THE MARKET LEADER IN IT, SECURITY AND COMPLIANCE SERVICES FOR COMMUNITY FINANCIAL INSTITUTIONS

"The Emergence of the ISO in Community Banking"

Patrick H. Whelan – CISA

IT Security & Compliance Consultant

KONICA MINOLTA

MSPmentor 501

2014 Edition

Agenda

- **Brief Introduction to All Covered Finance**
- Regulatory Guidelines
- Current challenges
- Role of the Information Security Officer (ISO)
- Hybrid Concept
- Q&A

Patrick H. Whelan - CISA

- Strategic consultant focused on security, compliance, and infrastructure planning for community financial institutions.

- Provides financial institutions with strategic direction to align their IT infrastructure, processes, and capital outlay with the institution's vision.

- Prior to All Covered, a team member of Silversky, the market leader of enterprise-class information security and messaging services under direct FFIEC oversight.

- Prior to Silversky, Patrick designed physical security controls with ADT Fire & Security, a Tyco company.

- Degrees from Quinnipiac University and an active member of ISACA.

Company Overview

- 30+ years the leading provider for IT, Security, Compliance and Infrastructure Services
- Over 500 System Engineers across 24 Regional Office locations
- Hundreds of Financial Institutions Clients
- Finance Practice Remote Support Center
  - Application Support
  - General Business Applications
  - Banking Applications
  - NOC
  - Software Upgrades
- IT Compliance Professionals
  - IT Audit Support
  - Consulting Services
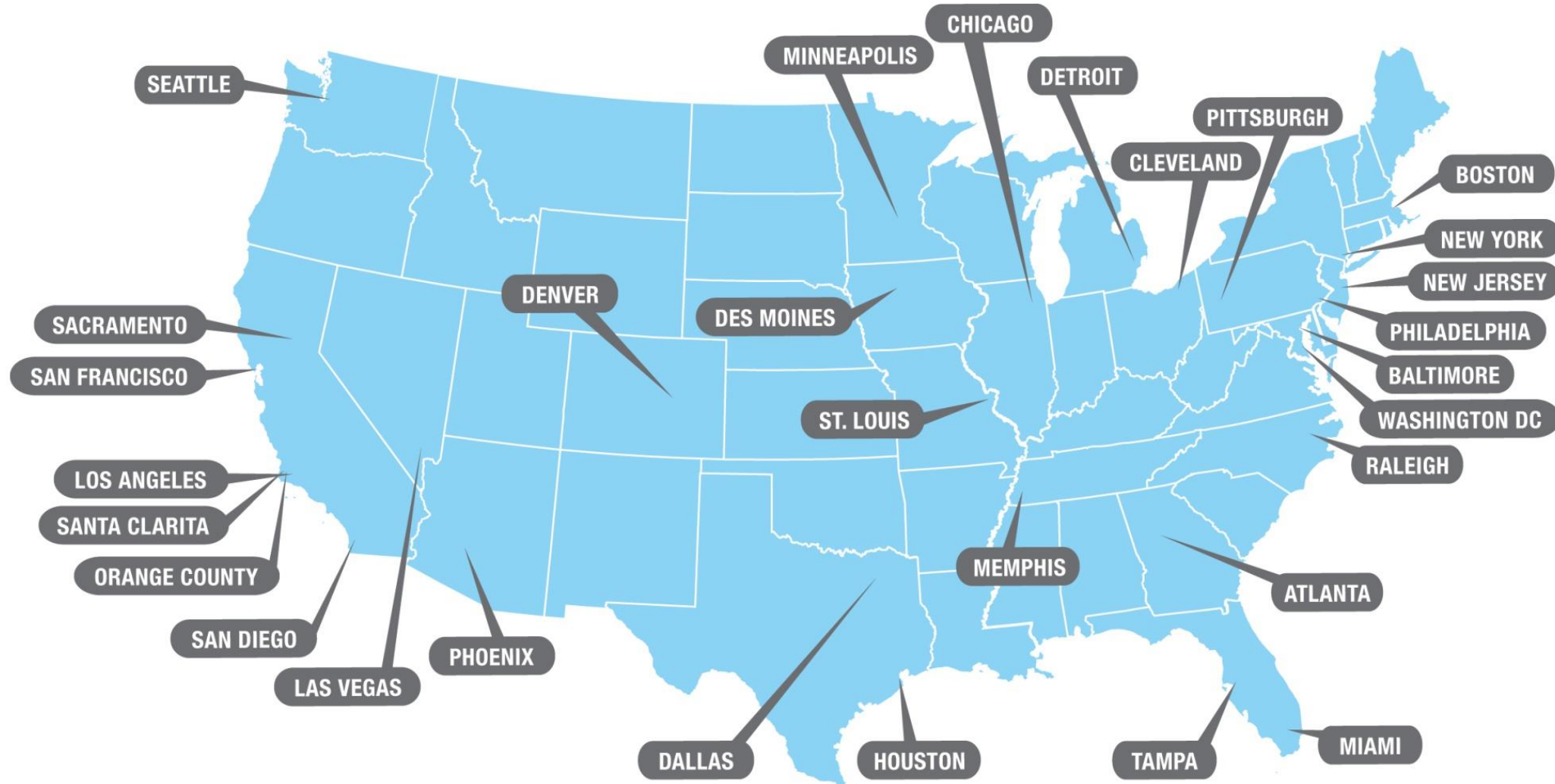
**IT Compliance
and Consulting**

