

Russ Horn & Leticia Saiid

Foundations of Information Security



1

Disclaimer

A FEW THINGS FIRST

This presentation is for information only.

Evaluate risks before acting based on ideas from this presentation.

This presentation contains opinions of the presenters.

Opinions may not reflect the opinions of Tandem.

This presentation is proprietary.

Unauthorized release of this information is prohibited.

Original material is copyright © 2022 Tandem.



2

Agenda

- Regulatory Foundations of Information Security
- Risk Management
- Role of ISO
- Vendor Management
- Business Continuity & Incident Management
- Assurance & Testing
- Education & Reporting



3



**Russ
Horn**

President



**Leticia
Saiid**

Chief of Staff



4

Tell us about you.



1. What title(s) do you hold at your bank?
2. How much ISO/cyber experience do you have?
3. What do you hope to gain from this pre-conference track?
4. What do you hope to gain from the overall conference?



5



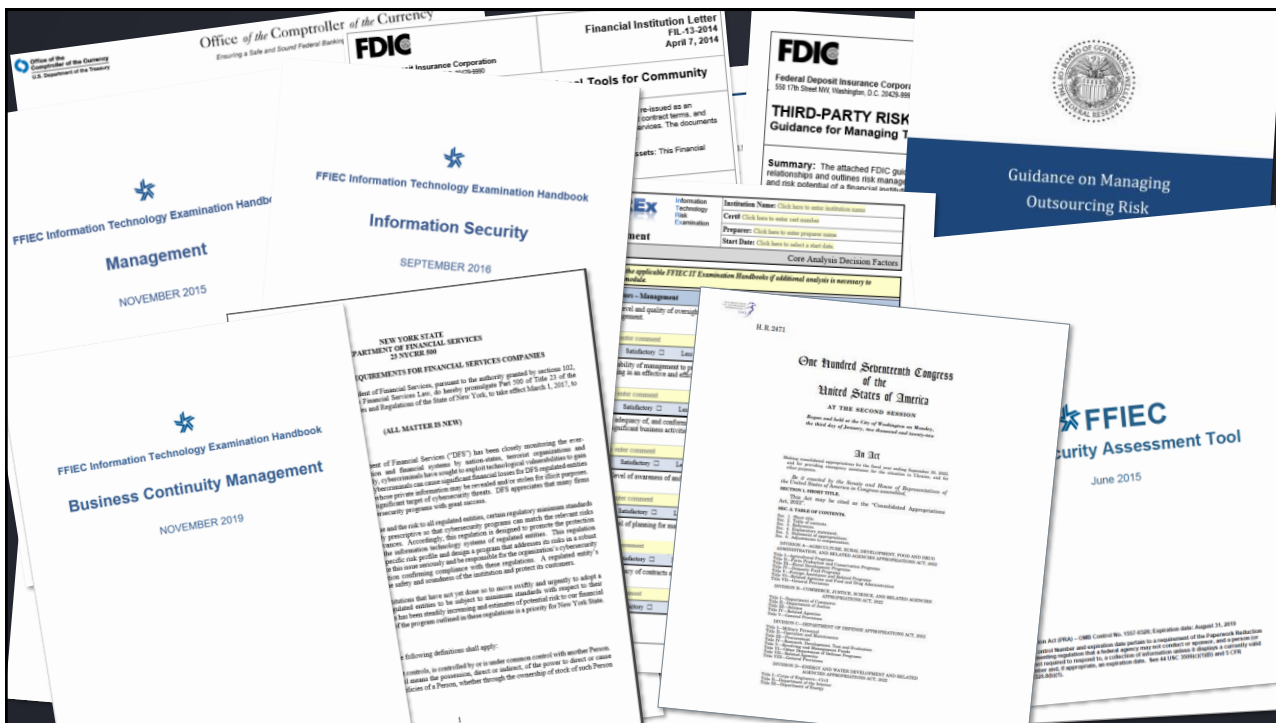
Regulatory Foundations of Information Security

6

U.S. Laws, Regulations, and Guidance related to Information Security



7



8

GLBA Section 501(b)



Gramm-Leach-Bliley Act

TITLE V—PRIVACY

Subtitle A—Disclosure of Nonpublic Personal Information

15 USC 6801.

SEC. 501. PROTECTION OF NONPUBLIC PERSONAL INFORMATION.


(a) **PRIVACY OBLIGATION POLICY.**—It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.

(b) **FINANCIAL INSTITUTIONS SAFEGUARDS.**—In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

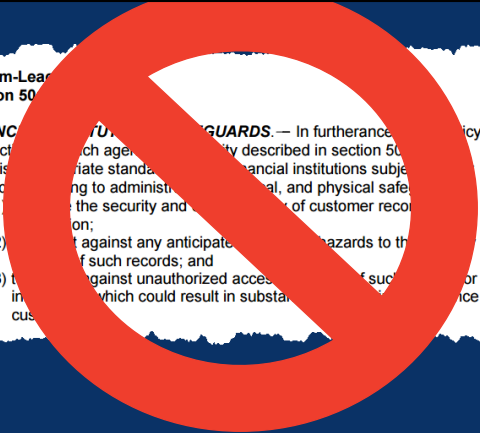



Ed Markey

Gramm-Leach-Bliley Act
Section 501(b)

FINANCIAL INSTITUTIONS SAFEGUARDS. — In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—

- (1) to insure the security and confidentiality of customer records and information;
- (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
- (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Ed Markey

Gramm-Leach
Section 501

FINANCIAL INSTITUTIONS SAFEGUARDS.— In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—

- (1) to insure the security and confidentiality of customer records and information;
- (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
- (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Joe Barton

REGULATIONS

BANK

BANK EXAMS

KEYS CONFERENCE

11

Interagency Guidelines Establishing Information Security Standards

TITLE V—PRIVACY

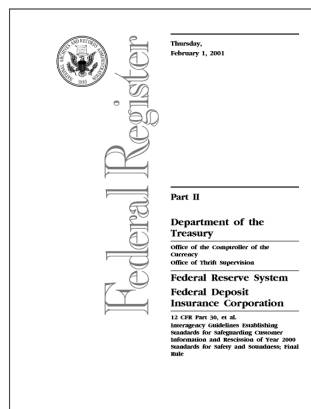
Subtitle A—Disclosure of Nonpublic Personal Information

15 USC 6801. **SEC. 501. PROTECTION OF NONPUBLIC PERSONAL INFORMATION.**

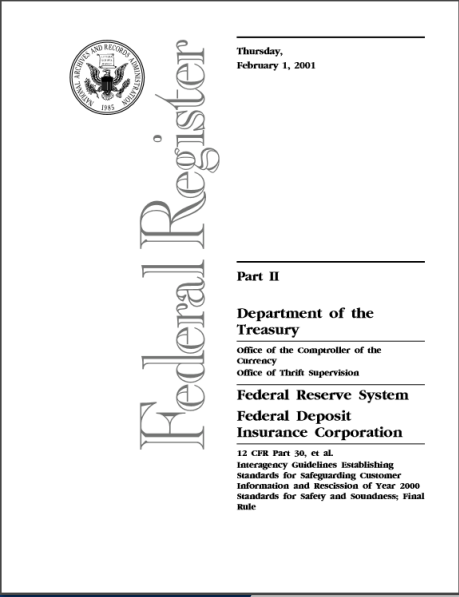
(a) **PRIVACY OBLIGATION POLICY.**—It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.

(b) **FINANCIAL INSTITUTIONS SAFEGUARDS.**—In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—

- (1) to insure the security and confidentiality of customer records and information;
- (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
- (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.




12



Interagency Guidelines Establishing Information Security Standards

- OCC 12 CFR Part 30
- FRB 12 CFR Part 208
- FDIC 12 CFR Part 364
- NCUA 12 CFR Part 748



13


Interagency Guidelines Establishing Information Security Standards

II. Standards for Safeguarding Customer Information

A. Information Security Program. Each bank shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. While all parts of the bank are not required to implement a uniform set of policies, all elements of the information security program must be coordinated.

B. Objectives. A bank's information security program shall be designed to:

1. Ensure the security and confidentiality of customer information;
2. Protect against any anticipated threats or hazards to the security or integrity of such information; and
3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.



14

GLBA Section 501(b)

Gramm-Leach-Bliley Act

TITLE V—PRIVACY

Subtitle A—Disclosure of Nonpublic Personal Information

15 USC 6801.

SEC. 501. PROTECTION OF NONPUBLIC PERSONAL INFORMATION.

(a) **PRIVACY OBLIGATION POLICY.**—It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.

(b) **FINANCIAL INSTITUTIONS SAFEGUARDS.**—In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.



15

Interagency Guidelines Establishing Information Security Standards

II. Standards for Safeguarding Customer Information

A. Information Security Program. Each bank shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. While all parts of the bank are not required to implement a uniform set of policies, all elements of the information security program must be coordinated.

B. Objectives. A bank's information security program shall be designed to:

1. Ensure the security and confidentiality of customer information;
2. Protect against any anticipated threats or hazards to the security or integrity of such information; and
3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.



16

Interagency Guidelines Establishing Information Security Standards

III. Development and Implementation of Information Security Program

- A. *Involve the Board of Directors*
- B. *Assess Risk*
- C. *Manage and Control Risk*
- D. *Oversee Service Provider Arrangements*
- E. *Adjust the Program*
- F. *Report to the Board*
- G. *Implement the Standards*
- A. *Supplement A (Response Program)*



17

Information Security Program

- **Involve the Board of Directors**
- Assess Risk
- Manage and Control Risk
- Oversee Service Provider Arrangements
- Adjust the Program
- Report to the Board
- Supplement A: Response Program

A. *Involve the Board of Directors.* The board of directors or an appropriate committee of the board of each insured depository institution shall:

1. Approve the institution's written information security program; and
2. Oversee the development, implementation, and maintenance of the institution's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.



18

Information Security Program

- Involve the Board of Directors
- **Assess Risk**
- Manage and Control Risk
- Oversee Service Provider Arrangements
- Adjust the Program
- Report to the Board
- Supplement A: Response Program

- B. Assess Risk.** Each institution shall:
1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.
 2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.
 3. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.



19

Information Security Program

- Involve the Board of Directors
- Assess Risk
- **Manage and Control Risk**
- Oversee Service Provider Arrangements
- Adjust the Program
- Report to the Board
- Supplement A: Response Program

- C. Manage and Control Risk.** Each institution shall:
1. Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the institution's activities. Each institution must consider whether the following security measures are appropriate for the institution and, if so, adopt those measures the institution concludes are appropriate:
 - a. Logical access controls
 - b. Physical access
 - c. Encryption
 - d. Modifications
 - e. Dual control, segregation of duties, background checks
 - f. Monitoring systems
 - g. Response programs
 - h. Continuity / DR



21

Information Security Program

- Involve the Board of Directors
- Assess Risk
- **Manage and Control Risk**
- Oversee Service Provider Arrangements
- Adjust the Program
- Report to the Board
- Supplement A: Response Program

- C. *Manage and Control Risk.* Each institution shall:
2. Train staff to implement the institution's information security program.
 3. Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the institution's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.
 4. Develop, implement, and maintain, as part of its information security program, appropriate measures to properly dispose of customer information and consumer information in accordance with each of the requirements of this paragraph III.



