

CHRISTOPHER HIDALGO

The Lazy Auditor's Guide to Regulation



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



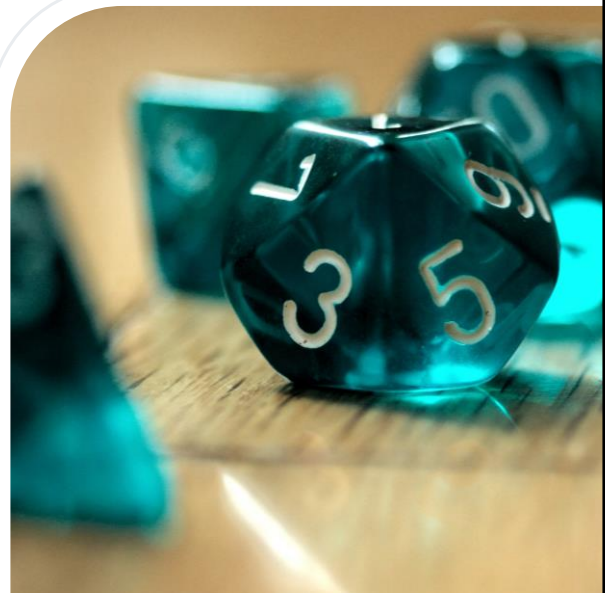
Christopher Hidalgo

ITIL-F, Audit and Security
Consultant



3

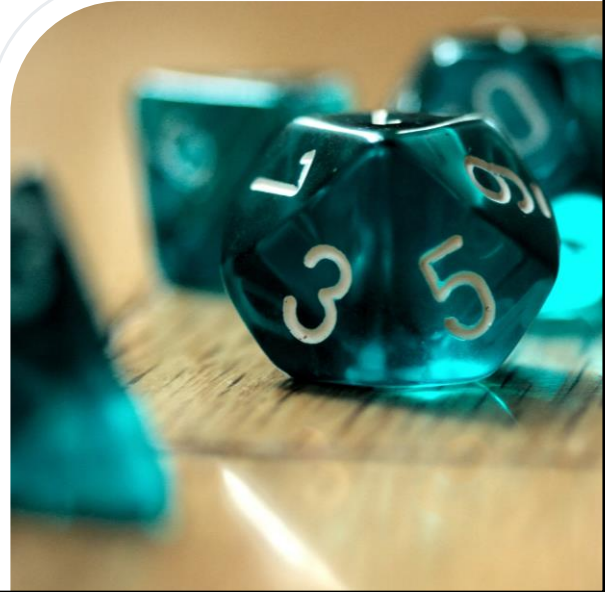
What do you mean by “lazy auditor’s guide”?



4



What do you mean by “resourceful auditor’s guide”?



5

This Guide is for...

HERE'S THE PLAN

- Security Practitioners new to Financial Institutions
- Governance, Risk, and Compliance (GRC) Analysts
- CIOs and CTOs that assume the ISO role
- The Compliance Officer with too many hats



6

Agenda

HERE'S THE PLAN

- Regulation vs. Guidance vs. Frameworks
- The FFIEC Approach
- The NIST Approach
- The Community Approach
- Recap



7



Regulation vs. Guidance vs. Frameworks

THE LAZY AUDITOR'S GUIDE TO REGULATION

8

Definitions



REGULATION VS. GUIDANCE VS. FRAMEWORKS

Regulation

Listed in the Code of Federal Regulations (CFR).

Rules that must be followed by financial institutions with examination.

Guidance

Provided by the Federal Financial Institutions Examination Council (FFIEC) specifically for financial institutions but are not regulation.

Close interpretations to what examiners evaluate to meet regulatory compliance.

Frameworks

Often provided by vendors, government entities, or independent organizations.

Provide recommendations based on industry best practices.

9

The CFR Interagency Guidelines Simplified

REGULATION VS. GUIDANCE VS. FRAMEWORKS

1. A written information security program/strategy
2. Risk assessment and management
3. Access controls for customer information systems
4. Physical access control for areas containing customer information
5. Encryption of customer information either stored or transmitted electronically
6. Change-control procedures
7. Dual control procedures, segregation of duties, and employee background checks
8. Security monitoring systems to detect unauthorized access to customer information
9. Incident-response program to address security incidents effectively
10. Methods to provide protection from physical destruction of customer information

Kegerreis, Davis, Schiller, and Wrozek (2020). IT Auditing: using controls to protect information assets (Third edition)