Private Cloud Computing

Security Services

**Network Monitoring
and Management**

**Network Design
and Installation**

Agenda

- Brief Introduction to All Covered Finance
- **Regulatory Guidelines**
- Current challenges
- Role of the Information Security Officer (ISO)
- Hybrid Concept
- Q&A

IT Booklets

Master Table of Contents

- Audit
- Business Continuity Planning
- Development and Acquisition
- E-Banking
- Information Security
- Management
- Operations
- Outsourcing Technology Services
- Retail Payment Systems
- Supervision of Technology Service Providers (TSP)
- Wholesale Payment Systems

www.FFIEC.GOV

A financial institution should ensure an adequate risk management structure exists within the organization. Some institutions **have a separate risk management department that is responsible for overseeing the areas of information security, business continuity planning, audit, insurance and compliance.** Regardless of the particular structure used, the institution should ensure that lines of authority are established for enforcing and monitoring controls. These risk management functions should play a key role in measuring, monitoring, and co

- The board is responsible for overseeing and approving the development, implementation, and maintenance of a comprehensive, written information security program, as required by the Gramm-Leach-Bliley Act (GLBA).
- The board may delegate information security monitoring to an independent audit function and information security management to an independent information security officer.
- Separate information security program management and monitoring from the daily security duties required in IT operations.
  - The ISO should be an **organization-wide risk manager rather than a production resource** devoted to IT operations.
  - To ensure independence, **the ISO should report directly to the board or senior management** rather than through the IT department.

Presidential Executive Order

Presidential Executive Order

Improving Critical Infrastructure Cybersecurity
(February 12, 2013)
Represents the latest in federal policy on cybersecurity

Current Bills in the U.S. Senate

Cyber Intelligence Sharing and Protection Act

To provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities, and for other purposes.

Cybersecurity Information Sharing Act of 2014

To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes

Regulatory Exam Focus

2012
Data Classification
IT Risk Assessment

2013
Business Continuity
Disaster Recovery

2014
Vendor Management
Cybersecurity

Agenda

- Brief Introduction to All Covered Finance
- Regulatory Guidelines
- **Current Challenges**
- Role of the Information Security Officer (ISO)
- Ideals

Challenges in IT Security

- Immergence of cybersecurity threats

- Lack of knowledge at Board and Executive level

- Who has IT oversight capabilities outside of IT?

  - ISO can't function under IT, but needs to coordinate with IT

- Institutions cannot outsource oversight

- Who on staff can we give this title to?