22



23

Information Security Program

- Involve the Board of Directors
- Assess Risk
- Manage and Control Risk
- **Oversee Service Provider Arrangements**
- Adjust the Program
- Report to the Board
- Supplement A: Response Program

D. Oversee Service Provider Arrangements. Each institution shall:

1. Exercise appropriate due diligence in selecting its service providers;
2. Require its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines; and
3. Where indicated by the institution's risk assessment, monitor its service providers to confirm that they have satisfied their obligations as required by paragraph D.2. As part of this monitoring, an institution should review audits, summaries of test results, or other equivalent evaluations of its service providers.



24

Information Security Program

- Involve the Board of Directors
- Assess Risk
- Manage and Control Risk
- Oversee Service Provider Arrangements
- **Adjust the Program**
- Report to the Board
- Supplement A: Response Program

E. Adjust the Program. Each institution shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the institution's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.



25

Information Security Program

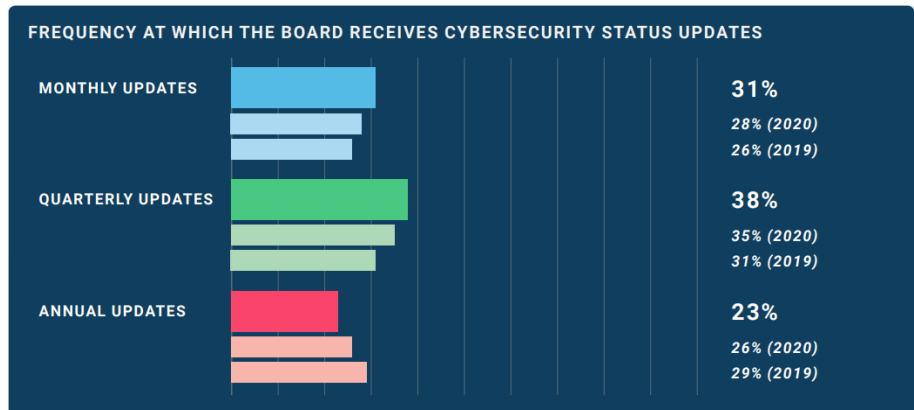
- Involve the Board of Directors
- Assess Risk
- Manage and Control Risk
- Oversee Service Provider Arrangements
- Adjust the Program
- **Report to the Board**
- Supplement A: Response Program

F. Report to the Board. Each institution shall report to its board or an appropriate committee of the board at least annually. This report should describe the overall status of the information security program and the institution's compliance with these Guidelines. The report, which will vary depending upon the complexity of each institution's program should discuss material matters related to its program, addressing issues such as: Risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations, and management's responses; and recommendations for changes in the information security program.



Information Security Program

- Involve the Board of Directors
- Assess Risk
- Manage and Control Risk
- Oversee Service Provider Arrangements
- Adjust the Program
- **Report to the Board**
- Supplement A: Response Program



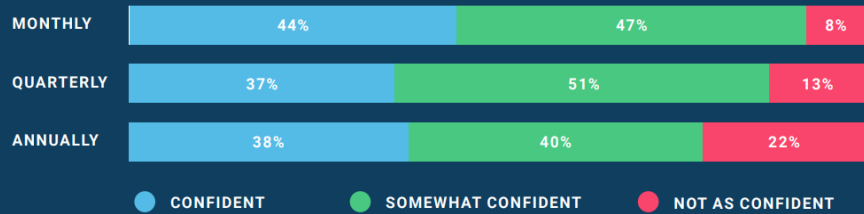
SOURCE: The State of Cybersecurity in the Financial Institution Industry | 2021 Survey Report | Tandem



Information Security Program

- Involve the Board of Directors
- Assess Risk
- Manage and Control Risk
- Oversee Service Provider Arrangements
- Adjust the Program
- **Report to the Board**
- Supplement A: Response Program

CONFIDENCE IN BOARD OF DIRECTORS' UNDERSTANDING OF INSTITUTION'S CYBERSECURITY POSTURE - BASED ON FREQUENCY OF STATUS UPDATES



SOURCE: The State of Cybersecurity in the Financial Institution Industry | 2021 Survey Report | Tandem



28

Information Security Program

- Involve the Board of Directors
- Assess Risk
- Manage and Control Risk
- Oversee Service Provider Arrangements
- Adjust the Program
- Report to the Board
- **Supplement A: Response Program**

- I. Background
- II. Components of a Response Program
- III. Customer Notice
 - A. Standard for Providing Notice
 - B. Content of Customer Notice
 - C. Delivery of Customer Notice



30

Information Security Program

- Involve the Board of Directors
- Assess Risk
- Manage and Control Risk
- Oversee Service Provider Arrangements
- Adjust the Program
- Report to the Board
- Supplement A: Response Program



Risk Management

Risk Management

Agenda

- Information Security Risk Assessment
- Asset Based Risk Assessments
- FFIEC Cybersecurity Assessment Tool



36

Information Security Program

- Involve the Board of Directors
- **Assess Risk**
- Manage and Control Risk
- Oversee Service Provider Arrangements
- Adjust the Program
- Report to the Board
- Supplement A: Response Program

B. *Assess Risk*. Each institution shall:

1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.
2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.
3. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.



38

Information Security Program

- Involve the Board of Directors
- **Assess Risk**
- Manage and Control Risk
- Oversee Service Provider Arrangements
- Adjust the Program
- Report to the Board
- Supplement A: Response Program

Responsibility	Reasonably Foreseeable Internal and External Threats	Data Type		Threat Type			Likelihood of Occurrence (High, Moderate, Low)	Potential Damage to the Bank (Major, Moderate, Minimal)	Adequacy of current policies, procedures, and controls (S=Satisfactory U=Unsatisfactory)	Exposure (High, Moderate, Low)	Current policies, procedures, controls	Department Responsible for Policy & Procedures	Sign off of Senior Mgr over Department Policies and Procedures	Comments
		Personal	Business	Unauthorized Access	Malware	Insider								
1 Compliance Officer; Bank-wide	Loose Lips (Employee Unintentional)	X		X			Low	Moderate	S	Low		HR		
2 Compliance Officer; Bank-wide	Unauthorized disclosure due to files/customer information left on desks	X		X			Moderate	Moderate	S	Low		HR Lending Operations Sales & Service		
3 IT Department	Computer monitors viewable by outsiders	X		X			Low	Minimal	S	Low		HR IT		
4 IT Department	Emails containing customer information or references sent to wrong recipients	X	X	X			Moderate	Moderate	S	Low		IT, HR		
5 Each Department	Disclosures sent to government authorities without following the Right to Financial Privacy (RTFP) Act	X		X			Low	Moderate	S	Low		Account Services HR		
6 Each Department	Sending mail/fax containing customer information to the wrong address	X		X			Low	Moderate	S	Low		IT Account Services Advantage Business Capital HR		
7 Each Department	Inadvertent disclosure to a pretext caller	X		X			Moderate	Moderate	S	Low		IT Account Services Call Center		
8 IT Department	Firewalls prove inadequate (hacker gains access)	X	X	X	X	X	Low	Major	S	Low		IT		



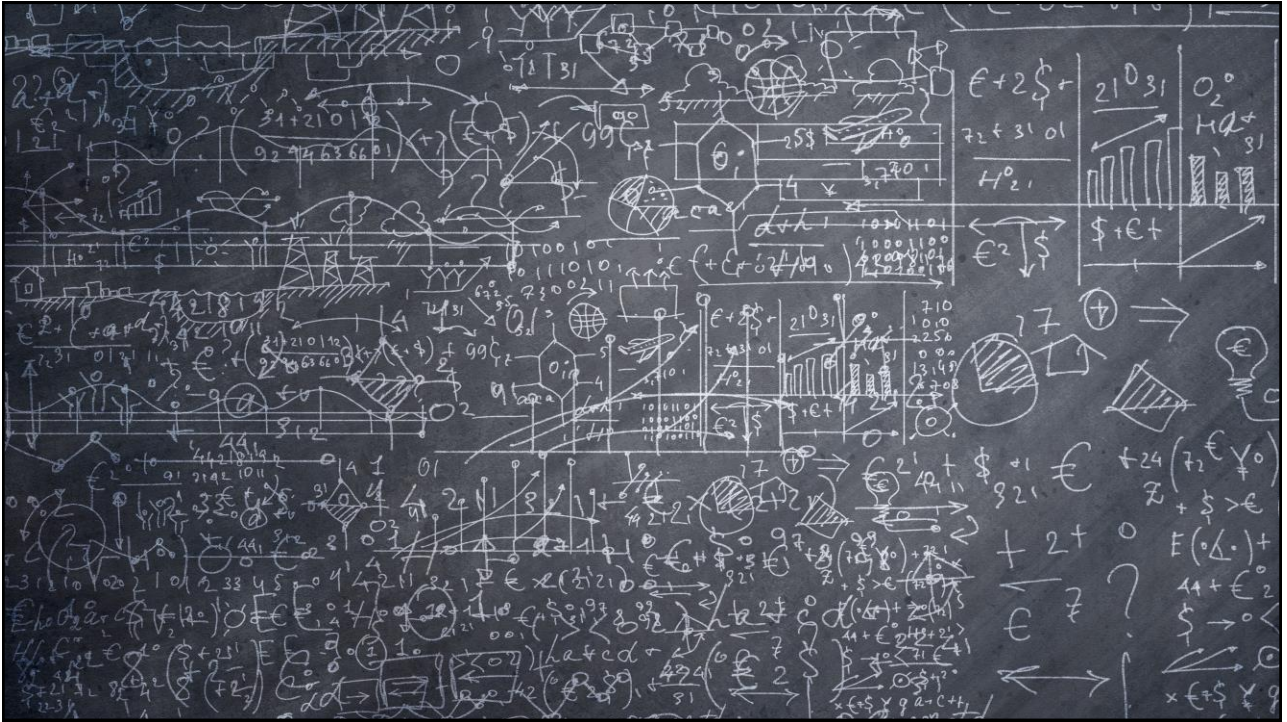
39

Information Security Risk Assessment

1. What is valuable about this risk assessment approach?
2. Are there any challenges with it?



40



41

FFIEC Cybersecurity Assessment Tool
Overview for Chief Executive Officers and Boards of Directors

In light of the increasing volume and sophistication of cyber threats, the Federal Financial Institutions Examination Council¹ (FFIEC) developed the Cybersecurity Assessment Tool (Assessment), on behalf of its members, to help institutions identify their risks and determine their cybersecurity preparedness. The Assessment provides a repeatable and measurable process for institutions to measure their cybersecurity preparedness over time. The Assessment incorporates cybersecurity-related principles from the *FFIEC Information Technology (IT) Examination Handbook* and regulatory guidance, and concepts from other industry standards, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework.²

Benefits to the Institution

For institutions using the Assessment, management will be able to enhance their oversight and management of the institution's cybersecurity by doing the following:

- Identifying factors contributing to and determining the institution's overall cyber risk.
- Assessing the institution's cybersecurity preparedness.
- Evaluating whether the institution's cybersecurity preparedness is aligned with its risks.
- Determining risk management practices and controls that are needed or need enhancement and actions to be taken to achieve the desired state.
- Informing risk management strategies.