10



The FFIEC Approach

THE LAZY AUDITOR'S GUIDE TO REGULATION

11

Information Security Booklet

THE FFIEC APPROACH



- Pros
 - Good coverage of the Interagency Guidelines Sections in the CFRs
 - Sections include specific security program components
 - Foundational to understanding the rest of the FFIEC booklets
- Cons
 - More conceptual than prescriptive
 - References to other documents are aging since 2016 release



12

Strategies

THE FFIEC APPROACH

1

Preview the
Text

2

Review
Summaries

3

Identify
Gaps

4

Evaluate and
Plan

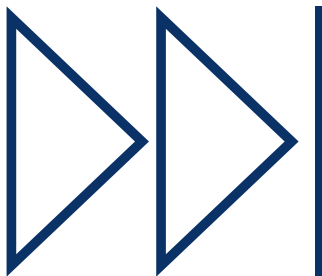
Guidance 101: Tips to Analyze Difficult Documentation (Alyssa Pugh)



13

Strategies Applied

THE FFIEC APPROACH



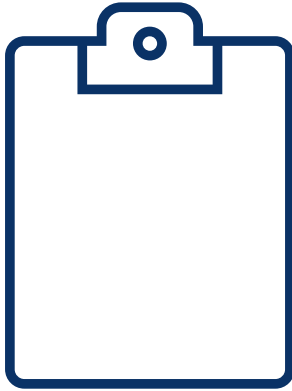
- Preview the Text
 - Read the Table of Contents
 - Read the Introduction section
- Read the Action Summaries
 - Drops the page count down to 22 Action Summaries
 - Gives you a quick “Are we doing this already?” gut check
- Identify Gaps
 - For areas that didn’t pass the gut check, review those sections and their booklet references to evaluate and plan how to get there



14

The Cybersecurity Assessment Tool

THE FFIEC APPROACH



- Pros
 - Coverage spans the FFIEC booklets
 - Controls pull from the action summary areas with prescriptive tools
 - Questionnaire format gives you a measurable gap analysis for your information security program
 - Built to convey results and status updates to executives
- Cons
 - Like the Information Security booklet, references to other documents have been superseded by new booklets



15

The Cybersecurity Assessment Tool

THE FFIEC APPROACH

Figure 1: Inherent Risk Profile Layout

	Category: Technologies and Connection Types	Risk Levels				
		Least	Minimal	Moderate	Significant	Most
Activity, Service, or Product	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)
	Wireless network access	No wireless access	Separate access points for guest wireless and corporate wireless	Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points)	Wireless corporate network access; significant number of users and access points (251–1,000 users; 26–100 access points)	Wireless corporate network access; all employees have access; substantial number of access points (>1,000 users; >100 access points)

FFIEC Cybersecurity Assessment Tool (p.4)



16

The Cybersecurity Assessment Tool

THE FFIEC APPROACH



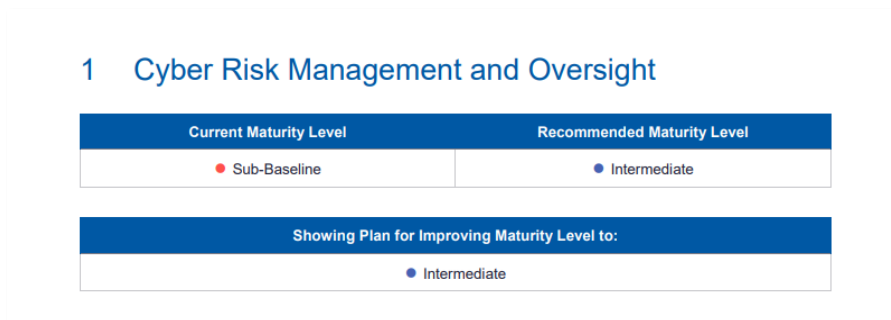
FFIEC Cybersecurity Assessment Tool (p.8)



17

Bonus: Tandem Cybersecurity Pro

THE FFIEC APPROACH



Download Documents > Gap Analysis



18

Bonus: Tandem Cybersecurity Pro

THE FFIEC APPROACH

1.1 Plan of Action

To Improve to Baseline

1. The risk assessment is updated to address new technologies, products, services, and connections before deployment.

To Improve to Evolving

1. Risk assessments are used to identify the cybersecurity risks stemming from new products, services, or relationships.
2. Cybersecurity tools and staff are requested through the budget process.

To Improve to Intermediate

1. The board or an appropriate board committee reviews and approves management's prioritization and resource allocation decisions based on the results of the cyber assessments.

