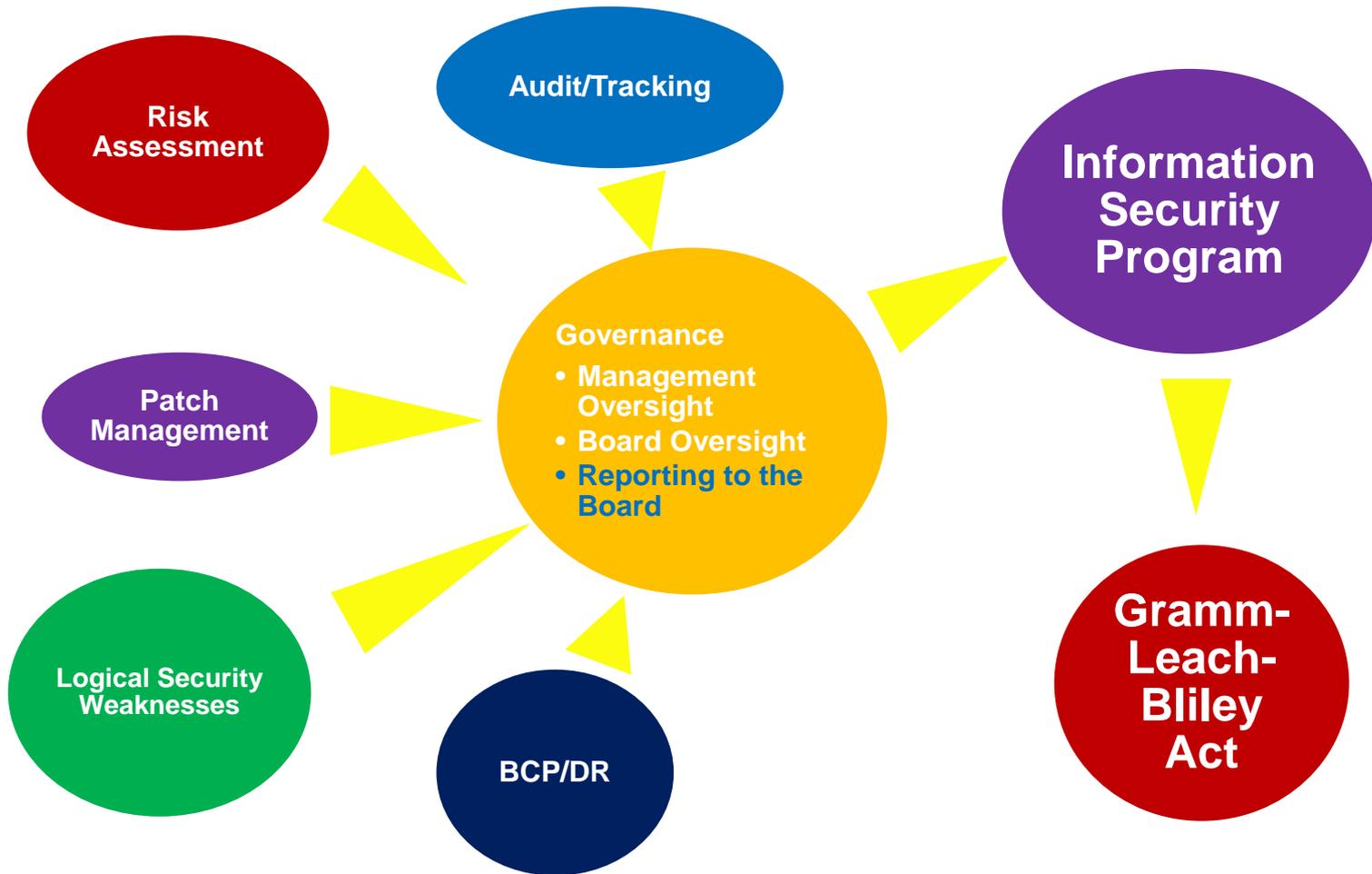


# Common Examination Findings

## Audit

General Controls Reviews  
Vulnerability Assessments  
Penetration Tests

- **Conduct at regular and appropriate intervals**
- **Establish scope based upon the risk assessment**
- **Formally track findings through to resolution and provide status reports to senior management and the Board**
  
- **Ensure the vulnerability assessment scope is appropriate and captures all necessary systems**
  - ◆ Maintain a current network topology





# Existing and Emerging Risks

## ACH/Wire Fraud & Corporate Account Takeover

- **Social Engineering and Identity Theft**
  - ◆ E-mail request for funds transfer
  - ◆ Unwilling to communicate by voice
  - ◆ May have limited account/personal information, though may seek to validate/obtain information
  - ◆ Potential for call-back numbers to be hijacked
  - ◆ Subsequent requests will follow if successful



