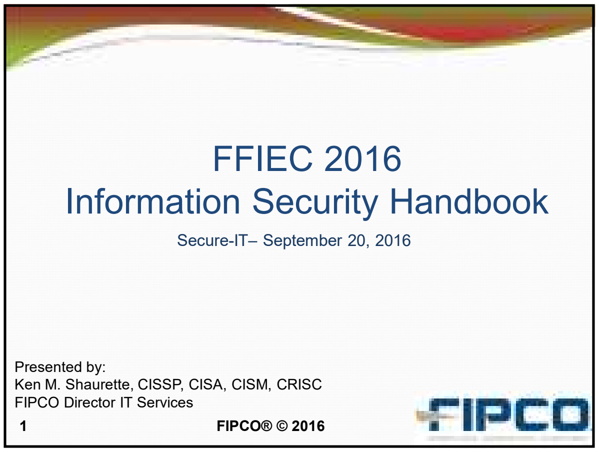
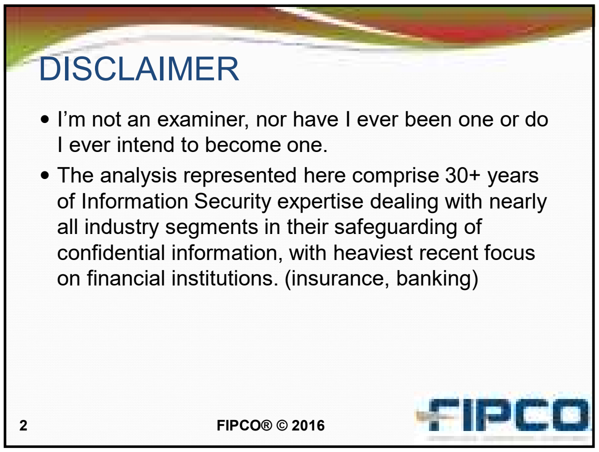


FFIEC 2016
Information Security Handbook

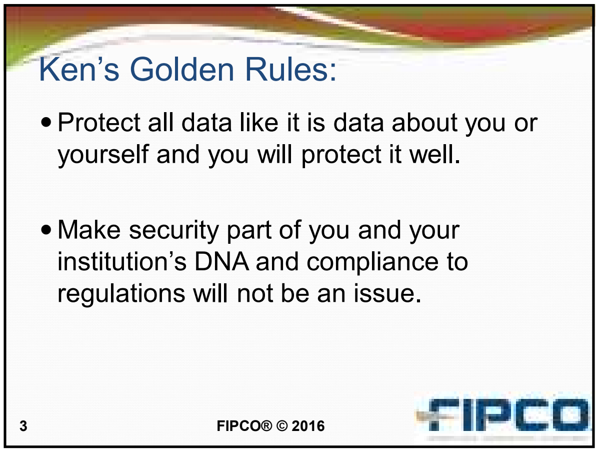
Secure-IT– September 20, 2016

Presented by:
Ken M. Shaurette, CISSP, CISA, CISM, CRISC
FIPCO Director IT Services



DISCLAIMER

- I'm not an examiner, nor have I ever been one or do I ever intend to become one.
- The analysis represented here comprise 30+ years of Information Security expertise dealing with nearly all industry segments in their safeguarding of confidential information, with heaviest recent focus on financial institutions. (insurance, banking)



Ken's Golden Rules:

- Protect all data like it is data about you or yourself and you will protect it well.
- Make security part of you and your institution's DNA and compliance to regulations will not be an issue.

Who are the Organizations?

- ***FFIEC*** = Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB).

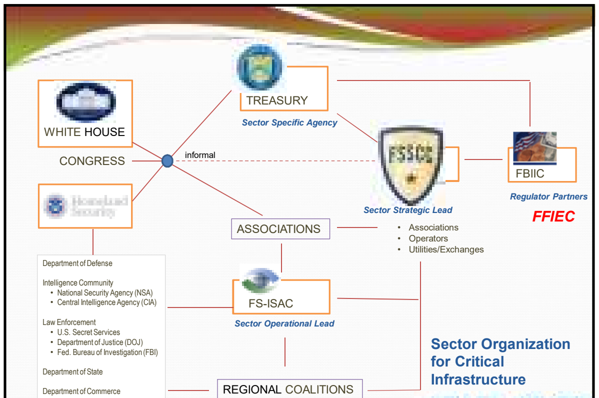
  The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions and to make recommendations to promote uniformity in the supervision of financial institutions.

Who are the Organizations?