- Average salary for ISO $100K-$150

7 Security Predictions for 2014

1. Making threat intelligence useful
2. Mobile threats
3. Emerging countries will experience more cyber attacks on banks
4. Attacks will spread to smaller institutions
5. New strategies for dealing with insider threats
6. Dealing with challenges created by the NIST framework
7. New needs around data security

from Booz Allen Hamilton

http://www.banktech.com/7-security-predictions-for-2014-from-booz-allen-hamilton/d/d-id/1296729?

Agenda

- Brief Introduction to All Covered Finance
- Regulatory Guidelines
- Current challenges
- Role of the Information Security Officer (ISO)
- Hybrid Concept
- Q&A

A **Information Security Officer** (**ISO**) is the resource within an institution responsible for establishing and maintaining the program to ensure information assets and technologies are adequately protected.

- Responsible and accountable for administration of the security program
- Authority to respond to a security event
- Have sufficient knowledge, background, and training to perform role
- Report to Board or Senior Management
- Independence to perform their assigned tasks

- Information Security Program
- Access Management
- IT Risk Assessment
- IT Risk Mitigation
- IT Audit Oversight
- IT Steering Committee
- Interface with Examiners & Auditors
- Monitoring Security Events
- Business Continuity Planning

- Disaster and Recovery Management
- Vendor Management
- Vulnerability Assessments
- Incident Response
- Board of Director Reporting
- Physical Security Management
- Information Security Awareness Training

IT Risk Assessment
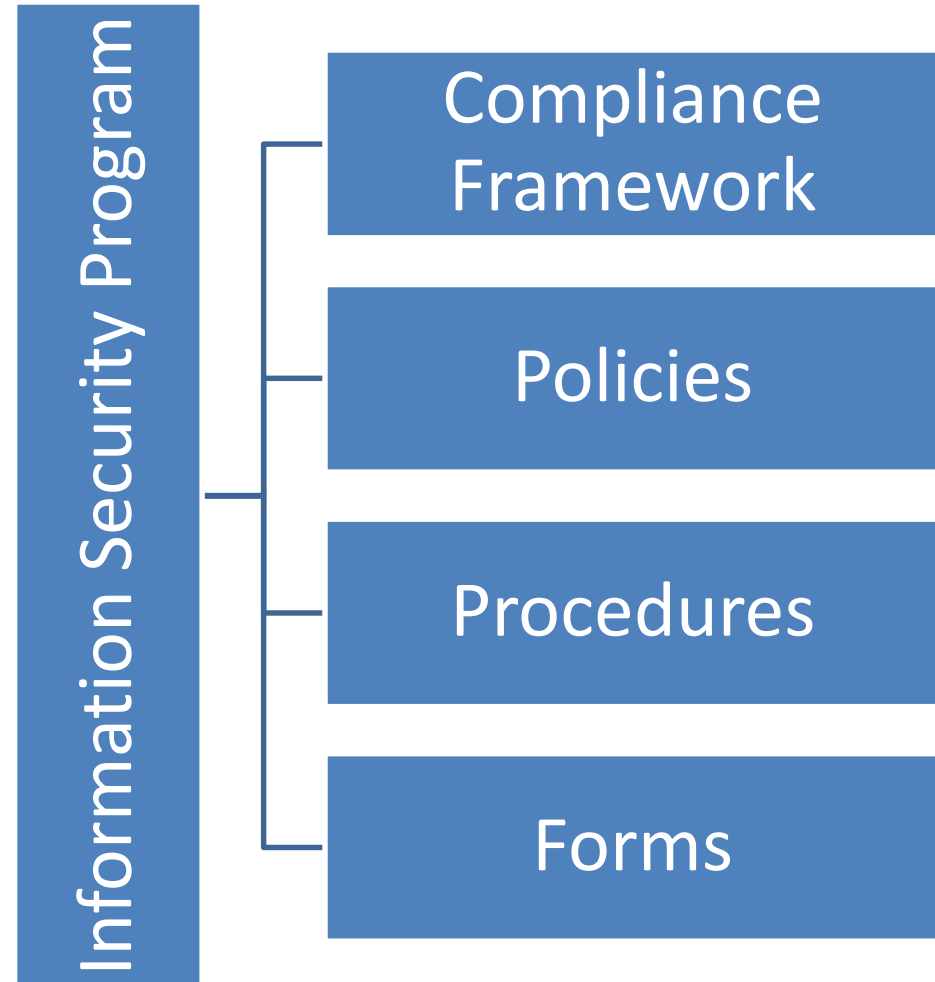
- Areas of Focus
  - Core System
  - Electronic Banking
  - Wire Transfer
  - Hardware
  - Applications
  - Network
  - Etc…

