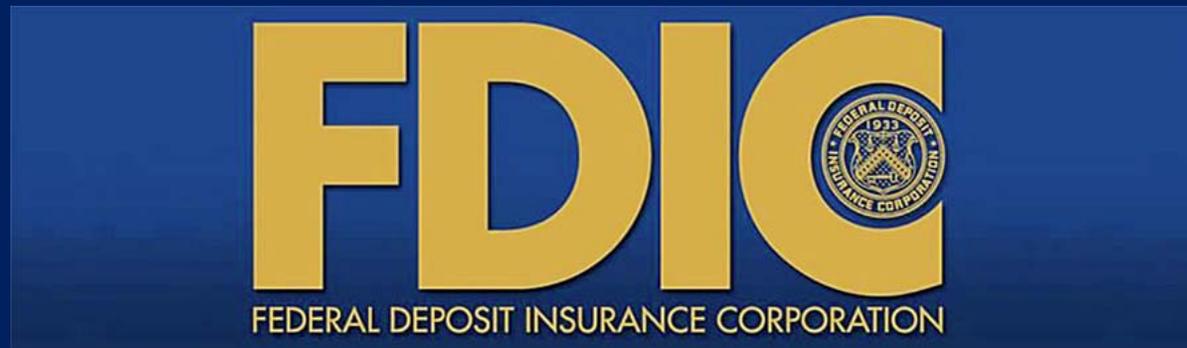
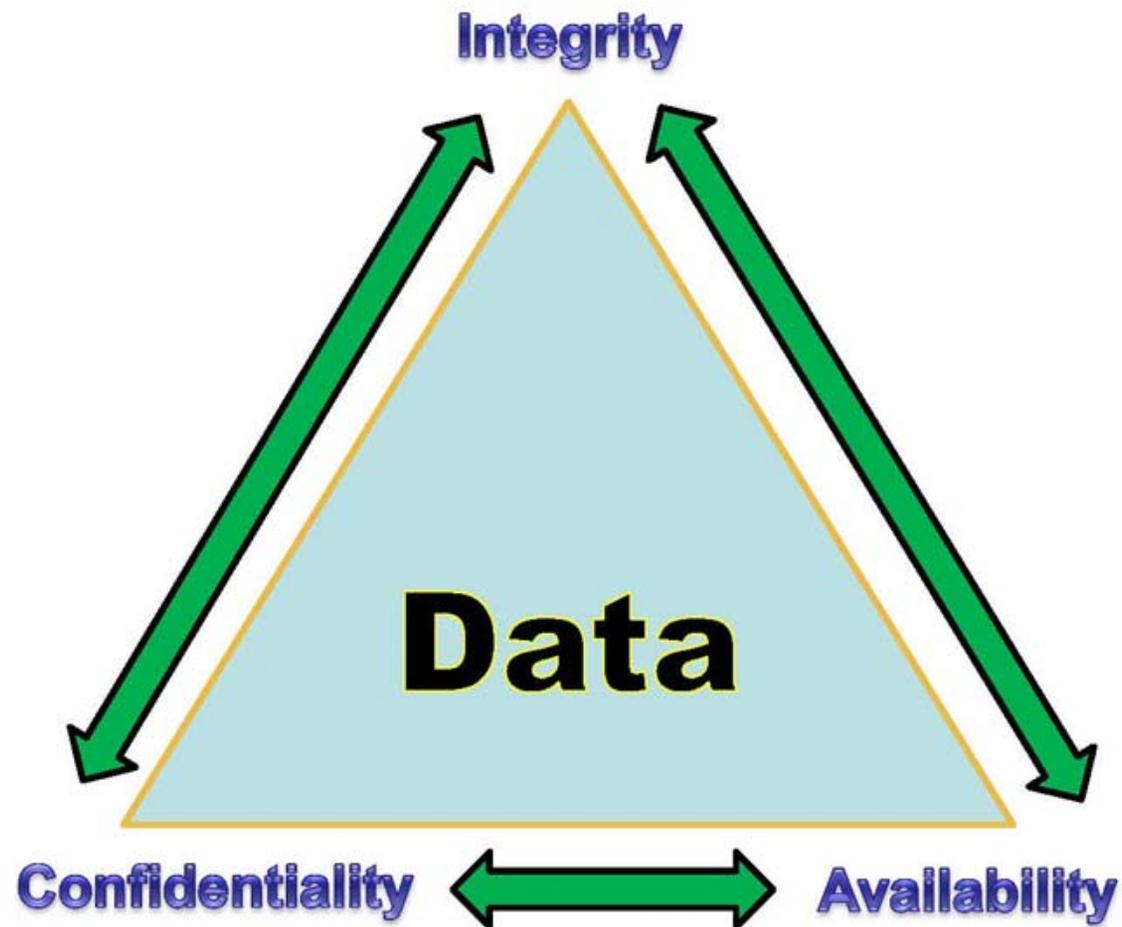