[Download Documents > Gap Analysis](#)



19



The NIST Approach

THE LAZY AUDITOR'S GUIDE TO REGULATION

20

The NIST Cybersecurity Framework

THE NIST APPROACH



- Pros
 - Designed for critical infrastructure
 - Breaks down an InfoSec Program into 5 parts
 - Plenty of additional resources
 - Quick Start Guide
 - Informational References
 - Major influence for the FFIEC CAT
 - Helpful for ISOs (vISOs) already familiar with the framework
 - Updates with evolving technologies (planned revisions for 2022)
- Cons
 - Categories (Activities) and Subcategories (Outcomes) may not match 1:1 with FFIEC requirements



21

Strategies

THE NIST APPROACH

1

Prioritize and
Scope your
program

2

Create your
Framework
Profile

3

Identify
Gaps

4

Evaluate and
Plan

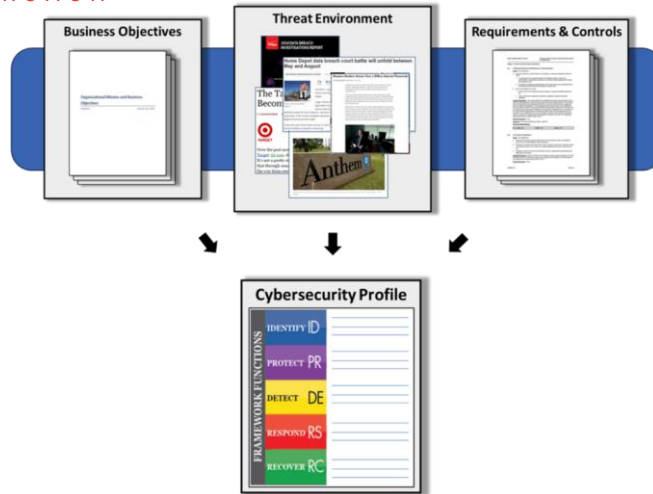
NIST Cybersecurity Framework Version 1.1 (p. 14)



22

The NIST Cybersecurity Framework

THE NIST APPROACH



<https://www.nist.gov/cyberframework/online-learning/components-framework>



23

The NIST Cybersecurity Framework

THE NIST APPROACH

FRAMEWORK FUNCTIONS	IDENTIFY ID	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
	PROTECT PR	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
	DETECT DE	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
	RESPOND RS	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
	RECOVER RC	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES

Figure 1: Framework Core Structure

NIST Cybersecurity Framework Version 1.1 (p. 6)



24

The NIST Cybersecurity Framework

THE NIST APPROACH

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Supply Chain Risk Management	ID.SC
	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
Detect	Maintenance	PR.MA
	Protective Technology	PR.PT
	Anomalies and Events	DE.AE
Respond	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
	Response Planning	RS.RP
Recover	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO02.06, APO03.01 ISO/IEC 27001:2013 Clause 4.1 NIST SP 800-53 Rev. 4 PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	COBIT 5 APO10.01, BAI04.02, BAI09.02 ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	COBIT 5 DSS04.02 ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14

<https://www.nist.gov/cyberframework/online-learning/informative-references>



25

The NIST Cybersecurity Framework

THE NIST APPROACH

FINANCIAL SERVICES SECTOR

- Conference of State Bank Supervisors' [Cybersecurity 101: A Resource Guide for Bank Executives](#) ²⁴
(A non-technical, easy-to-read resource on cybersecurity that community bank CEOs, senior executives and board members can use to help mitigate cybersecurity threats at their banks.)
- Federal Financial Institutions Examination Council's [Cybersecurity Assessment Tool](#)
(An Assessment is based on the cybersecurity assessment that the FFIEC members piloted in 2014, which was designed to evaluate community institutions' preparedness to mitigate cyber risks. NIST defines cybersecurity as "the process of protecting information by preventing, detecting, and responding to attacks.")
- Federal Financial Institutions Examination Council's [Mapping Cybersecurity Assessment Tool to NIST Cybersecurity Framework](#)
- The Financial Industry Regulatory Authority [Report on Cybersecurity Practices](#) ²⁵
(A report which details practices that firms can tailor to their business model as they strengthen their cybersecurity efforts.)
- The Cyber Risk Institute's [The Profile](#) ²⁶
(A customization of the NIST Cybersecurity Framework that financial institutions can use for internal and external cyber risk management assessment and as a mechanism to evidence compliance with various regulatory frameworks)