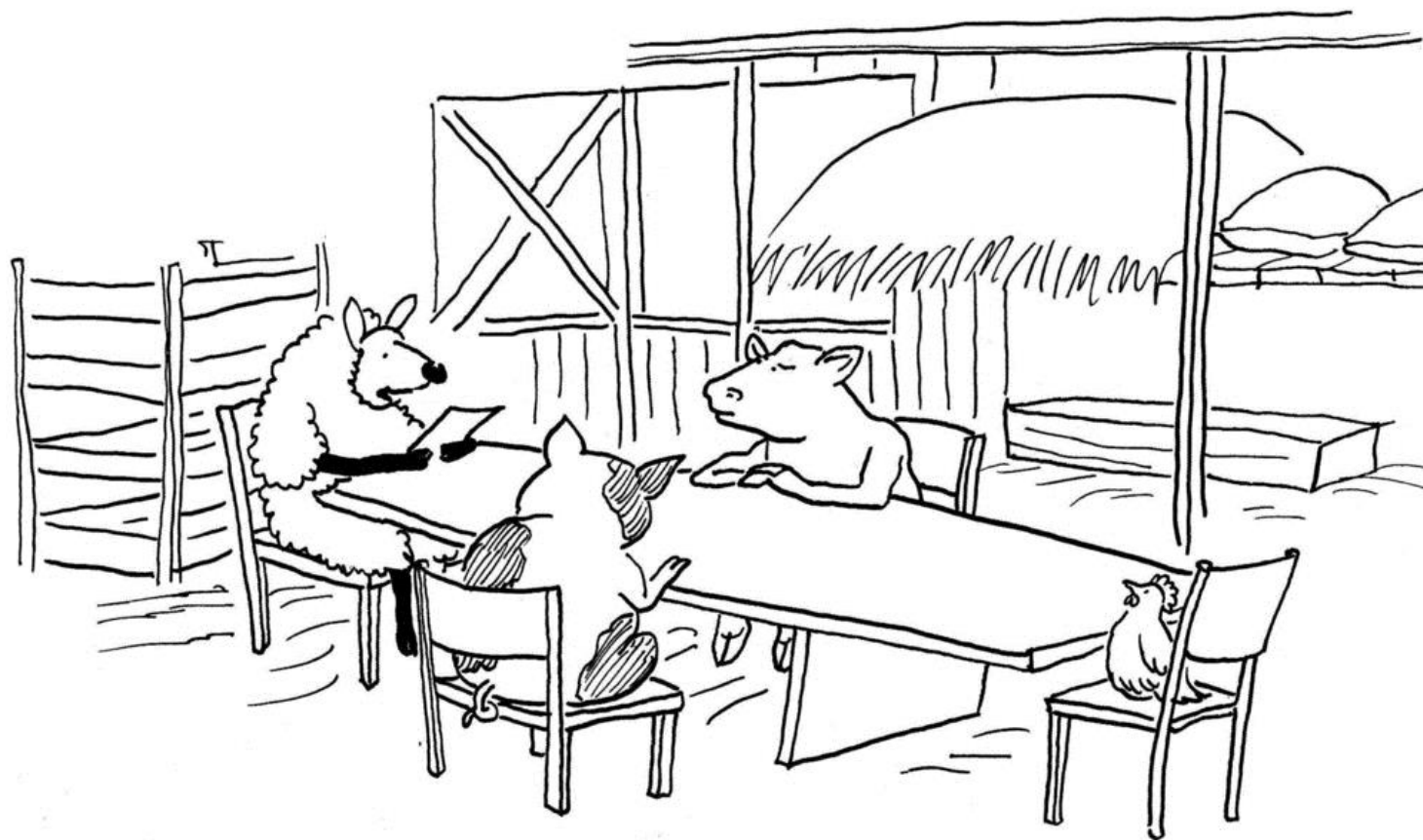# IT Risk Mitigation

1. Risk Identification
2. Risk Measurement
3. Risk Mitigation
4. Review & Monitoring

IT Audit Oversight

"Just because you are compliant does not mean you are secure, but if you are secure you are most likely compliant"

- External audit findings