CEO and Board of Directors

The role of the chief executive officer (CEO), with management's support, may include the responsibility to do the following:

- Develop a plan to conduct the Assessment.
- Lead employee efforts during the Assessment to facilitate timely responses from across the institution.
- Set the target state of cybersecurity preparedness that best aligns to the board of directors' (board) stated (or approved) risk appetite.
- Review, approve, and support plans to address risk management and control weaknesses.
- Analyze and present results for executive oversight, including key stakeholders and the board, or an appropriate board committee.

¹ The FFIEC comprises the principals of the following: The Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liaison Committee.

² A mapping is available in [Appendix B, Mapping Cybersecurity Assessment Tool to the NIST Cybersecurity Framework](#). NIST reviewed and provided input on the mapping to ensure consistency with Framework principles and to highlight the complementary nature of the two sources.

June 2015 1

Official Title:
FFIEC Cybersecurity Assessment Tool

Release Date:
June 30, 2015

Page Count:
123 Pages

Highlights:

- Overview for Chief Executive Officers and Boards of Directors
- Users Guide
- Inherent Risk Profile
- Cybersecurity Maturity

43

FFIEC Cybersecurity Assessment Tool

Have you completed the
Cybersecurity Assessment
Tool?



44

FFIEC Cybersecurity Assessment Tool

Objectives

- To help institutions identify their risks and determine their cybersecurity maturity.
- The Assessment provides institutions with a repeatable and measurable process to inform management of their institution's risks and cybersecurity preparedness.



45

FFIEC Cybersecurity Assessment Tool

Process

- Part One: Inherent Risk Profile
- Part Two: Cybersecurity Maturity
- Interpreting & Analysis

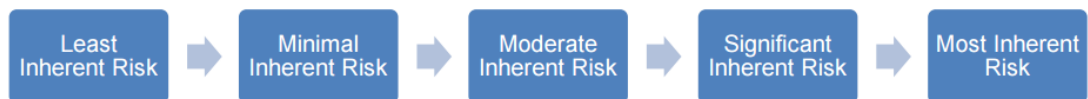


46

Part one: Inherent Risk Profile

Consists of 78 questions across 5 categories:

- Technology and Connection Types
- Delivery Channels
- Online/Mobile Products and Technology Services
- Organizational Characteristics
- External Threats



47

Part one: Inherent Risk Profile

Inherent Risk Profile Excerpt

Activity, Service or Product	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Category: Technologies and Connection Types					
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)



48

Part Two: Cybersecurity Maturity

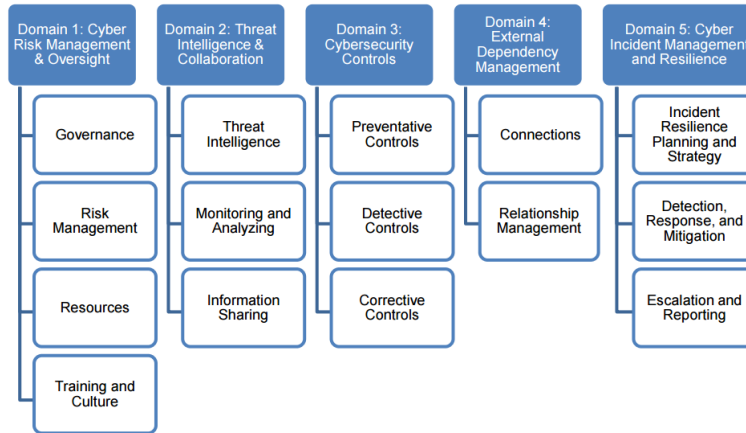
- Cyber Risk Management and Oversight
- Threat Intelligence and Collaboration
- Cybersecurity Controls
- External Dependency Management
- Cyber Incident Management and Resilience



49

Cybersecurity Maturity Model

Domain > Assessment Factor > Contributing Components > Declarative Statements



50

Cybersecurity Maturity Model

Figure 4: Cybersecurity Maturity

		Domain 1: Cyber Risk Management and Oversight	
		Assessment Factor: Governance	
Maturity Level	Component	Y, N	Assessment Factor
OVERSIGHT	Baseline		Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs. (FFIEC Information Security Booklet, page 3) Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. (FFIEC Information Security Booklet, page 6) Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually. (FFIEC Information Security Booklet, page 5) The budgeting process includes information security related expenses and tools. (FFIEC E-Banking Booklet, page 20) Management considers the risks posed by other critical infrastructures (e.g., telecommunications, energy) to the institution. (FFIEC Business Continuity Planning Booklet, page J-12)
	Evolving		At least annually, the board or an appropriate board committee reviews and approves the institution's cybersecurity program. Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity. Cybersecurity tools and staff are requested through the budget process. There is a process to formally discuss and estimate potential expenses associated with cybersecurity incidents as part of the budgeting process.

51

Cybersecurity Maturity Levels

Maturity Levels Defined	
Baseline	Baseline maturity is characterized by minimum expectations required by law and regulations or recommended in supervisory guidance. This level includes compliance-driven objectives. Management has reviewed and evaluated guidance.
Evolving	Evolving maturity is characterized by additional formality of documented procedures and policies that are not already required. Risk-driven objectives are in place. Accountability for cybersecurity is formally assigned and broadened beyond protection of customer information to incorporate information assets and systems.
Intermediate	Intermediate maturity is characterized by detailed, formal processes. Controls are validated and consistent. Risk-management practices and analysis are integrated into business strategies.
Advanced	Advanced maturity is characterized by cybersecurity practices and analytics that are integrated across lines of business. Majority of risk-management processes are automated and include continuous process improvement. Accountability for risk decisions by frontline businesses is formally assigned.
Innovative	Innovative maturity is characterized by driving innovation in people, processes, and technology for the institution and the industry to manage cyber risks. This may entail developing new controls, new tools, or creating new information-sharing groups. Real-time, predictive analytics are tied to automated responses.



52

Cybersecurity Maturity Levels

- All declarative statements in each maturity level, and previous levels, must be attained and sustained to achieve that domain's maturity level.



53

Cybersecurity Maturity Levels

Figure 4: Cybersecurity Maturity

		Domain 1: Cyber Risk Management and Oversight	
		Assessment Factor: Governance	
Maturity Level	Y, N	Assessment Factor	
OVERSIGHT	Baseline	Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs. (FFIEC Information Security Booklet, page 3) Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. (FFIEC Information Security Booklet, page 6) Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually. (FFIEC Information Security Booklet, page 5) The budgeting process includes information security related expenses and tools. (FFIEC E-Banking Booklet, page 20) Management considers the risks posed by other critical infrastructures (e.g., telecommunications, energy) to the institution. (FFIEC Business Continuity Planning Booklet, page J-12)	
	Evolving	At least annually, the board or an appropriate board committee reviews and approves the institution's cybersecurity program. Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity. Cybersecurity tools and staff are requested through the budget process. There is a process to formally discuss and estimate potential expenses associated with cybersecurity incidents as part of the budgeting process.	

54

Cybersecurity Maturity Levels

- All declarative statements in each maturity level, and previous levels, must be attained and sustained to achieve that domain's maturity level.
- While management can determine the institution's maturity level in each domain, the Assessment is not designed to identify an overall cybersecurity maturity level.



55

FFIEC Cybersecurity Assessment Tool

Interpreting & Analyzing

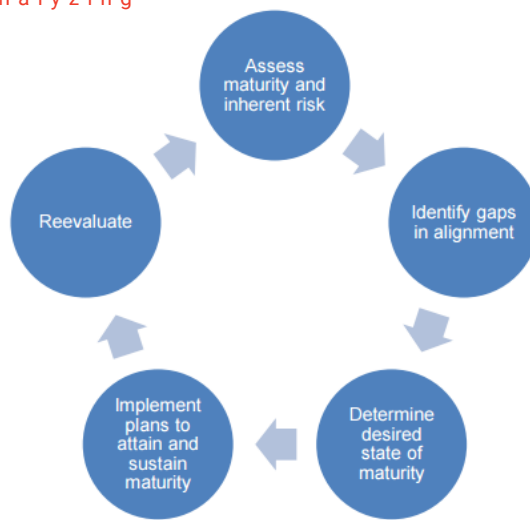
Risk/Maturity Relationship		Inherent Risk Levels				
		Least	Minimal	Moderate	Significant	Most
Cybersecurity Maturity Level for Each Domain	Innovative				■	■
	Advanced			■	■	■
	Intermediate		■	■	■	
	Evolving	■	■	■		
	Baseline	■	■			



56

FFIEC Cybersecurity Assessment Tool

Interpreting & Analyzing

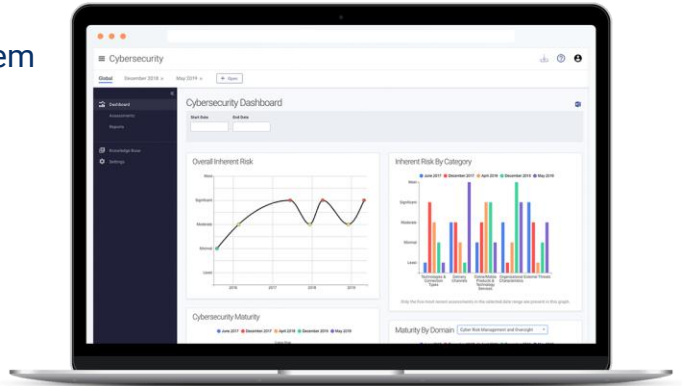


57

Statistics from the CAT

Tandem Cybersecurity Assessment Tool

- More than 1,000 institutions have signed up for the automated Tandem CAT tool
- 776 institutions have completed at least 1 assessment using the tool and opted into anonymous Peer Analysis
- Statistics only include institutions that opted in to participate in anonymous Peer Analysis



58

FFIEC Cybersecurity Assessment Tool

Overall Risk/Maturity

		Inherent Risk				
		Least	Minimal	Moderate	Significant	Most
Cybersecurity Maturity	Innovative	0.13%	0.13%	0.00%	0.00%	0.00%
	Advanced	0.13%	0.26%	0.00%	0.00%	0.00%
	Intermediate	0.39%	2.06%	0.13%	0.00%	0.00%
	Evolving	0.64%	13.53%	1.29%	0.13%	0.00%
	Baseline	9.15%	62.11%	2.58%	0.00%	0.00%
	Sub-Baseline	0.39%	6.57%	0.39%	0.00%	0.00%



59

FFIEC Cybersecurity Assessment Tool

What are some of the benefits of the Assessment Tool?



60

FFIEC Cybersecurity Assessment Tool

What are some of the challenges with the Assessment Tool?