<https://www.nist.gov/cyberframework/critical-infrastructure-resources>



26

FFIEC CAT to NIST CSF Mapping

THE NIST APPROACH

Tier 2: Risk Informed

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
Risk management practices are approved by management but may not be established as organizational-wide policy. (p. 10)	D1.RM.RMP.B.1: An information security and business continuity risk management function(s) exists within the institution.
Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements. (p. 10)	D2.Tl.Th.B.3: Threat information is used to enhance internal risk management and controls. D1.G.Ov.Int.5: The board or an appropriate board committee ensures management's annual cybersecurity self-assessment evaluates the institution's ability to meet its cyber risk management standards. D1.G.SP.Int.2: Management periodically reviews the cybersecurity strategy to address evolving cyber threats and changes to the institution's inherent risk profile.
There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established. (p. 10)	D1.G.Ov.B.2: Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. D1.TC.Tr.B.1: Annual information security training is provided. D1.TC.Tr.E.2: Management is provided cybersecurity training relevant to their job responsibilities.
Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties. (p. 10)	D1.RM.RMP.E.1: The risk management program incorporates cyber risk identification, measurement, mitigation, monitoring and reporting. D1.R.SI.E.3: Staff with cybersecurity responsibilities have the requisite qualifications to perform the necessary tasks of the position.

FFIEC CAT, Appendix B



27

FFIEC CAT to NIST CSF Mapping

THE NIST APPROACH

Appendix A: Framework Core

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
ID.AM-1: Physical devices and systems within the organization are inventoried. (p. 20)	D1.G.IT.B.1: An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained.
ID.AM-2: Software platforms and applications within the organization are inventoried. (p. 20)	D1.G.IT.B.1: An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained.
ID.AM-3: The organizational communication and data flow is mapped. (p. 20)	D4.C.Co.B.4: Data flow diagrams are in place and document information flow to external parties. D4.C.Co.Int.1: A validated asset inventory is used to create comprehensive diagrams depicting data repositories, data flow, infrastructure, and connectivity.
ID.AM-4: External information systems are mapped and catalogued. (p. 20)	D4.RM.Dd.B.2: A list of third-party service providers is maintained. D4.C.Co.B.3: A network diagram is in place and identifies all external connections.
ID.AM-5: Resources are prioritized based on the classification / criticality / business value of hardware, devices, data, and software. (p. 20)	D1.G.IT.B.2: Institution assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value.
ID.AM-6: Workforce roles and responsibilities for business functions, including cybersecurity, are established. (p. 20)	D1.R.SI.B.1: Information security roles and responsibilities have been identified. D1.TC.Cu.B.1: Management holds employees accountable for complying with the information security program.
ID.BE-1: The organization's role in the supply chain is identified and communicated. (p. 21)	D1.G.SP.A.3: The cybersecurity strategy identifies and communicates the institution's role as a component of critical infrastructure in the financial services industry.

FFIEC CAT, Appendix B



28

Bonus: NIST to Tandem Mapping

THE NIST APPROACH

NIST Category	NIST Subcategory	Tandem References
<ul style="list-style-type: none"> Identify <p>Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.</p>	ID.AM-1: Physical devices and systems within the organization are inventoried	Business Continuity Plan (Systems/Equipment) Policies <ul style="list-style-type: none"> Asset Management Network Diagrams
	ID.AM-2: Software platforms and applications within the organization are inventoried	Business Continuity Plan (Software) Asset Management Policy
	ID.AM-3: Organizational communication and data flows are mapped	Network Diagrams Policy Information Security Risk Assessment (Data Flow)
	ID.AM-4: External information systems are catalogued	Business Continuity Plan (Systems/Equipment) Policies <ul style="list-style-type: none"> Asset Management Network Diagrams
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	Business Continuity Plan (Systems/Equipment)
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Policies (Policy Responsibility by Position Report)
<ul style="list-style-type: none"> Identify <p>Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.</p>	ID.BE-1: The organization's role in the supply chain is identified and communicated	N/A
	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	Business Continuity Plan Risk Assessment Considering Critical Infrastructure Knowledge Base Article

[Support Dashboard > Resources](#)



29



The Community Approach

THE LAZY AUDITOR'S GUIDE TO REGULATION

30

Cyber Risk Institute's The Profile

THE COMMUNITY APPROACH



- Pros
 - Custom version of the NIST CSF designed for financial institutions
 - Familiar NIST Functions along with Governance and Supply/Dependency Management
 - Questionnaire format gives you a measurable gap analysis for your information security program
 - Includes references that span across FFIEC Booklets, CAT, and NIST CSF
- Cons
 - Still very new since release in 2018 by the FSSCC to being maintained by the Cyber Risk Institute (CRI) as of 2020.