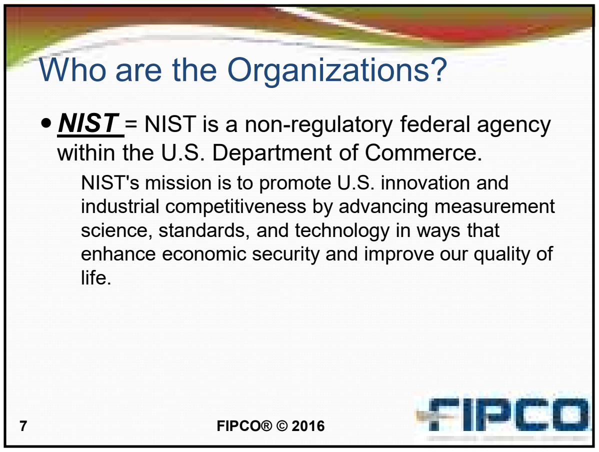
- **FSSCC** = 70+ members consist of financial trade associations, financial utilities, and the most critical financial firms.

  FSSCC partners with the public sector on policy issues concerning the resilience of the sector. Over the years, the FSSCC has built and maintained relationships with the U.S. Treasury and Homeland Security Departments, all the federal financial regulatory agencies and law enforcement agencies (e.g., FBI, U.S. Secret Service).

  FBIIC – Financial and Banking Information Infrastructure Committee.



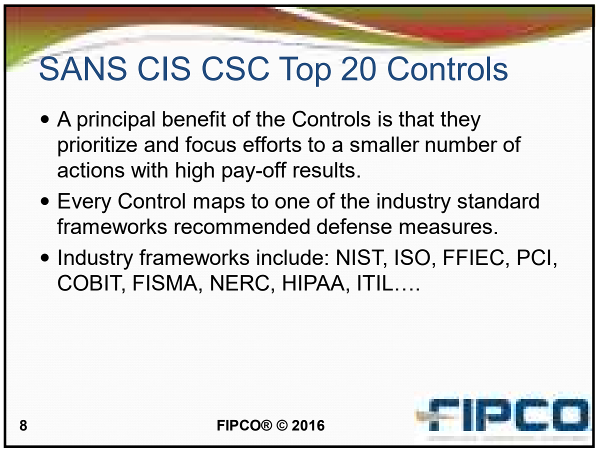
Sector Organization for Critical Infrastructure



Who are the Organizations?

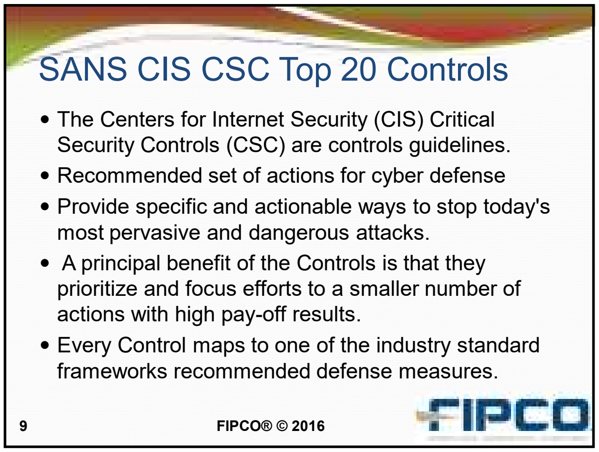
- ***NIST*** = NIST is a non-regulatory federal agency within the U.S. Department of Commerce.

  NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.



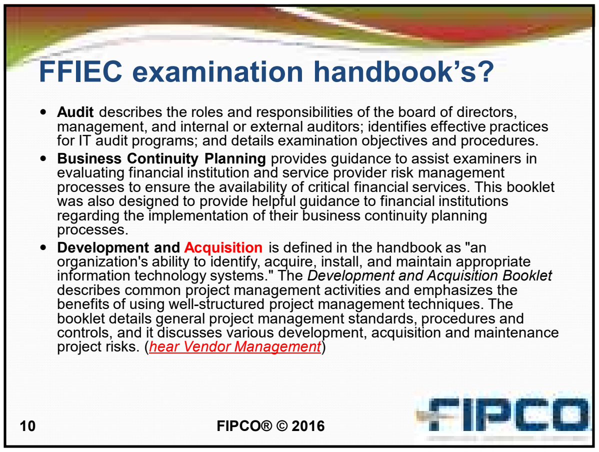
SANS CIS CSC Top 20 Controls

- A principal benefit of the Controls is that they prioritize and focus efforts to a smaller number of actions with high pay-off results.
- Every Control maps to one of the industry standard frameworks recommended defense measures.
- Industry frameworks include: NIST, ISO, FFIEC, PCI, COBIT, FISMA, NERC, HIPAA, ITIL….