61

FFIEC Cybersecurity Assessment Tool

Overall Risk/Maturity

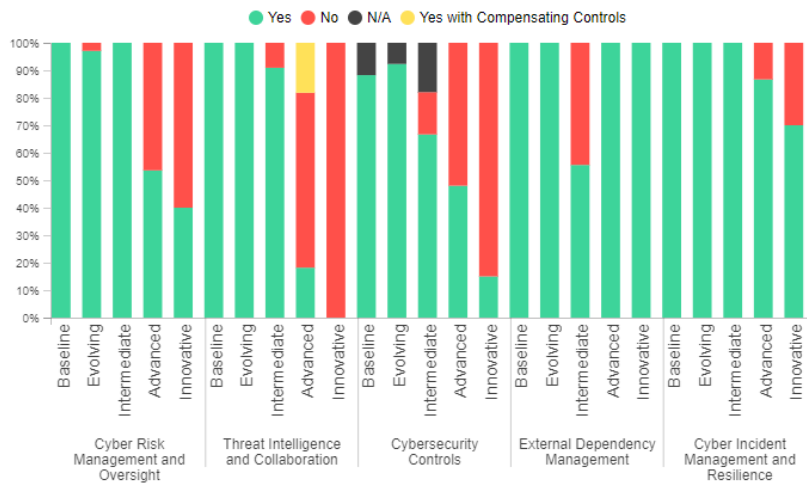
		Inherent Risk				
		Least	Minimal	Moderate	Significant	Most
Cybersecurity Maturity	Innovative	0.13%	0.13%	0.00%	0.00%	0.00%
	Advanced	0.13%	0.26%	0.00%	0.00%	0.00%
	Intermediate	0.39%	2.06%	0.13%	0.00%	0.00%
	Evolving	0.64%	13.53%	1.29%	0.13%	0.00%
	Baseline	9.15%	62.11%	2.58%	0.00%	0.00%
	Sub-Baseline	0.39%	6.57%	0.39%	0.00%	0.00%



62

CAT Maturity Levels by Domain

Source: Peer Analysis Data | Tandem



63

The Role of ISO

65

Information Security Officer(s)

Management should designate at least one **information security officer** responsible and accountable for implementing and monitoring the information security program. Information security management responsibilities may be distributed across various lines of business depending on where the risk decisions are made and the institution's size, complexity, culture, nature of operations, or other factors.

Information security officers should report directly to the board or senior management and have sufficient authority, stature within the organization, knowledge, background, training, and independence to perform their assigned tasks. To ensure appropriate segregation of duties, the **information security officers** should be independent of the IT operations staff and should not report to IT operations management. **Information security officers** should be responsible for responding to security events by ordering emergency actions to protect the institution and its customers from imminent loss of information; managing the negative effects on the confidentiality, integrity, availability, or value of information; and minimizing the disruption or degradation of critical services.

FFIEC Information Security – I.B. Responsibility and Accountability (pg. 5)

66

ISO



A requirement to designate a Corporate Information Security Officer was almost part of the Interagency Guidelines Establishing Information Security Standards per GLBA

incorporations are critical to the system.

4. *Designation of Corporate Information Security Officer.* The Agencies considered whether the Guidelines should require that the bank's board of directors designate a "Corporate Information Security Officer" with the responsibility to develop and administer the bank's information security program. Most of the comment letters requested that this requirement not be adopted because adding a new personnel position would be financially burdensome. The FDIC agrees that a new position with a specific title is not necessary. The final Guidelines do, however, require that the authority for the development, implementation, and administration of the bank's information security program be clearly expressed although not assigned to a particular individual.

5. *Managing and Controlling Risk.*

67

Information Security Officer(s)

6. Determine whether management has designated one or more individuals as an information security officer and determine appropriateness of the reporting line.

FFIEC Information Security – Appendix A, Objective 2, Question 6 (pg. 59)



68

Information Security Officer(s)

1. Evaluate the quality of Board and management oversight of the IT function. Consider the following:
 - Adequacy of the process for developing and approving IT policies
 - Scope and frequency of IT-related meetings
 - Existence of a Board-approved comprehensive information security program
 - Designation of an individual or committee to oversee the information security program, including cybersecurity
 - Composition of IT-related committees (e.g., Board, senior management, business lines, audit, and IT)

InTREx – Management, Procedure 1 (pg. 3)



69

Information Security Officer(s)

Qualities

Sufficient authority 01

Stature within the organization 02

Knowledge 03

04 Background

05 Training

06 Independence



70

Information Security Officer(s)

Qualities



- Sufficient authority
- Stature within the organization



- Stature within the organization
- Independence



- Knowledge
- Background
- Training



- Stature within the organization
- Knowledge
- Background



71

ISO Independence in Guidance

“To ensure independence, the CISO should report directly to the board, a board committee, or senior management and not IT operations management.”

https://ithandbook.ffiec.gov/media/274809/ffiec_itbooklet_management.pdf

“Information security officers should report directly to the board or senior management... To ensure appropriate segregation of duties, the information security officers should be independent of the IT operations staff and should not report to IT operations management.”

https://ithandbook.ffiec.gov/media/274793/ffiec_itbooklet_informationsecurity.pdf