# Cybersecurity and Operational Risk Perspectives



# Cybersecurity

## Evolution of Data Security



# Cybersecurity

## Evolution of Data Security



# Cybersecurity

## Evolution of Data Security



# Cybersecurity

## Definition

- ❑ The National Institute of Standards and Technology (NIST) defines cybersecurity as:

*“The process of protecting information by preventing, detecting, and responding to attacks.”*

- ❑ NIST Framework for Cybersecurity:

- Identify
- Protect
- Detect
- Respond
- Recover

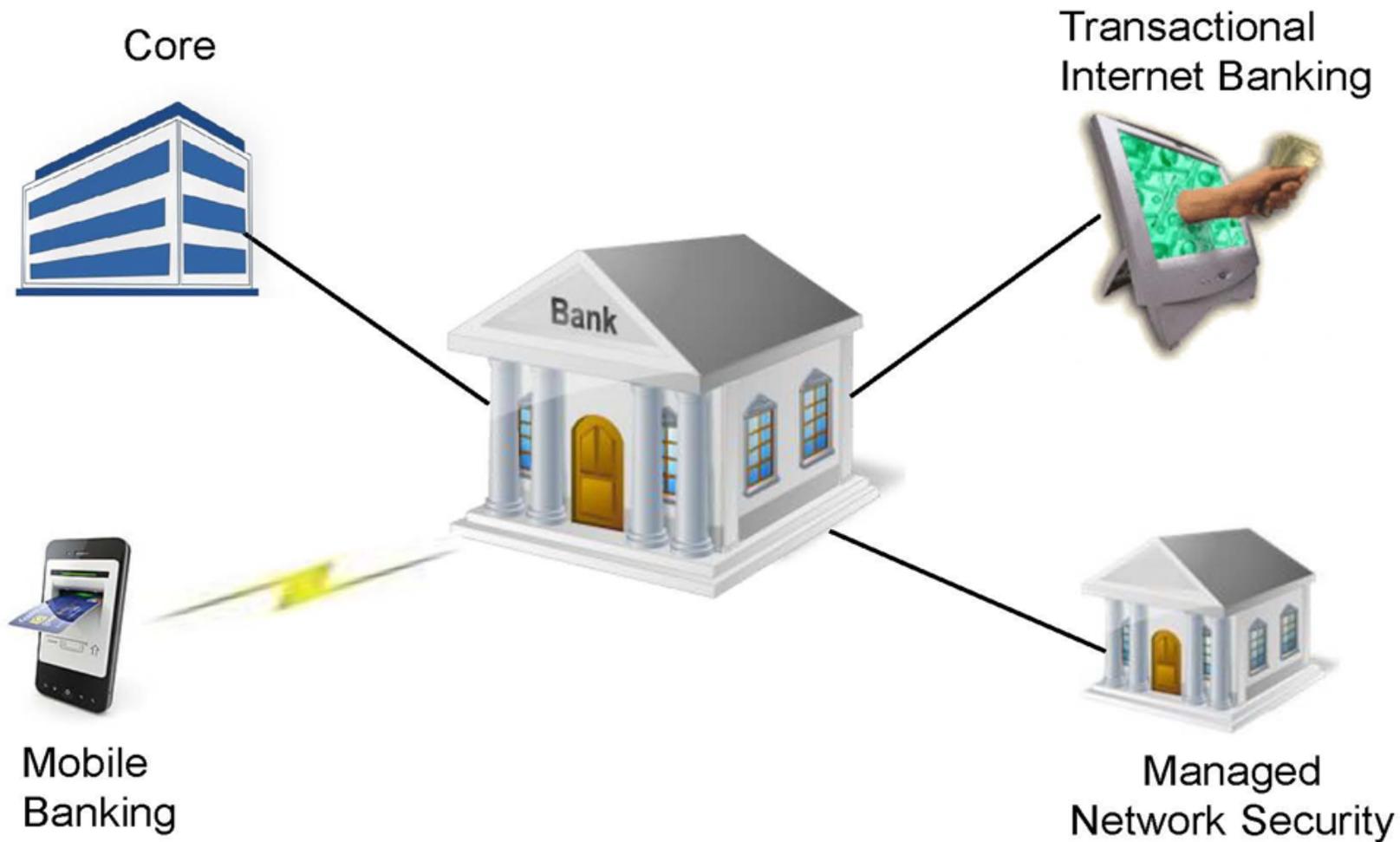
# Cybersecurity

## Governance

- ❑ Cyber Risk is a Business Risk!
- ❑ The Board should communicate their support for Information Security Programs (ISP) and establish a robust governance structure to:
  - ◆ Ensure strategic planning and budgeting provide sufficient resources.
  - ◆ Provide sufficient authority, resources, and independence for information security and IT audit.
  - ◆ Ensure all personnel have ISP training customized to their position.
  - ◆ Establish reporting that assures the Board that the ISP is working.

# Cybersecurity

## Third-Party Management



# Cybersecurity

## Contract Provisions – Appendix J

- ◆ Technology Service Provider Business Continuity Planning (BCP) expectations Outlined in Appendix-J of the BCP Handbook of the FFIEC IT Examination Guidelines (available at [www.ffiec.gov](http://www.ffiec.gov)).
- ◆ Issued in February 2015 (FDIC FIL-9-2015).
- ◆ Focus on Strengthening Resilience of Outsourced Technology Services.
- ◆ Four key elements financial institutions should consider as part of the technology service provider relationships:
  - Third-party management;
  - Third-party capacity;
  - Testing; and
  - Cyber resilience.