SANS CIS CSC Top 20 Controls

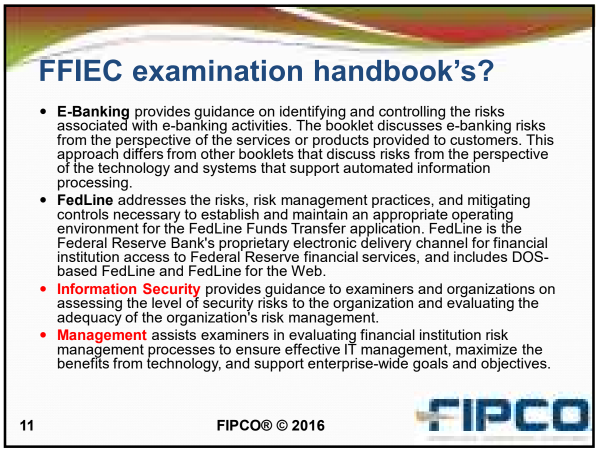
- The Centers for Internet Security (CIS) Critical Security Controls (CSC) are controls guidelines.
- Recommended set of actions for cyber defense
- Provide specific and actionable ways to stop today's most pervasive and dangerous attacks.
- A principal benefit of the Controls is that they prioritize and focus efforts to a smaller number of actions with high pay-off results.
- Every Control maps to one of the industry standard frameworks recommended defense measures.



FFIEC examination handbook's?

- **Audit** describes the roles and responsibilities of the board of directors, management, and internal or external auditors; identifies effective practices for IT audit programs; and details examination objectives and procedures.
- **Business Continuity Planning** provides guidance to assist examiners in evaluating financial institution and service provider risk management processes to ensure the availability of critical financial services. This booklet was also designed to provide helpful guidance to financial institutions regarding the implementation of their business continuity planning processes.
- **Development and Acquisition** is defined in the handbook as "an organization's ability to identify, acquire, install, and maintain appropriate information technology systems." The *Development and Acquisition Booklet* describes common project management activities and emphasizes the benefits of using well-structured project management techniques. The booklet details general project management standards, procedures and controls, and it discusses various development, acquisition and maintenance project risks. (*hear Vendor Management*)

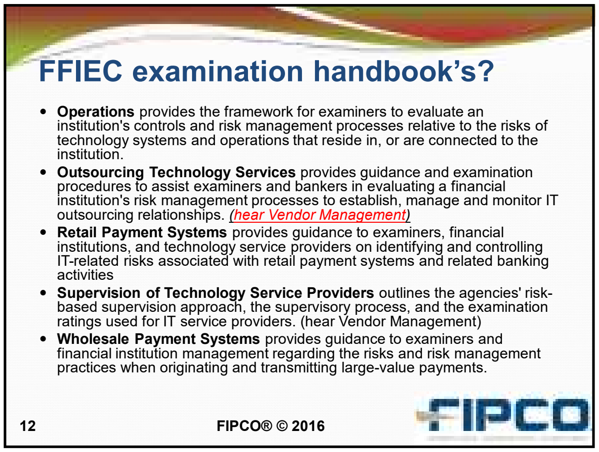
10 FIPCO® © 2016



FFIEC examination handbook's?

- **E-Banking** provides guidance on identifying and controlling the risks associated with e-banking activities. The booklet discusses e-banking risks from the perspective of the services or products provided to customers. This approach differs from other booklets that discuss risks from the perspective of the technology and systems that support automated information processing.
- **FedLine** addresses the risks, risk management practices, and mitigating controls necessary to establish and maintain an appropriate operating environment for the FedLine Funds Transfer application. FedLine is the Federal Reserve Bank's proprietary electronic delivery channel for financial institution access to Federal Reserve financial services, and includes DOS-based FedLine and FedLine for the Web.
- **Information Security** provides guidance to examiners and organizations on assessing the level of security risks to the organization and evaluating the adequacy of the organization's risk management.
- **Management** assists examiners in evaluating financial institution risk management processes to ensure effective IT management, maximize the benefits from technology, and support enterprise-wide goals and objectives.

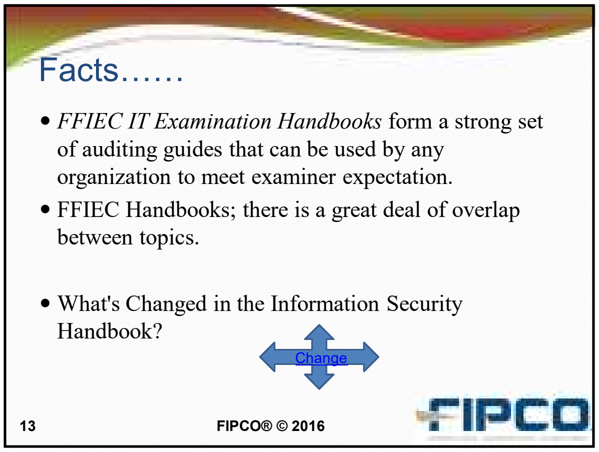
11 FIPCO® © 2016



FFIEC examination handbook's?