72

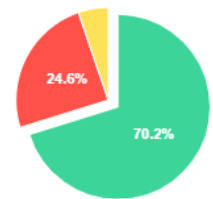


73

ISO Independence

1. The cybersecurity function has a clear reporting line that does not present a conflict of interest.

- Yes 70.20% 
- Yes with Compensating Controls 5.24%
- No 24.55%

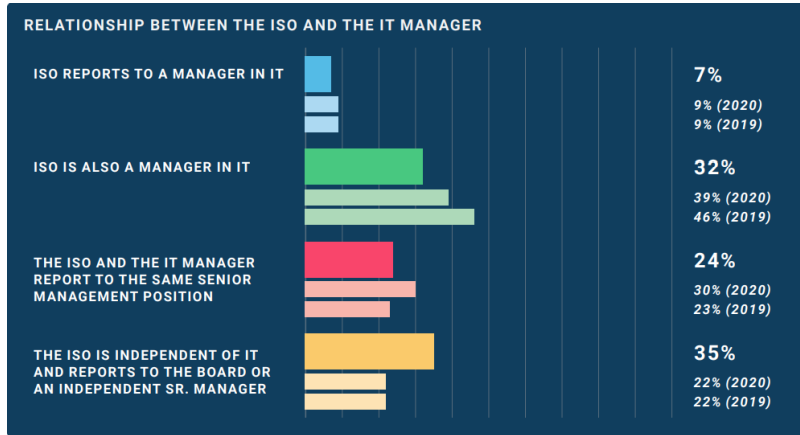


SOURCE: Peer Analysis Data | Cybersecurity Assessment Tool | Tandem



74

ISO Independence

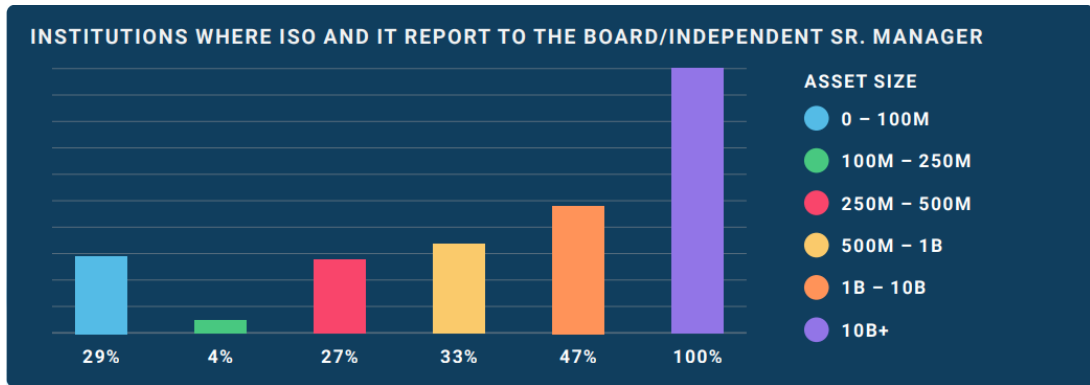


SOURCE: Tandem 2021 State of Cybersecurity in the Financial Institution Industry



75

ISO Independence



SOURCE: Tandem 2021 State of Cybersecurity in the Financial Institution Industry



76



TAKE THE SURVEY

THE STATE OF CYBERSECURITY

Complete our survey to be entered to win an Amazon gift card

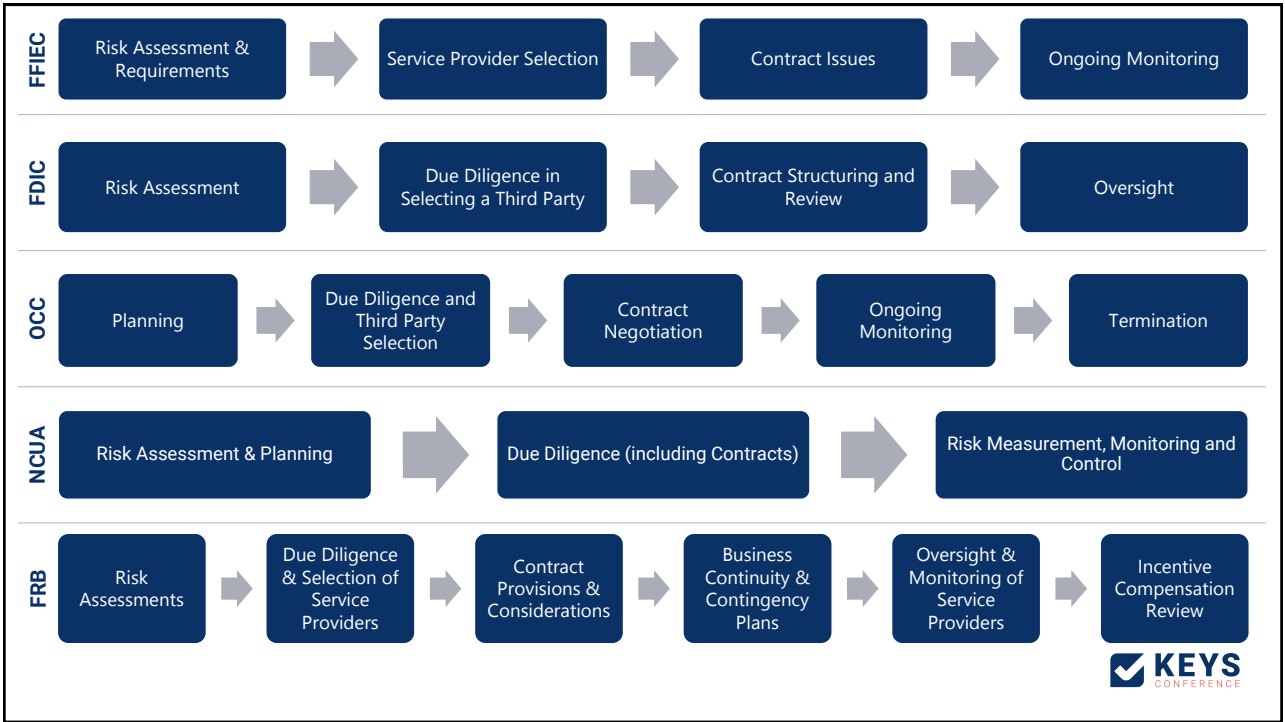
<https://tandem.app/survey>

77

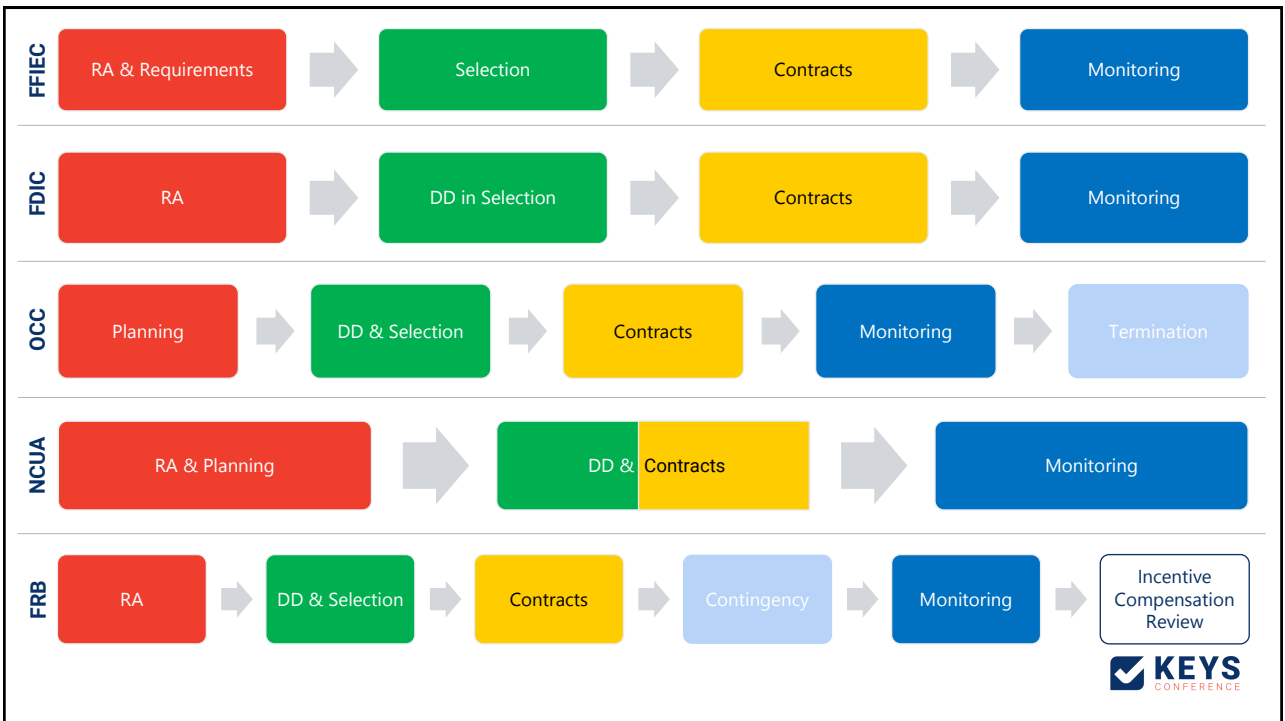


Vendor Management

78



79



80



81

Planning & Risk Assessment

Definition of **Business Requirements** may include:

1. Scope and nature
2. Standards and service levels
3. Minimum acceptable service provider characteristics
4. Monitoring and reporting
5. Transition requirements
6. Contract duration, termination, and assignment
7. Contractual protections against liability

FFIEC Outsourcing Technology Services Booklet (pg. 6-7)



82

Due Diligence & Selection

REQUEST FOR PROPOSAL

RFP Goal: Determine if the vendor can meet your needs, including:

- the institution's objectives
- the scope and nature of the work to be performed
- the expected production service levels
- delivery timelines, measurement requirements, and control measures
- the institution's expectations for security, business continuity, and change control

“A financial institution should generate the RFP from the information developed during the requirements definition phase.”

FFIEC Outsourcing Technology Services Booklet



83

Due Diligence & Selection

How do you know which vendors need to provide which documents?



84



STOP USING THE BUCKET METHOD

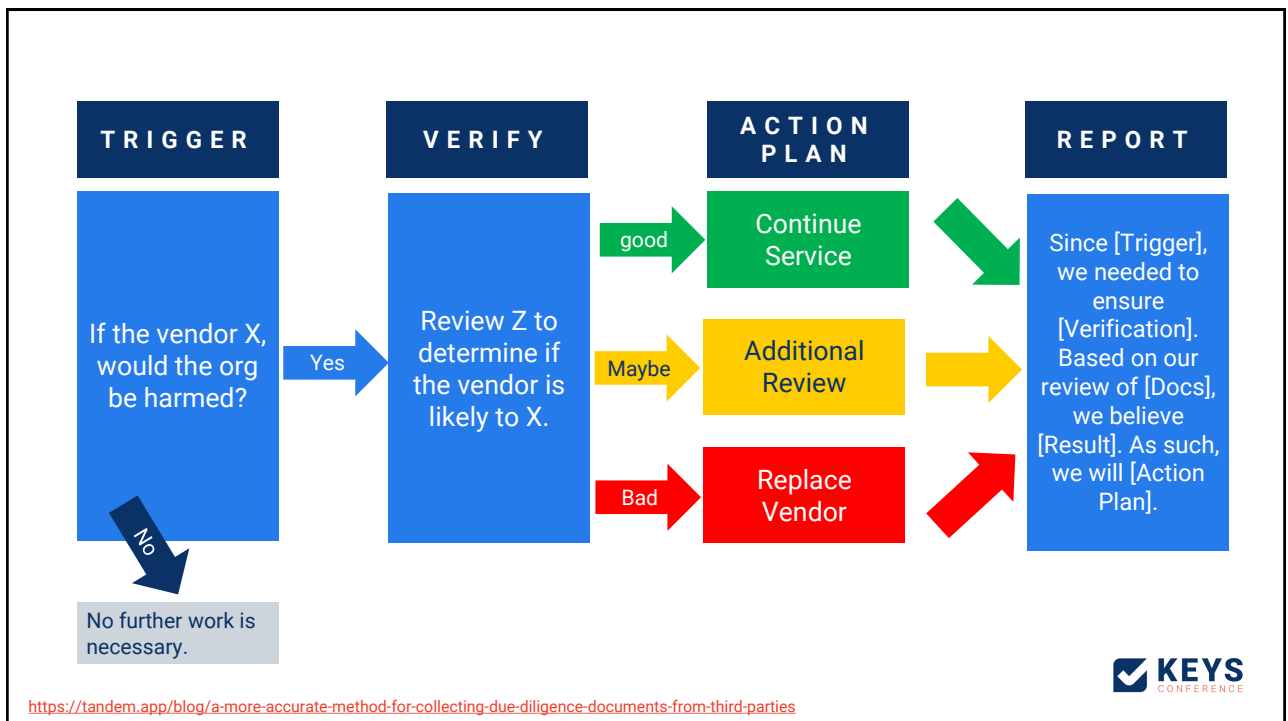
#emptythebucket

Problems created by this method:

1. Unnecessary document exceptions
2. Missed relevant documents



85



86

Read more in Tandem Knowledge Base.



[Review Template: BCP](#)

A BCP Review template is included with Tandem Vendor Management. This article provides a question on the BCP Review.

[Review Template: Financial Statement](#)

Review this article to learn how to utilize the Financial Statement Review template in Vendor Management.

[Review Template: FinTech](#)

A FinTech Review template is included with Tandem Vendor Management. This article provides a question on the FinTech Review.

[Review Template: Security Testing](#)

A Security Testing Review template is included with Tandem Vendor Management to help with security testing.

[Review Template: SOC Report](#)

A SOC Report review template is included with Tandem Vendor Management. This article provides a question on the SOC Report Review.

87

What are some of your frustrations trying to get due diligence documents?



88

Contract Structure & Review

What is in a Service Level Agreement (SLA)?

1. Availability and timeliness of services
2. Confidentiality and integrity of data
3. Change control
4. Security standards compliance
5. Help desk support

According to the FFIEC, SLAs define:

1. **Requirements the vendor is expected to meet.**
2. **Penalties if the vendor cannot meet those requirements.**

FFIEC Outsourcing Technology Services Booklet (pg. 15)



89

Oversight & Monitoring



90

Continuity & Termination

What questions the Termination Continuity Plan will answer:

- Is there an exit strategy?
- Is there a cancellation clause?
- How can you get data out?
- What form will the data be in?
- Will residual data be left with the provider?
- How long will it take?
- Will there be downtime?



91



92



Business Continuity & Incident Management

93

Business Continuity

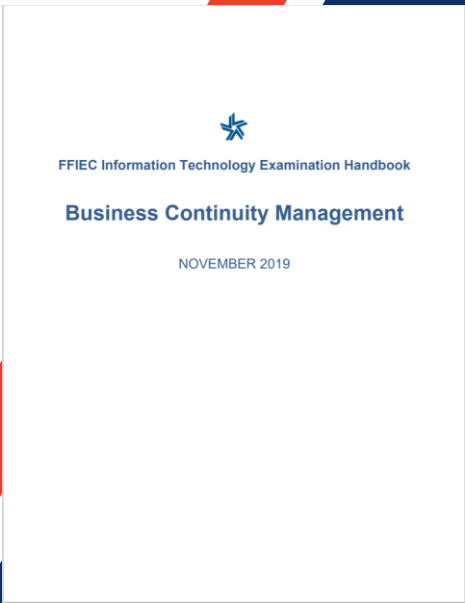
“C.1.h. Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures”

- FDIC - 12 CFR Part 364 Appendix B III C 1 h
- OCC - 12 CFR Part 30 Appendix B III C 1 h
- FRB - 12 CFR Part 208 Appendix D-2 III C 1 h
- NCUA – 12 CFR Part 748 Appendix A III C 1 h