- Internal audit findings
- Remediation management

The cow mooed, the pig oinked,
the chicken clucked, I bleated, end of meeting."

Business Continuity Plan

- Annual revisions
- Test plans
- Test results

Vendor Management

- Program revisions
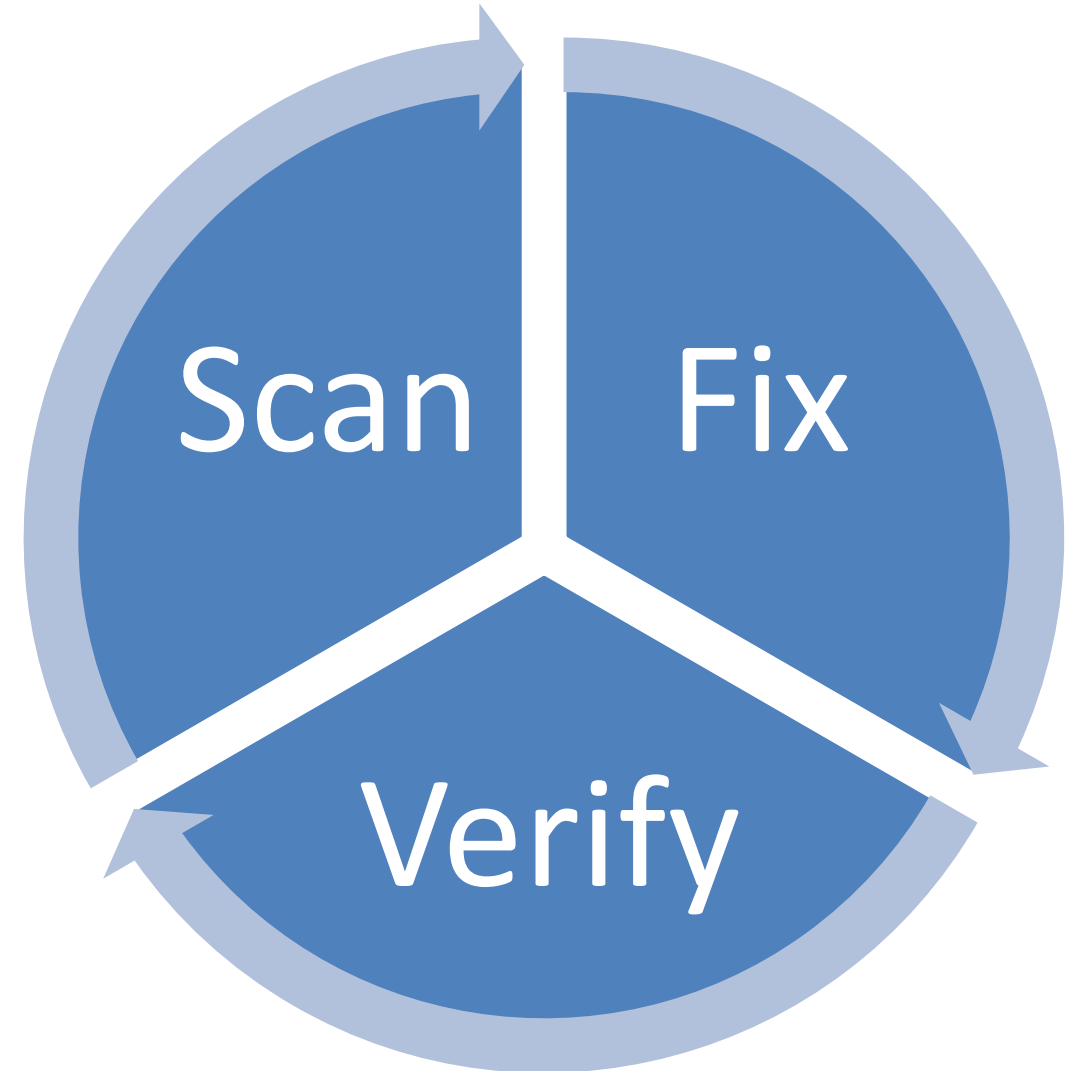- Annual vendor review results