31

Strategies

THE COMMUNITY APPROACH

1

Determine
Impact Tier

2

Assess
against
Diagnostic
Statements

3

Identify
Gaps

4


Develop and
implement a
plan



32

Cyber Risk Institute's The Profile

THE COMMUNITY APPROACH



Tier 1: National/Super-National Impact

Question 1.1 Overview: North American governments (the United States, in particular ["USG"]) have designated various Financial Services Sector institutions as critical and systemically important by way of several different designations through various different regulators and regulatory bodies. These designations imply a high level of systemic importance and therefore result in the alignment of designated institutions to the highest impact tier: **Tier 1: National/Super-National Impact.**

Question 1.1: Check the Box(es) that apply: Is your institution designated as systemically important to the Financial Services Sector under one of the following designations?

- ☐ a. Critical Infrastructure Institution under section 9 of Executive Order 13636
- ☐ b. Global Systemically Important Bank (G-SIB)¹
- ☐ c. Global Systemically Important Insurer (G-SII)
- ☐ d. Non-Bank Non-Insurer Global Systemically Important Financial Institution (NBNI G-SIFI)
- ☐ e. Designated Financial Markets Utility (e.g., SIFMU's, D-FMUs)
- ☐ f. Multi-Regional Data Processing Service (MDPS)
- ☐ g. Domestically Systemic Important Bank (D-SIB)²
- ☐ h. Regional Technology Service Provider (TSP)
- ☐ i. Core clearing and settlement institution
- ☐ j. Financial institution that plays a significant role in critical financial markets

If No to all: Proceed to **Question 1.2.**

If Yes to any: Your institution is designated a **Tier 1: National/Super-National Impact.**



33

Cyber Risk Institute's The Profile

THE COMMUNITY APPROACH



GOVERNANCE

Strategy and Framework (GV.SF)

GV.SF-1.1: The organization has a cyber risk management strategy and framework that is approved by the appropriate governing authority (e.g., the Board or one of its committees) and incorporated into the overall business strategy and enterprise risk management framework.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓



34

Cyber Risk Institute's The Profile

THE COMMUNITY APPROACH

Response Guidance

The organization's cyber risk management strategy and framework should be a prominent part of all business strategies, practices, policies, and procedures. The cyber risk management strategy should align with long-term business strategies and the technologies to support these strategies. Management can support an enterprise information security program and enterprise risk management framework by setting a strong security culture that begins with Board involvement and ongoing cybersecurity awareness training that is expected at all levels of management and staff.

Include information about the organization's cyber risk management strategy and framework. Document the approval of the strategy and framework by the Board (or one of its committees) and outline how the strategy/framework incorporates business strategy and links to the enterprise risk management framework. For example, the cyber risk management framework may be part of the organization's overall enterprise risk management framework. Describe how that framework is established and executed for cyber risk management.



35

Cyber Risk Institute's The Profile

THE COMMUNITY APPROACH

Examples of Effective Evidence

- Cyber risk management strategy and framework, including evidence of approval by the Board (or one of its committees) or other appropriate governing authority
- Enterprise risk management frameworks based on a recognized standard-setting authority framework
- Policies, standards, procedures, and guidelines specific to cyber risk management
- Organizational chart to demonstrate functional roles, responsibilities, and independence
- Relevant Board and committee (e.g., cyber risk strategy committee, steering committee, etc.) meeting minutes and approvals where cyber risk management strategy is discussed



36

Recap

THE LAZY AUDITOR'S GUIDE TO REGULATION

- Regulation vs. Guidance vs. Frameworks
- The FFIEC Approach
- The NIST Approach
- The Community Approach



37



38




DON'T FORGET!

Fill out the survey to get your sticker!

39



THANKS FOR JOINING!

The Lazy Auditor's Guide to Regulation

Christopher Hidalgo
ITIL-F, Audit and Security Consultant

40

Upcoming Sessions

TANDEM

Testing, B-C-P

Savannah Richardson, Tandem

RISK & COMPLIANCE

Problem Solving vs. Problem Finding: Responding to IT/GLBA Exam and Audit Findings

Joseph Ellis, CoNetrix Security



41

Slide References

THE LAZY AUDITOR'S GUIDE TO REGULATION

- Kegerreis, Davis, Schiller, and Wrozek (2020). IT Auditing: using controls to protect information assets (Third edition)
- Guidance 101: Tips to Analyze Difficult Documentation (Alyssa Pugh).
<https://secure.tandem.app/Videos/Index>
- Implementing the NIST Cybersecurity Framework (Udemy Course) by Jason Dion and Kip Boyle (Mentioned on slide 21)
- <https://www.nist.gov/cyberframework/online-learning/components-framework> (slide 23)
- <https://www.nist.gov/cyberframework/online-learning/informative-references>
- <https://www.nist.gov/cyberframework/critical-infrastructure-resources>
- Cyber Risk Institute's The Profile <https://cyberriskinstitute.org/the-profile/>



42