Interagency Guidelines Establishing Information Security Standards



94




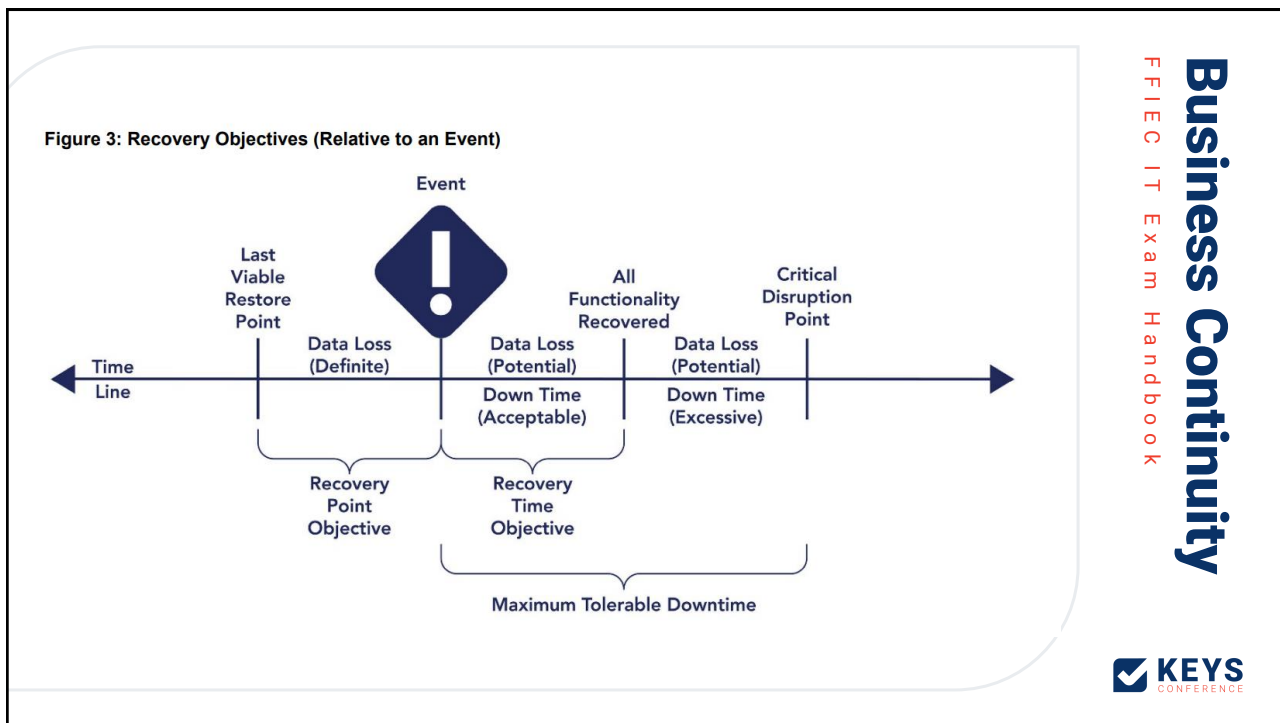
Official Title:
 FFIEC Information Technology Examination Handbook, Business Continuity Management Booklet

Release Date:
 November 2019

Agencies:

- FDIC
- Federal Reserve
- NCUA
- OCC
- CFPB





Ransomware BCP Tabletop Test

- How would we detect a ransomware attack?
- What decisions would need to be made, by whom, and at what point in time?
- How would we recover?
- Would we ever consider paying the ransom?
- Could our backups get infected?
- Who would be needed during recovery?
- How long would it take to recovery?
- How would the incident be documented? By whom?



98

Incident Management

Supplement A to Appendix B - Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

- FDIC - 12 CFR Part 364 Appendix B Supplement A
- OCC - 12 CFR Part 30 Appendix B Supplement A
- FRB - 12 CFR Part 208 Appendix D-2 Supplement A
- NCUA – 12 CFR Part 748 Appendix A Supplement A

Interagency Guidelines Establishing Information Security Standards



100

Components of a Response Program

1. At a minimum, an institution's response program should contain procedures for the following:
 - a. Assess
 - b. Notifying primary Federal regulator
 - c. File a SAR
 - d. Contain and control the incident
 - e. Notifying customers when warranted.

Interagency Guidelines Establishing Information Security Standards



101

Components of a Response Program

2. Where an incident of unauthorized access to customer information involves customer information systems maintained by an institution's service providers, **it is the responsibility of the financial institution to notify the institution's customers and regulator.** However, an institution may authorize or contract with its service provider to notify the institutions' customers or regulator on its behalf.

Interagency Guidelines Establishing Information Security Standards



102

Sensitive Customer Information

According to GLBA, what constitutes sensitive customer information?



103

Sensitive Customer Information

- A customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number
- Password that would permit access to the customer's account
- Any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name or password or password and account number

Interagency Guidelines Establishing Information Security Standards



104

Customer Notice

Is there anything that would prevent us from notifying customers of a breach immediately?



105

Customer Notice

Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation.

Interagency Guidelines Establishing Information Security Standards



106

Content of Customer Notice

- Notice should be clear and conspicuous
- Describe incident and type of customer information compromised
- Explain what the institution has done to protect the customer's information
- Recommend that the customer review account information and inform the institution of any suspicious activity
- Describe fraud alerts and explain how customers can place fraud alerts in their consumer reports
- Explain how customers can obtain a free credit report and recommend customers periodically obtain and review credit reports for fraudulent activity
- Provide information about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft

Interagency Guidelines Establishing Information Security Standards



108

Delivery of Customer Notice

Customer notice should be delivered in any manner designed to ensure that a customer can reasonably be expected to receive it. For example, the institution may choose to contact all customers affected by telephone or by mail, or by electronic mail for those customers for whom it has a valid email address and who have agreed to receive communications electronically.

Interagency Guidelines Establishing Information Security Standards



109

Exam Finding Discussion



- During an IT exam, the examiner discovers you had an incident where you accidentally sent one customer another customer's personal information.
- To respond to the incident, your institution personally called both customers to explain the situation.
- The examiner says you should have written each customer rather than called and is going to write this up as a "violation" per GLBA.
- Should this be a violation, why or why not?



110

H.R. 2471

One Hundred Seventeenth Congress
of the
United States of America

AT THE SECOND SESSION

Began and held at the City of Washington on Monday,
the third day of January, two thousand and twenty-two

In Act

Making consolidated appropriations for the fiscal year ending September 30, 2022, and for providing emergency assistance for the situation in Ukraine, and for other purposes.

As it enacted by the Senate and House of Representatives of the United States of America in Congress assembled.

SECTION I. SHORT TITLE.

This Act may be cited as the "Consolidated Appropriations Act, 2022."

SEC. 2. TABLE OF CONTENTS.

Sec. 1. Short title.

Sec. 2. Table of contents.

Sec. 3. Enactment statement.

Sec. 4. Department of appropriations.

Sec. 5. Appropriation to transportation.

DIVISION A—AGRICULTURE, RURAL DEVELOPMENT, FOOD AND TRUCK ADMINISTRATION, AND RELATED AGENCIES APPROPRIATIONS ACT, 2022

Title I—Agricultural Programs

Title II—Food Production and Conservation Programs

Title III—Rural Development Programs

Title IV—Domestic Food Programs

Title V—Energy, Department of Food and Drug Administration

Title VI—Related Agencies and Food and Drug Administration

Title VII—General Provisions

DIVISION B—COMMERCE, JUSTICE, SCIENCE, AND RELATED AGENCIES APPROPRIATIONS ACT, 2022

Title I—Department of Commerce

Title II—Department of Justice

Title III—Science

Title IV—Related Agencies

Title V—General Provisions

DIVISION C—DEPARTMENT OF DEFENSE APPROPRIATIONS ACT, 2022

Title I—Military Personnel

Title II—Operations and Maintenance

Title III—Procurement

Title IV—Research, Development, Test and Evaluation

Title V—Acquisition and Management Funds

Title VI—Other Department of Defense Programs

Title VII—General Provisions

DIVISION D—ENERGY AND WATER DEVELOPMENT AND RELATED AGENCIES APPROPRIATIONS ACT, 2022

Title I—Curtis E. Emmerich Chair

Title II—Department of the Interior

Title III—Department of Energy

Official Title:
Consolidated Appropriations Act

Release Date:
March 2022

Key Details:

- A requirement to report cyber incidents to the CISA within 72 hours.
- A requirement to report making a ransomware payment to the CISA within 24 hours.
- The ACT tasks the CISA Director to partner with other agencies to publish a Notice of Proposed Rulemaking within 24 months.



111



TAKE THE SURVEY

THE STATE OF CYBERSECURITY

Complete our survey to be entered to win an Amazon gift card

<https://tandem.app/survey>

112



IT Audits, Testing, & Assurance

113

IT Audits, Testing, & Assurance



114

IT Audits, Testing, & Assurance

- Types of Tests & Evaluations
- Audit Plan / Risk Assessment
- Independence
- 3rd Party Auditors / Engagement Letter
- Reporting & Exception Tracking
- IT Exams

Source: FFIEC IT Exam Handbook, Information Security Booklet



115

Types of Tests & Evaluations



Source: FFIEC IT Exam Handbook, Information Security Booklet



117

Audit Plan / Risk Assessment

4. Evaluate the IT audit risk assessment process. Consider the following:
- Identification of a comprehensive IT audit universe
 - Utilization of a risk scoring/ranking system to prioritize audit resources
 - Establishment of Board-approved audit cycles

Decision Factor 2 ▲


Source: InTREx



118

Audit Plan / Risk Assessment

Why do we conduct an audit risk assessment?

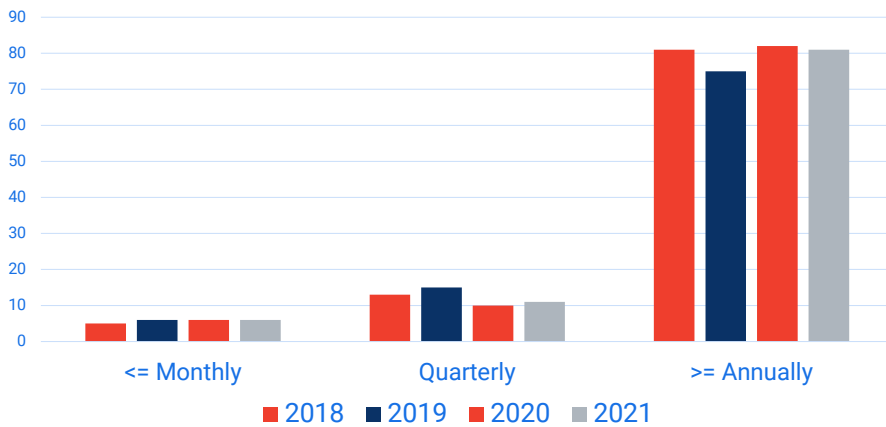




119

Frequency

IT Audits



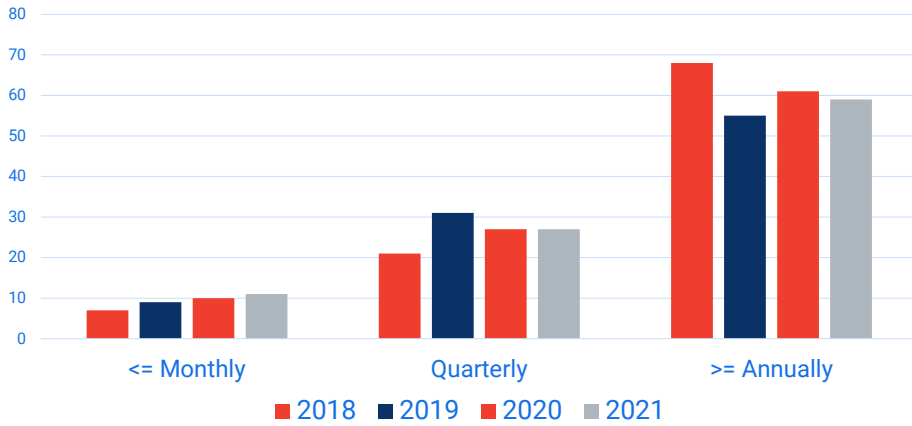
SOURCE: Tandem 2021 State of Cybersecurity in the Financial Institution Industry