# Cybersecurity

## Third-Party Management Contract Considerations

- ◆ Right to Audit
- ◆ Establishing & monitoring performance standards
- ◆ Default and termination
- ◆ Subcontracting
- ◆ Foreign-based third parties
- ◆ BCP testing
- ◆ Data governance
- ◆ Updates
- ◆ Security Issues

# Cybersecurity Summary



# IT and Operations Examinations

## InTREx – General Information

- ◆ Revised Information Technology Examination Program (InTREx) that replaced FDIC's legacy IT examination process.
- ◆ Issued on June 30, 2016 (FDIC Release: FIL-43-2016).
- ◆ Designed to strengthen the identification, assessment, and validation of IT and operational risks at financial institutions.
- ◆ InTREx includes enhancements to address cybersecurity elements.
- ◆ Developed in collaboration with the Federal Reserve and Conference of State Bank Supervisors.
- ◆ Aligns more directly with the Uniform Rating System for Information Technology (URSIT) that addresses critical components of IT risk.
- ◆ URSIT component ratings could lead to enhanced discussions on specific areas of strength and weaknesses within the IT area.

# IT and Operations Examinations

## InTREx – Program Administration

- ◆ InTREx will be less burdensome on financial institutions and provide better information to more effectively risk scope an IT exams.
- ◆ The FDIC’s legacy “technology profile script” and IT Officer’s Questionnaire will be eliminated.
- ◆ Simplified Information Technology Profile (ITP) will focus on the types of technologies utilized and changes since the last examination.
- ◆ ITP will allow examination staff to more effectively risk scope an examination; customize information requests; and ensure suitable examination staff is assigned commensurate with the complexity of the institution's information technologies.