# Existing and Emerging Risks

## ACH/Wire Fraud & Corporate Account Takeover

- **Corporate Account Takeover**
  - ◆ Malware infects customer's computer
  - ◆ Used to initiate fraudulent ACH or wire transfer through bank's cash management system
  - ◆ Controls and security awareness programs are essential
- **Governing Legislation**
  - ◆ Electronic Funds Transfer Act of 1978
  - ◆ UCC 4a - "commercially reasonable"
- **FIL-50-2011 "Supplement to *Authentication in an Internet Banking Environment*"**



# Existing and Emerging Risks

## ACH/Wire Fraud & Corporate Account Takeover

- **FIL-50-2011 “Supplement to *Authentication in an Internet Banking Environment*”**
  - ◆ Requires annual risk assessments
  - ◆ Directs that controls must exceed device ID and challenge questions
    - Controls must be stronger for commercial accounts, with multi-factor authentication recommended
  - ◆ Requires layered security for all accounts, including anomaly detection and response
  - ◆ States that User IDs and passwords alone are insufficient for customer-level system administrators
  - ◆ Mandates customer awareness and education



# Existing and Emerging Risks

## ACH/Wire Fraud & Corporate Account Takeover

- **Corporate Account Takeover – Actions**
  - ◆ Disable Internet banking/cash management access
  - ◆ Change all account numbers and credentials
  - ◆ Complete customer-level forensic analysis and vulnerability assessment
  - ◆ Implement customer-level patch and virus management programs
  - ◆ Isolate customer's funds management workstation
  - ◆ Offer strong authentication



# Existing and Emerging Risks

## ACH/Wire Fraud & Corporate Account Takeover

- **Funds Transfer Activity – Traditional Controls**
  - ◆ Contractual requirements/responsibilities
  - ◆ Authorizations for funds transfer requests
  - ◆ Validation procedures
  - ◆ Dual controls
  - ◆ Audits
  - ◆ Security awareness training
  - ◆ Authorization limits
  - ◆ Waivers



# Existing and Emerging Risks

## Distributed Denial of Service (DDoS)

- **Renders Internet-based services unavailable**
  - ◆ Be aware of pathways to internal systems
  
- **Assess nature and criticality of internet-based services**
  - ◆ Understand what's at risk
  - ◆ Develop incident response and business continuity plans
  - ◆ Identify points-of-contact
  - ◆ Do you have viable alternatives?
  - ◆ How will you communicate with customers?
  - ◆ Blocking sources of attack can be difficult
  
- **Notify local FBI and FDIC Field Offices**



# Existing and Emerging Risks Cloud/Hosting

- **What is Cloud?**
- **Benefits**
  - ◆ Cost reduction, flexibility, scalability, speed
- **Risks/Concerns/Questions**
  - ◆ Type of Cloud?
  - ◆ Who has access to the data?
  - ◆ Where is the data?
  - ◆ Is the data backed-up?
  - ◆ What is the third-party's control structure?
  - ◆ Can you perform effective/on-going due-diligence?
  - ◆ How difficult is it to disengage?

## **FFIEC Cloud Computing Statement**

<http://ithandbook.ffiec.gov/reference-materials.aspx>



# Existing and Emerging Risks

## Third-Party Payment Processing

- **Account relationships with entities that process payments for other businesses**
- **Can create risk in several areas**
  - ◆ Credit, legal, and compliance risks
  - ◆ Potential for BSA/AML risks
- **The bank bears the risk as the “Originating Depository Financial Institution”**



## ***www.fdic.gov***

- FIL 12-99: Uniform Rating System for Information Technology
- FIL 22-2001: Security Standards for Customer Information
- FIL 68-2001: 501(b) Examination Guidance and Procedures
- FIL 27-2005: Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
- FIL 81-2005: IT Risk Management Program
- FIL 44-2008: Guidance for Managing Third Party Risk
- FIL 3-2012: Payment Processor Relationships
- FIL 100-2007: Identity Theft Red Flags
- FIL 103-2005 and FIL 50-2011: Authentication in an Internet Banking Environment



# Resources

***<http://ithandbook.ffiec.gov>***

- FFIEC IT Handbooks

***<http://ithandbook.ffiec.gov/reference-materials.aspx>***

- FFIEC Cloud Computing Statement
- FFIEC Joint Statement on End of Support for Windows XP Operating System

***[www.fdic.gov/regulations/resources/director/video.html](http://www.fdic.gov/regulations/resources/director/video.html)***

- Directors' Resource Center Technical Assistance Video Program

***[www.communitybankingconnections.org/articles/2013/Q4/Community-Bank-Operations.cfm](http://www.communitybankingconnections.org/articles/2013/Q4/Community-Bank-Operations.cfm)***

- Federal Reserve Board Article: Risk Related to End of Support for Microsoft Windows XP



# FDIC IT Contacts

**Dave Sanders**

dsanders@fdic.gov

816-234-8527

IT Supervisor

**A.J. Steiger**

asteiger@fdic.gov

816-234-8521

IT Exam Specialist

**Report Request Fax Number**

816-234-8182

**Your respective Field Supervisor or Case Manager**

**Questions?**