122

Frequency

External Penetration Tests



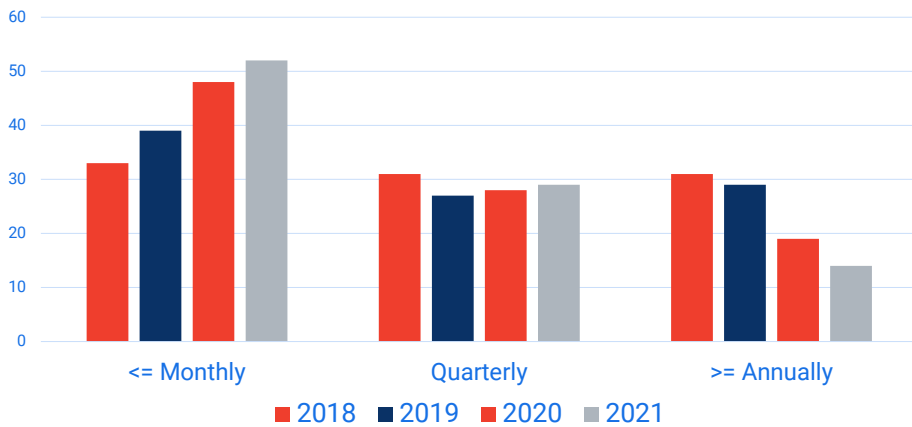
SOURCE: Tandem 2021 State of Cybersecurity in the Financial Institution Industry



123

Frequency

Social Engineering Tests



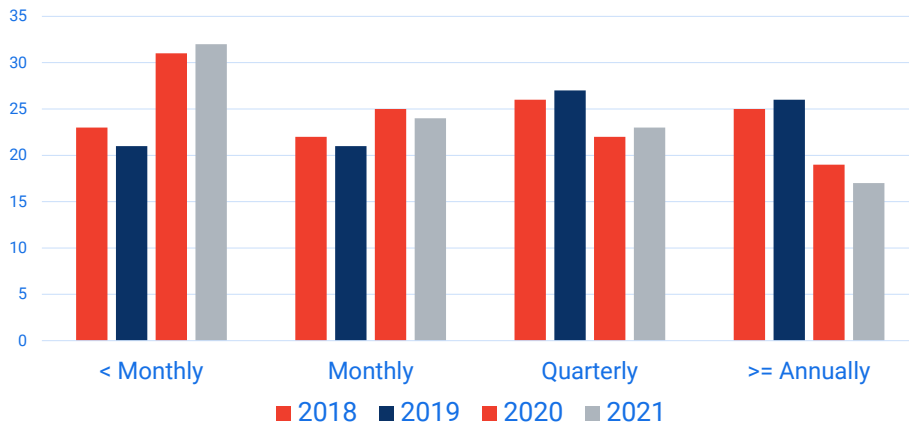
SOURCE: Tandem 2021 State of Cybersecurity in the Financial Institution Industry



124

Frequency

Vulnerability Scanning



SOURCE: Tandem 2021 State of Cybersecurity in the Financial Institution Industry



125

Independence



Independent tests have the potential to reduce bias, increase capabilities, and increase knowledge about threats and technologies. Independence gives credibility to the test results. To be considered independent, testing personnel should not be responsible for the design, installation, maintenance, and operation of the tested system, or the policies and procedures that guide its operation.

SOURCE: FFIEC IT Exam Handbook, Information Security Booklet



126

3rd Party Auditors / Engagement Letter

Source: (1) FFIEC IT Exam Handbook, Audit Booklet (2) InTREx

- Expectations and responsibilities
- Scope of the audit
- Objectives
- Cost of work
- Resource requirements
- Audit timeframe
- Resulting reports
- Institution access to audit workpapers

SOURCES: (1) FFIEC IT Exam Handbook, Audit Booklet (2) InTREx



127

Reporting & Exception Tracking

- Audit rating
- Description of controls
- Observations / findings
 - Risk level
 - References to guidance or standards
 - Observation details
 - Repeat finding?
 - Recommendation for remediation
 - Remediation cost estimate
 - Bank response
- Supporting work program / work papers



129

Reporting & Exception Tracking

Reference	Risk Rating	Cost Estimate	Finding	Responsibility	Target Date	Formal Response	Completion Date
101-Oct21	High	Low	Fire extinguishers do not comply with safety code	Joe Banker	11/31/2021	Management has hired a company to inspect all fire extinguishers quarterly.	11/20/2021



130

Reporting & Exception Tracking

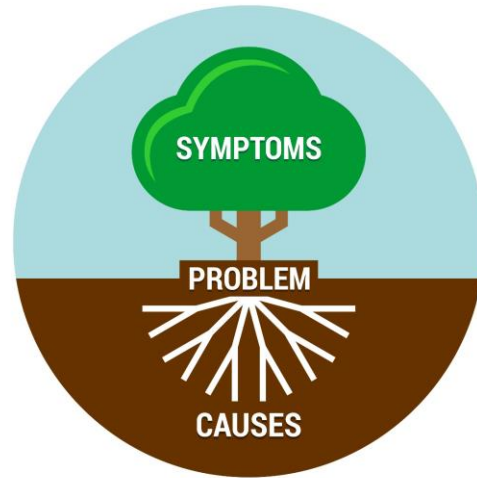
“ The audit department should send IT audit reports to appropriate management and directly to the board of directors or a designated board committee.

SOURCE: FFIEC IT Exam Handbook, Management Booklet



131

Reporting & Exception Tracking



132

Root Cause Discussion

During your audit, you discover the following terminated employees still have active accounts. What are some possible root cause issues to be resolved?

Scenario 1:

- 2 out of 20 domain accounts
- 3 out of 20 core accounts
- 4 out of 20 accounts for SaaS1
- 18 out of 20 accounts for SaaS2
- 7 out of 20 accounts for local app1

Scenario 2:

- 0 out of 20 domain accounts
- 0 out of 20 core accounts
- 0 out of 20 accounts for SaaS1
- 19 out of 20 accounts for SaaS2
- 0 out of 20 accounts for local app1



133

Risk Acceptance Discussion



- During an audit in year 1, you report a finding.
- The institution formally accepts the risk of the finding.
- You are conducting an audit in year 2 and note the same observation.
- Would this be written as a “finding” in your report? Why or why not?



134

IT Exam Work Programs

- InTREx (FDIC, FRB, many states)
- InTREx-CU / “New Part 748” (NCUA)
- Community Bank Supervision Handbook (OCC)
- FFIEC IT Examination Handbook (all agencies may reference)



135

September 11, 2018

Interagency Statement Clarifying the Role of Supervisory Guidance

The Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, and Office of the Comptroller of the Currency (together, the "prudential agencies") are responsible for promoting safer and sounder and effective consumer compliance at supervised institutions. The Bureau of Consumer Financial Protection ("Bureau," and, with the prudential agencies, the "agencies") is generally responsible for regulating the offering and provision of consumer financial products or services under the federal consumer financial laws. The agencies are issuing this statement to explain the role of supervisory guidance and to describe the agencies' approach to supervisory guidance.

Difference between supervisory guidance and laws or regulations

The agencies issue various types of supervisory guidance, including interagency statements, advisories, bulletins, policy statements, questions and answers, and frequently asked questions, to their respective supervised institutions. A law or regulation has the force and effect of law.¹ Unlike a law or regulation, supervisory guidance does not have the force and effect of law, and the agencies do not take enforcement actions based on supervisory guidance. Rather, supervisory guidance outlines the agencies' supervisory expectations or priorities and articulates the agencies' general views regarding appropriate practices for a given subject area. Supervisory guidance often provides examples of practices that the agencies generally consider consistent with safety-and-soundness standards or other applicable laws and regulations, including those designed to protect consumers. Supervised institutions at times request supervisory guidance, and such guidance is important to provide insight to industry, as well as supervisory staff, in a transparent way that helps to ensure consistency in the supervisory approach.

Ongoing agency efforts to clarify the role of supervisory guidance

The agencies are clarifying the following policies and practices related to supervisory guidance:

- The agencies intend to limit the use of numerical thresholds or other "bright-lines" in describing expectations in supervisory guidance. Where numerical thresholds are used, the agencies intend to clarify that the thresholds are exemplary only and not suggestive of requirements. The agencies will continue to use numerical thresholds to talk, and otherwise make clear, the applicability of supervisory guidance or programs to supervised institutions, and as required by statute.


¹ Government agencies issue regulations that generally have the force and effect of law. Such regulations generally take effect only after the agency proposes the regulation to the public and responds to comments on the proposal in a final rulemaking document.

Official Title:
Interagency Statement Clarifying the Role of Supervisory Guidance

Release Date:
September 11, 2018

Agencies:

- FDIC
- Federal Reserve
- NCUA
- OCC
- CFPB



136

Interagency Statement Clarifying the Role of Supervisory Guidance



Examiners will not criticize a supervised financial institution for a "violation" of guidance. Rather, any citations will be for violations of law, regulation, or non-compliance with enforcement orders or other enforceable conditions.



137



Education and Reporting

138



139

Facilitating Change

How to get Employee Buy-In



140

How would you risk rate this for yourself?

Home Security



High (3)

Medium (2)

Low (1)



141

5 Steps

1. Believe
2. Gather Support
3. Individualize
4. Reinforce
5. Appreciate



142

Believe



143

Believe in

Good of the Mission



Staff's Ability to Improve



Gather Support



You are contagious | Vanessa Van Edwards | TEDxLondon



146

Gather Support



147

Leadership Language

STATS

Source	Statistic
ABC News	Malicious emails are up 600% in 2021
Business Insider	The largest ransomware payout to date has been \$40 million
National Security Institute	The average ransomware payout has gone from \$5,000 to \$200,000 in the past 4 years
Coveware	The average downtime resulting from a ransomware attack is 21 days



EVIDENCE

In past 12 months

- # failed tests
- # repeat offenders
- # users with poor passwords
- # users with unnecessary access
- # end-user specific audit findings



MONEY

- If you are missing certain controls will your insurance still payout?
- If you show up in a Google search how will that impact your reputation?
- How much will a breach cost you?
- How long will your network be down due to a breach?



148

Individualize



149

ALBERT EINSTEIN

German-born theoretical physicist



“If you can’t explain it simply, you don’t understand it well enough.”