- **Operations** provides the framework for examiners to evaluate an institution's controls and risk management processes relative to the risks of technology systems and operations that reside in, or are connected to the institution.
- **Outsourcing Technology Services** provides guidance and examination procedures to assist examiners and bankers in evaluating a financial institution's risk management processes to establish, manage and monitor IT outsourcing relationships. *(hear Vendor Management)*
- **Retail Payment Systems** provides guidance to examiners, financial institutions, and technology service providers on identifying and controlling IT-related risks associated with retail payment systems and related banking activities
- **Supervision of Technology Service Providers** outlines the agencies' risk-based supervision approach, the supervisory process, and the examination ratings used for IT service providers. (hear Vendor Management)
- **Wholesale Payment Systems** provides guidance to examiners and financial institution management regarding the risks and risk management practices when originating and transmitting large-value payments.

12 FIPCO® © 2016

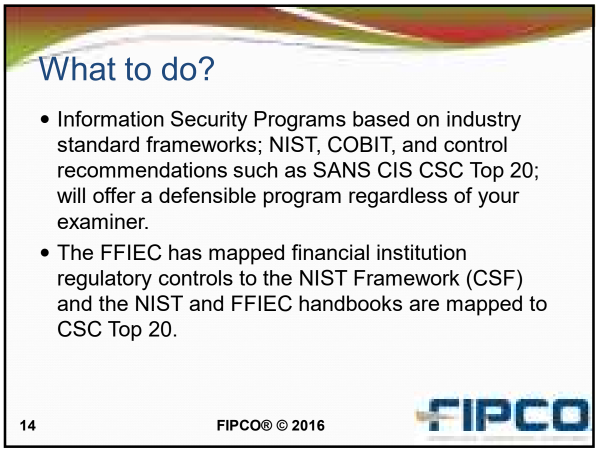


Facts……

- *FFIEC IT Examination Handbooks* form a strong set of auditing guides that can be used by any organization to meet examiner expectation.
- FFIEC Handbooks; there is a great deal of overlap between topics.
- What's Changed in the Information Security Handbook?

Change

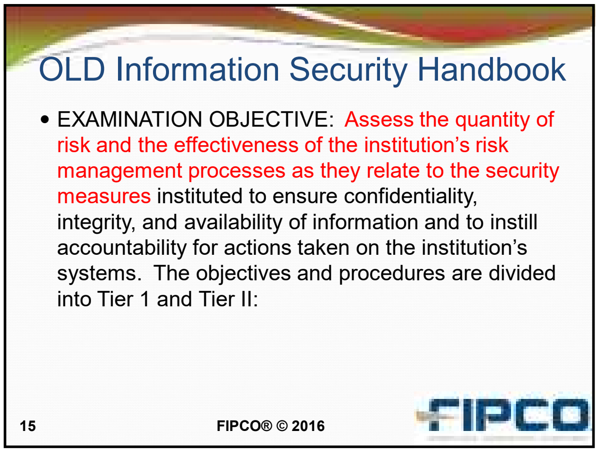
13 FIPCO® © 2016



What to do?

- Information Security Programs based on industry standard frameworks; NIST, COBIT, and control recommendations such as SANS CIS CSC Top 20; will offer a defensible program regardless of your examiner.
- The FFIEC has mapped financial institution regulatory controls to the NIST Framework (CSF) and the NIST and FFIEC handbooks are mapped to CSC Top 20.

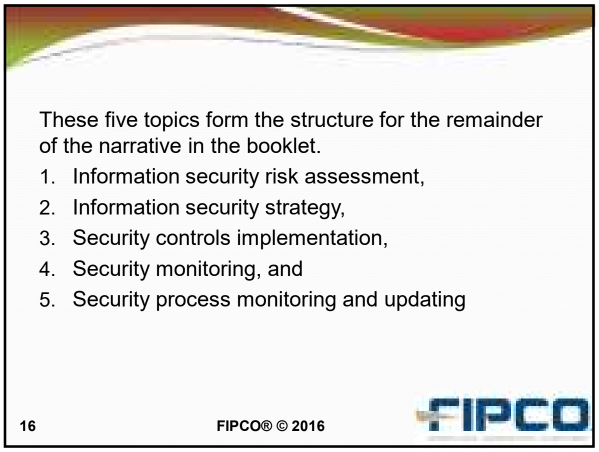
14 FIPCO® © 2016



OLD Information Security Handbook

- EXAMINATION OBJECTIVE: Assess the quantity of risk and the effectiveness of the institution’s risk management processes as they relate to the security measures instituted to ensure confidentiality, integrity, and availability of information and to instill accountability for actions taken on the institution’s systems. The objectives and procedures are divided into Tier 1 and Tier II:

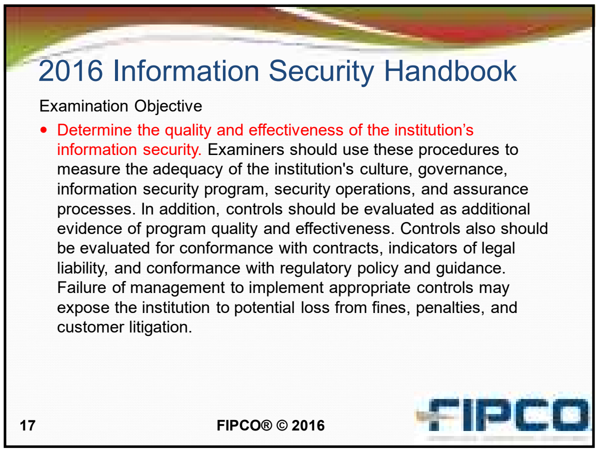
15 FIPCO® © 2016



These five topics form the structure for the remainder of the narrative in the booklet.

1. Information security risk assessment,
2. Information security strategy,
3. Security controls implementation,
4. Security monitoring, and
5. Security process monitoring and updating

16 FIPCO® © 2016

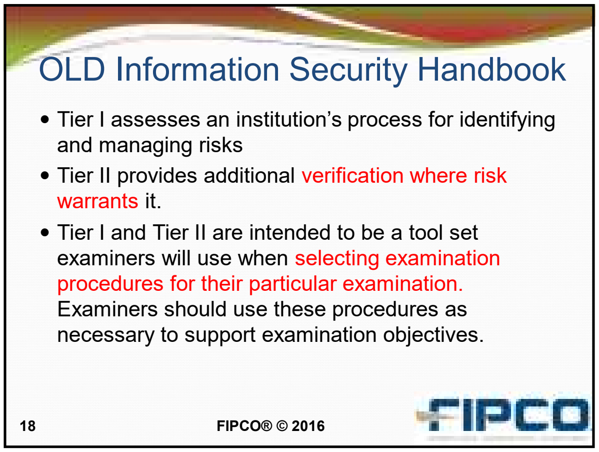


2016 Information Security Handbook

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.

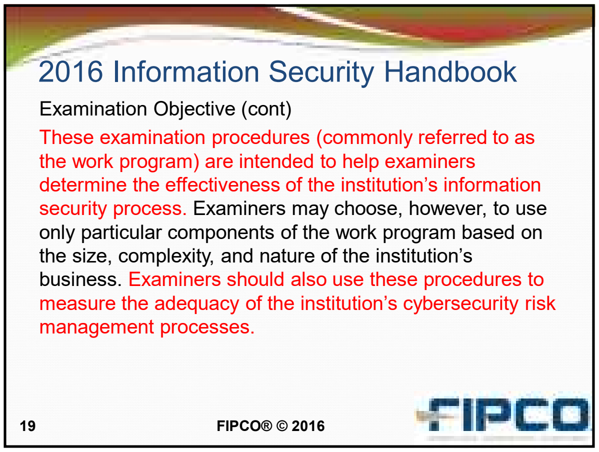
17 FIPCO® © 2016



OLD Information Security Handbook

- Tier I assesses an institution's process for identifying and managing risks
- Tier II provides additional verification where risk warrants it.
- Tier I and Tier II are intended to be a tool set examiners will use when selecting examination procedures for their particular examination. Examiners should use these procedures as necessary to support examination objectives.

18 FIPCO® © 2016

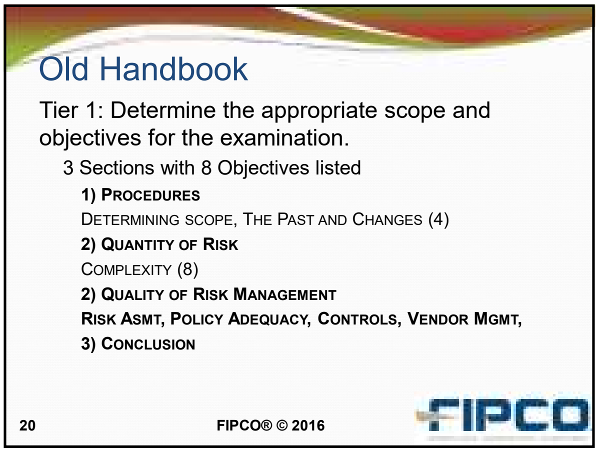


2016 Information Security Handbook

Examination Objective (cont)

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.