Vendor Due-Diligence

☑ Third-Party Reviewed Financials

☑ SSAE 16 (data centers and operations)

☑ Insurance Coverage - including Cyber-liability

☑ BCP and Disaster Recovery Testing

☑ Annual Penetration Testing

☑ Long Held Industry-Specific Focus
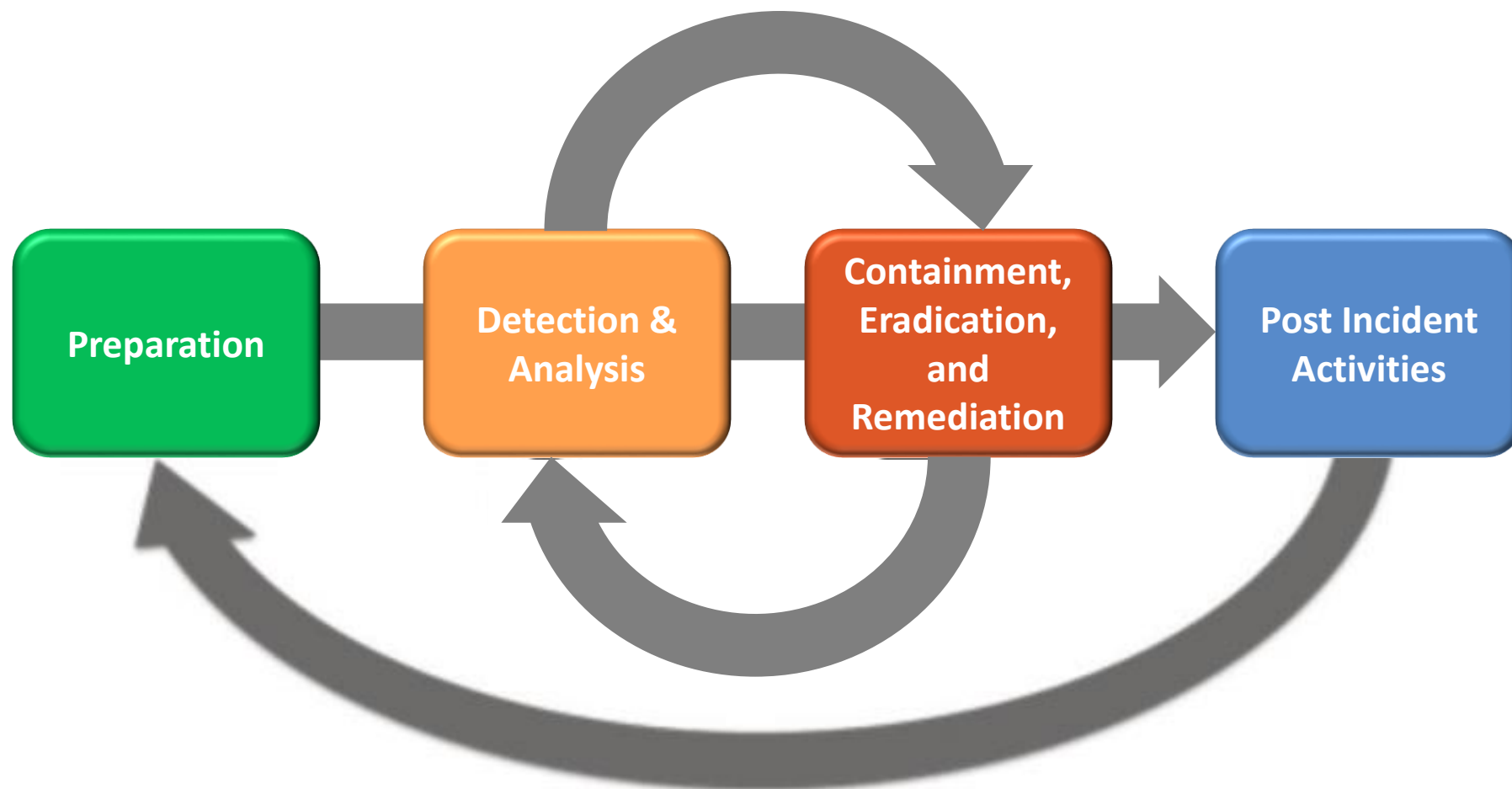
☑ Reference-able Client Base