150



Science of Learning

<https://deansforimpact.org/resources/the-science-of-learning/>



151

MAKE IT BUILD

MAKE IT SPECIFIC

MAKE IT CONNECTED



152

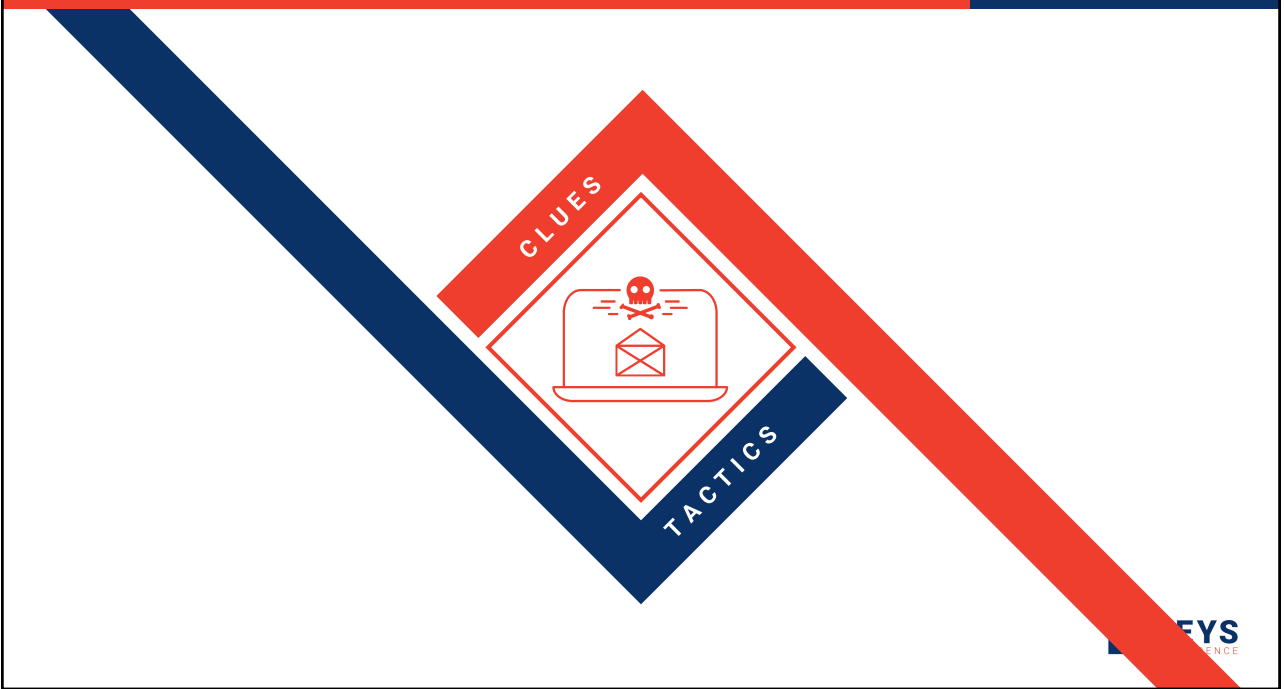
PHISHING

FFIEC INFORMATION SECURITY BOOKLET

"A digital form of social engineering that uses authentic-looking – but bogus – email to request information from users or direct them to fake websites that request information."



153



154

When You Receive an Email...

BEWARE OF TACTICS

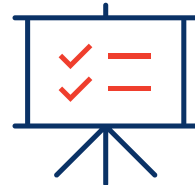
- Urgency
- Loss
- Authority
- Familiarity
- Reciprocation
- Popularity

CHECK FOR CLUES

- Links and Attachments
- Unfamiliar Sender
- Unexpected Email
- Errors
- Familiar, yet Unusual
- Personal Topics

155

Delivery Options

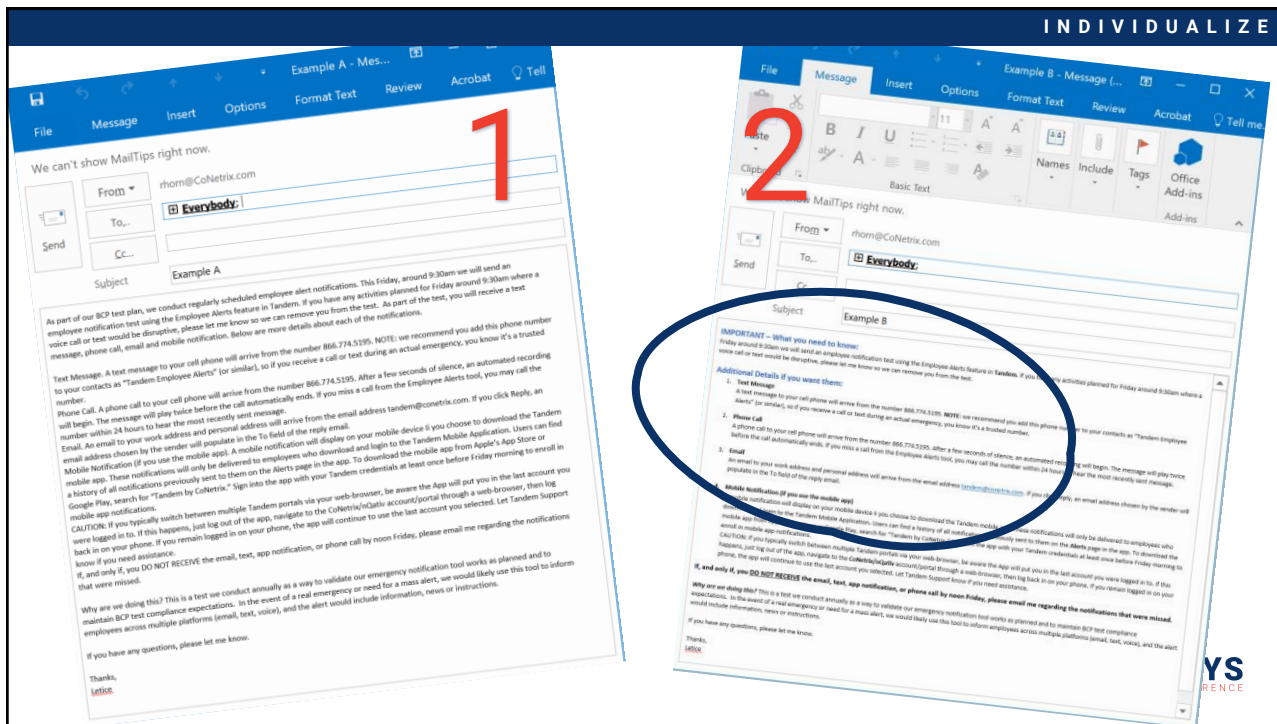




158



159



160

INDIVIDUALIZE

AutoSave Off Send List - Read-Only Search (Alt+Q) Leticia Said

File Home Insert Page Layout Formulas Data Review View ActivityHD Help Table Design

Clipboard Font Alignment Number Styles Cells Editing Analysis Sensitivity

User	Last Name	Email	Department	Group	other people
Leticia	Said	lsaid@conetrix.com	CNX	leader	who don't see the effort and time put into taking care
				young adult	who are less at a place in life for growth
				long-time employee	who don't see the growth the company has experienc
				team lead	who don't have people they are responsible for
				relational support person	who spend their time in more technical roles
				young adult	who are less at a place in life for growth
				young adult	who are less at a place in life for growth
				relational sales person	who spend their time in more technical roles
				long-time employee	who don't see the growth the company has experienc
				a person who has experienced different roles	who have only ever known one job or department
				person who has had a career outside of CoNetrix	who have only known one company
				person who has had a career outside of CoNetrix	who have only known one company
				long-time employee	who don't see the growth the company has experienc
				general manager	who don't see the effort and time put into taking care
				relational sales person	who spend their time in more technical roles
				supervisor	who don't see the effort and time put into taking care
				marketing minded individual	who are siloed in their specific task or division
				remote	who work from the main office

161

MAKE IT BUILD

MAKE IT SPECIFIC

MAKE IT CONNECTED



162

Reinforce



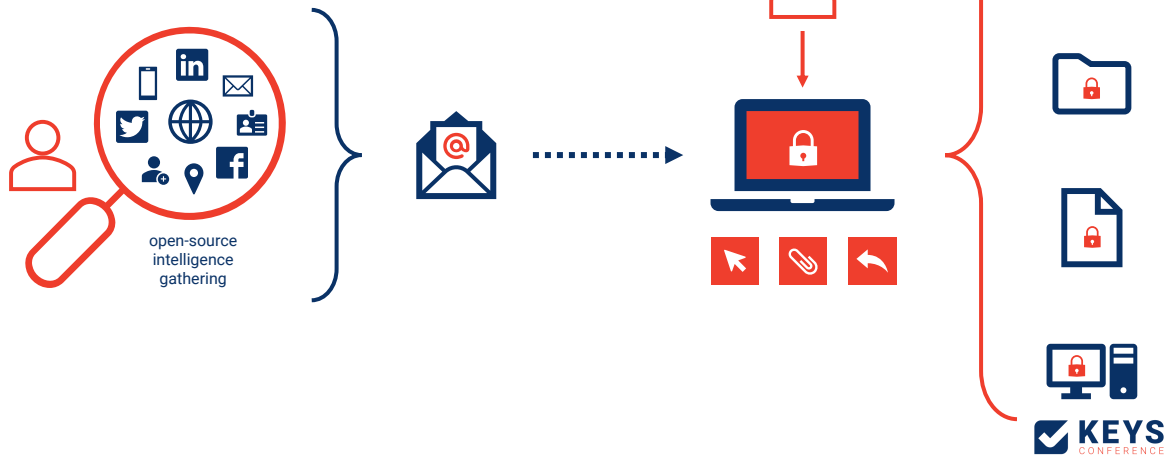
163

MAKE IT MEANINGFUL
MAKE IT FREQUENT



164

Sample Phishing Education



165

FBI: Hackers Are Compromising Legit QR Codes to Send You to Phishing Sites

The scheme exploits how QR codes have grown in popularity during the pandemic.



By Michael Kan

January 19, 2022



(Photo by Noam Galai/Getty Images)



<https://www.pcmag.com/news/fbi-hackers-are-compromising-legit-qr-codes-to-send-you-to-phishing-sites>

166

HIGHER
or
LOWER



167

SCIENCE OF: RETAINING NEW INFORMATION

REINFORCE

The average downtime due to ransomware attacks.

~~7 DAYS~~
21 DAYS

<https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf>



KEYS CONFERENCE

168

SCIENCE OF: SOLVING PROBLEMS

REINFORCE

MAKE IT AUTOMATIC

MAKE IT ABOUT IMPROVEMENT

KEYS CONFERENCE

169




170

SCIENCE OF: SOLVING PROBLEMS

REINFORCE

MAKE IT AUTOMATIC

MAKE IT ABOUT IMPROVEMENT



171

GEORGE BERNARD SHAW

Irish playwright



“The single biggest problem in communication is the illusion that it has taken place.”



172

From: John Doe <jdoo@tandem.com>

Wrong domain

Sent: Tuesday, March 29th, 2022 8:00 AM

Unfamiliar sender

To: Leticia Saiid <lsaiid@conetrix.com>

Subject: FWD: From Tandem Conference

Odd Subject

Hello valued member,

Impersonal Salutation

I hope you are as excited for the event as I am.

Errors

Here is a copy of your event registration... Pls review & fill out attached form BEFORE 12:00 TODAY.

Urgency

[Reg0329.html \(7KB\)](#)

Links & Attachments



173

Appreciate



174

APPRECIATE

Appreciate When You See a Shift in

Habits



Attitudes



175

MAKE IT ABOUT GROWTH

MAKE IT REWARDED



176

Recap

1. B
2. G
3. I
4. R
5. A



177



178



179