# IT and Operations Examinations

## InTREx – Components

### ITP

Information Technology  
Profile

Risk Profile

Qualitative Adjustment

### Work Program

Core Modules

Expanded  
Modules

Supplemental  
Workprograms

# IT and Operations Examinations

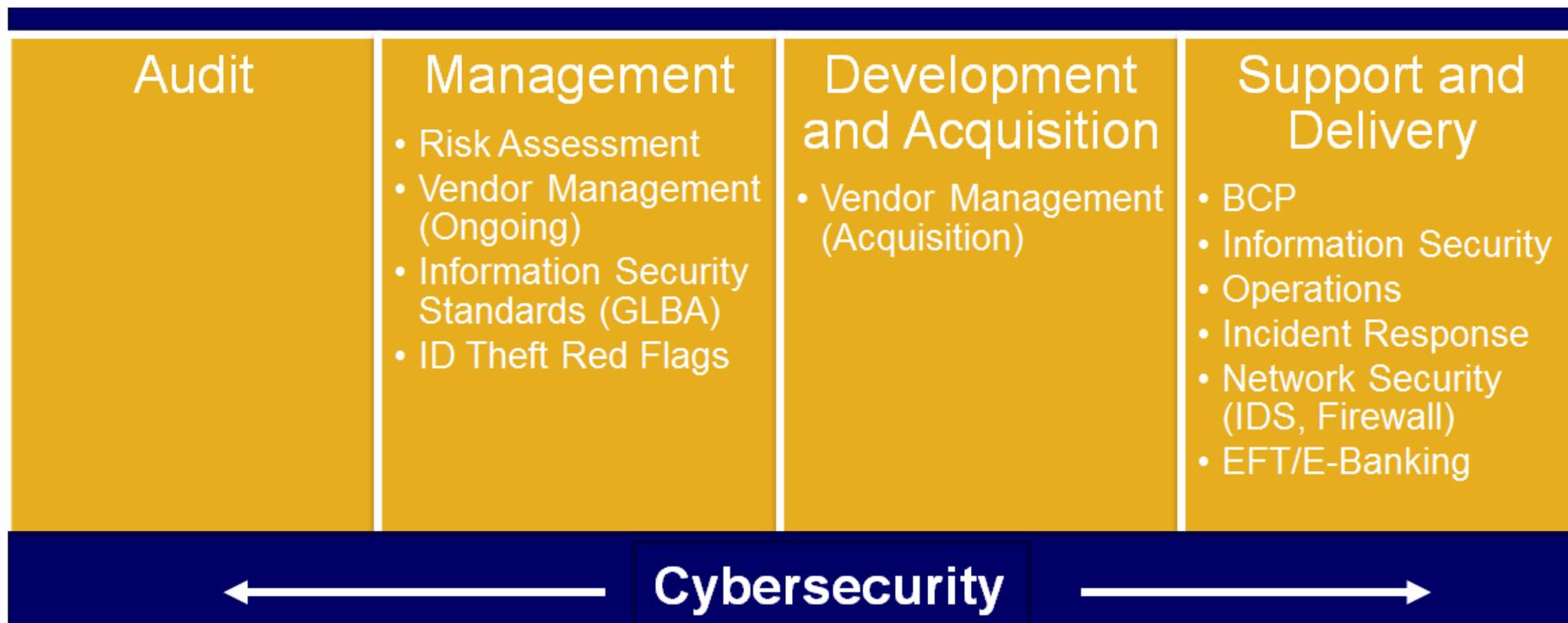
## InTREx – Core Modules

I. Audit

II. Management

III. Support and Delivery

IV. Development and Acquisition



# Cybersecurity and Operational Risk Perspectives

**Q&A**  
QUESTIONS & ANSWERS SESSION