19 FIPCO® © 2016



Old Handbook

Tier 1: Determine the appropriate scope and objectives for the examination.

3 Sections with 8 Objectives listed

1) Procedures

Determining scope, The Past and Changes (4)

2) Quantity of Risk

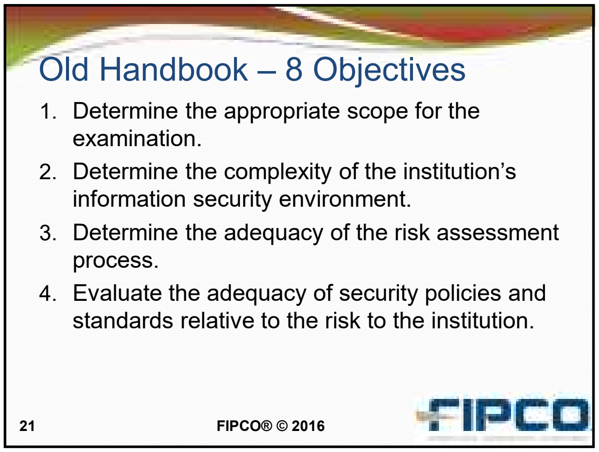
Complexity (8)

2) Quality of Risk Management

Risk Asmt, Policy Adequacy, Controls, Vendor Mgmt,

3) Conclusion

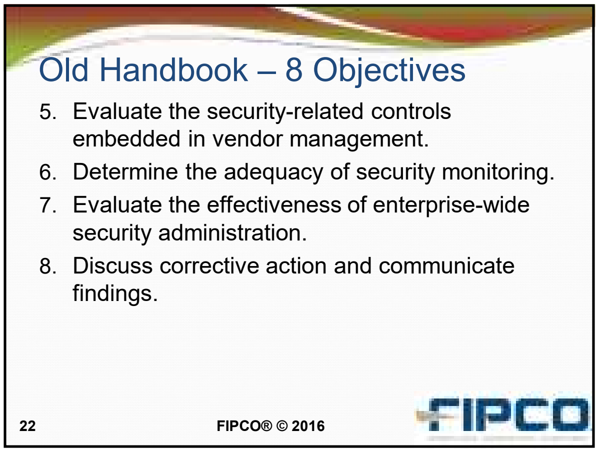
20 FIPCO® © 2016



Old Handbook – 8 Objectives

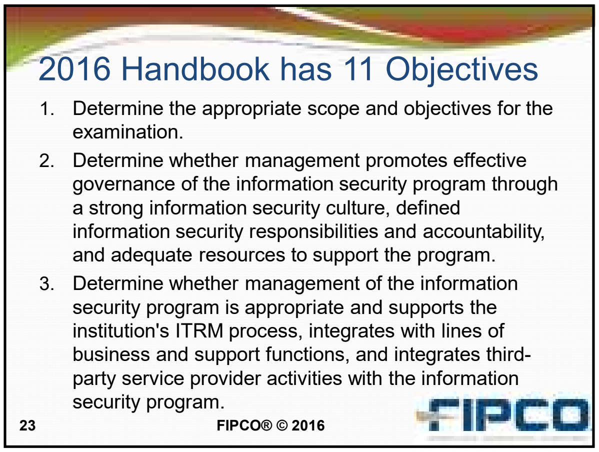
1. Determine the appropriate scope for the examination.
2. Determine the complexity of the institution's information security environment.
3. Determine the adequacy of the risk assessment process.
4. Evaluate the adequacy of security policies and standards relative to the risk to the institution.

21 FIPCO® © 2016



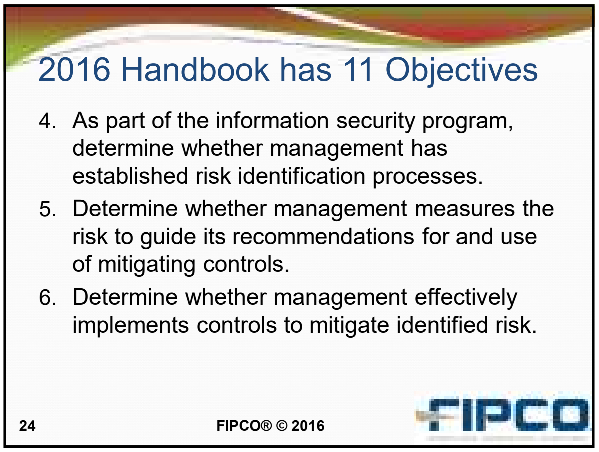
Old Handbook – 8 Objectives

5. Evaluate the security-related controls embedded in vendor management.
6. Determine the adequacy of security monitoring.
7. Evaluate the effectiveness of enterprise-wide security administration.
8. Discuss corrective action and communicate findings.