☑ Clear Legal Standing

Security Event Management

- FFIEC require logs be reviewed to help prevent breaches

- Reviewing log data is time consuming

- Compliance reports need to be easy to read for auditors

- Remediating threats is a necessary component to comply; but doing so takes security expertise

Turning this...

...to that

Collaboration

Financial Services
Information Sharing & Analysis Center

Information Security Program
- Annual revisions to Program
- Training
  - Date of annual training
  - Status of training (number trained / number not trained)
  - Agenda for training

Information Technology Risk Assessment
- Board Summary of findings
  - Overview of process

Audit Information
- External audit findings
- Internal audit findings
- All audit recommendations

IT Steering Committee
- All meeting minutes (quarterly meetings)

Business Continuity Plan
- Annual revisions
- Test plans
- Test results

Vendor Management
- Program revisions
- Annual vendor review results

Internal Vulnerability Assessment
- Completed assessment
- Findings
- Remediation plan

Incident Reporting
- Virus Findings/Reporting throughout the year
- Security Incidents Follow Up / Details

- Brief Introduction to All Covered Finance
- Regulatory Guidelines
- Current challenges
- Role of the Information Security Officer (ISO)
- Hybrid Concept
- Q&A

Hybrid Approach to ISO

Cannot:

- Outsource Oversight
- Afford Dedicated FTE
- Overtask Existing FTE's
- Assume Risk

Can:

- Simplify Oversight
- Outsource InfoSec Tasks
- Utilize Consultative Help
- Mitigate Risk

- ISO with Outsourcing Advisory and Task Execution
  - <$2 billion in assets
  - Provides independent voice
  - Provides information security focus
  - Keeps costs in check
- Dedicated ISO
  - $2 billion in assets
  - Provides independent voice
  - Provides information security focus
- Dedicated Information Security Team (more than 2 FTE's)
  - $5 billion in assets

ISO Advisory Service

- Internal IT Security Assessment
- IT Security Assessment Remediation Planning
- IT Security Remediation Planning
- IT Security Program
- Annual IT Risk Assessment
- Business Continuity Assessment and Planning
- IT Audit Support

ISO Advisory Service

Vulnerability Assessment and Remediation

3rd Party PenTest & Social Engineering Management

Log Management and Security Incident Event Management

IT Security Training

IT Steering Committee Meeting Guidance and Participation

Compliance/Risk Management Committee Participation

Board Training, Reporting and Meeting Participation

Question and Answer

Thanks!

Call me anytime
908.596.0843

Patrick H. Whelan – CISA

Pwhelan@allcovered.com

LinkedIn: http://www.linkedin.com/in/patrickhwhelan