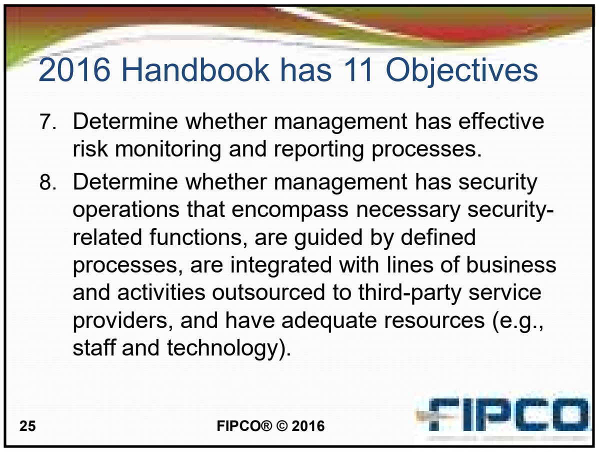
2016 Handbook has 11 Objectives

1. Determine the appropriate scope and objectives for the examination.
2. Determine whether management promotes effective governance of the information security program through a strong information security culture, defined information security responsibilities and accountability, and adequate resources to support the program.
3. Determine whether management of the information security program is appropriate and supports the institution's ITRM process, integrates with lines of business and support functions, and integrates third-party service provider activities with the information security program.



2016 Handbook has 11 Objectives

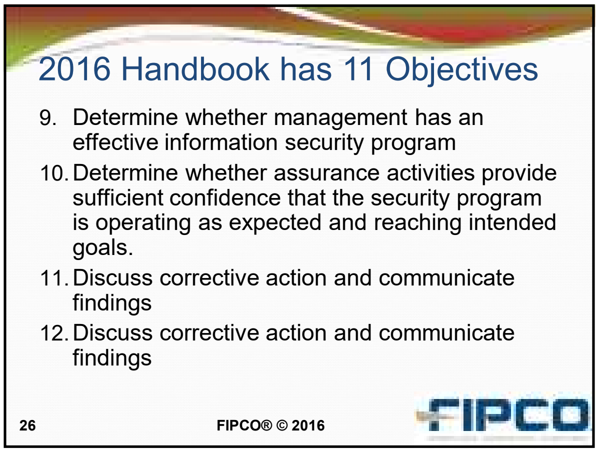
4. As part of the information security program, determine whether management has established risk identification processes.
5. Determine whether management measures the risk to guide its recommendations for and use of mitigating controls.
6. Determine whether management effectively implements controls to mitigate identified risk.



2016 Handbook has 11 Objectives

7. Determine whether management has effective risk monitoring and reporting processes.
8. Determine whether management has security operations that encompass necessary security-related functions, are guided by defined processes, are integrated with lines of business and activities outsourced to third-party service providers, and have adequate resources (e.g., staff and technology).

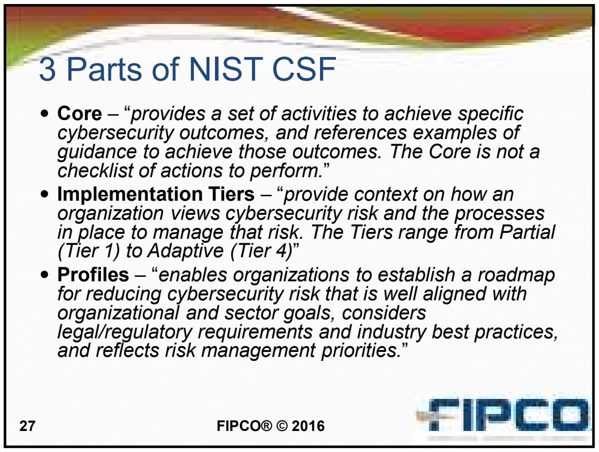
25 FIPCO® © 2016



2016 Handbook has 11 Objectives

9. Determine whether management has an effective information security program
10. Determine whether assurance activities provide sufficient confidence that the security program is operating as expected and reaching intended goals.
11. Discuss corrective action and communicate findings
12. Discuss corrective action and communicate findings

26 FIPCO® © 2016



3 Parts of NIST CSF

- **Core** – *"provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. The Core is not a checklist of actions to perform."*
- **Implementation Tiers** – *"provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4)"*
- **Profiles** – *"enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities."*

27 FIPCO® © 2016

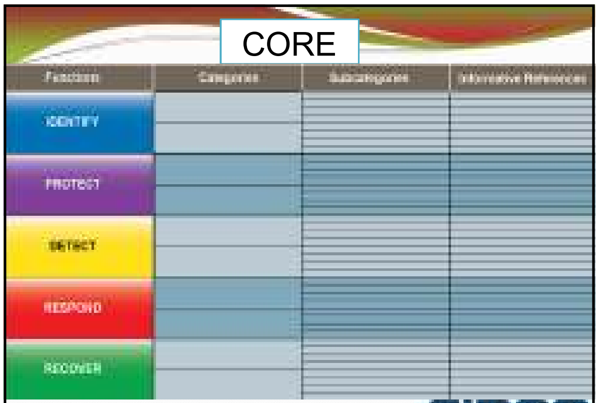
Part 1 Core

Four (4) elements:

1. **Functions** – there are five (5) Functions; Identify, Protect, Detect, Response, and Recover
2. **Categories** – each of the five Functions is further divided in to Categories
3. **Subcategories** – each of the Categories is further divided in Subcategories
4. **Informative References** – each Subcategory is supported by one or more Informative References (standards, guidelines, and practices)

28 FIPCO® © 2016

CORE



29 FIPCO® © 2016

Part 1 Implementation: 4 Tiers

Current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints. (THINK MATURITY with a TWIST)

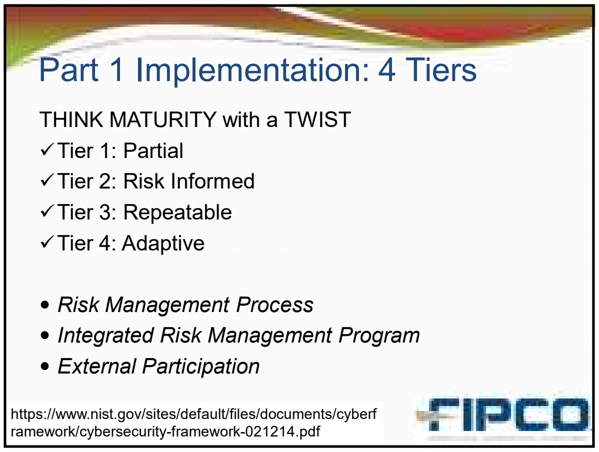
✓Tier 1: Partial

✓Tier 2: Risk Informed

✓Tier 3: Repeatable

✓Tier 4: Adaptive

https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf



Part 1 Implementation: 4 Tiers

THINK MATURITY with a TWIST

✓Tier 1: Partial

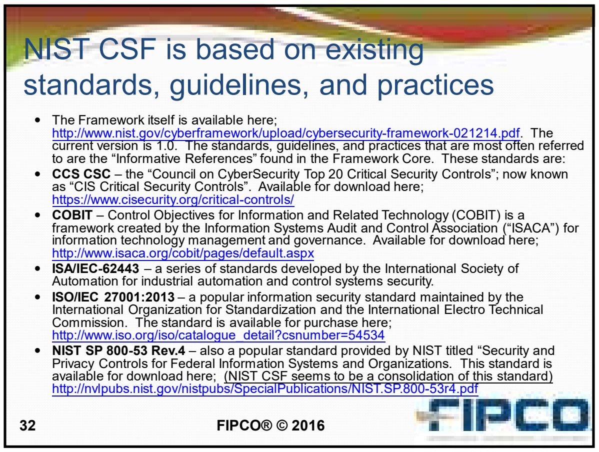
✓Tier 2: Risk Informed

✓Tier 3: Repeatable

✓Tier 4: Adaptive

- *Risk Management Process*
- *Integrated Risk Management Program*
- *External Participation*

https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf



NIST CSF is based on existing standards, guidelines, and practices

- The Framework itself is available here; http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf. The current version is 1.0. The standards, guidelines, and practices that are most often referred to are the "Informative References" found in the Framework Core. These standards are:
- **CCS CSC** – the "Council on CyberSecurity Top 20 Critical Security Controls"; now known as "CIS Critical Security Controls". Available for download here; https://www.cisecurity.org/critical-controls/
- **COBIT** – Control Objectives for Information and Related Technology (COBIT) is a framework created by the Information Systems Audit and Control Association ("ISACA") for information technology management and governance. Available for download here; http://www.isaca.org/cobit/pages/default.aspx
- **ISA/IEC-62443** – a series of standards developed by the International Society of Automation for industrial automation and control systems security.
- **ISO/IEC 27001:2013** – a popular information security standard maintained by the International Organization for Standardization and the International Electro Technical Commission. The standard is available for purchase here; http://www.iso.org/iso/catalogue_detail?csnumber=54534
- **NIST SP 800-53 Rev.4** – also a popular standard provided by NIST titled "Security and Privacy Controls for Federal Information Systems and Organizations. This standard is available for download here; (NIST CSF seems to be a consolidation of this standard) http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

32 FIPCO® © 2016

Questions & Discussion

CLICK HERE

33 FIPCO® © 2016