# NIST Cybersecurity & Risk Management

## Course Self- Directed Exercise Compilation Document

## Episode 1.3: NIST Publications

Challenge:

1. What value does/can NIST publications provide to you as an auditor?
2. What value does/can the NIST CSF provide to you as an auditor?
3. What value does/can the NIST RMF provide to you as an auditor?

## Episode 1.6: The Toolkit

Assembling your Case Study Toolkit

*What will you need?*

- NIST SP 800-37R2

# NIST Cybersecurity & Risk Management

- NIST CSF:
- CSF Framework PDF & CSF Core Excel
- CIS Controls
- PCI DSS

## Episode 2.1: Table Me

- Review Table 2 (Identify Function & Categories, pp. 24-29) and use the information to consider the following questions:

1. Which of these categories are you most familiar with?
2. Which of these subcategories are you most familiar with?

# NIST Cybersecurity & Risk Management

3. Which of the informative references are you most familiar with?

4. Which of these categories do you find most challenging when performing an audit? Why?

5. Which of these subcategories is most difficult for you to use during an audit when working with clients?

## Episode 2.2: NMAP

1. Learn about/try Nmap
2. Load and examine a sample inventory file

- What machines did you find?

What software/applications were

inventoried?

- **Optional :** Establish your own inventory using NMAP – scan a friendly network (with permission):
- Hardware (computers and IoT)
- Software (aps)
- Data

## Episode 2.3: Create a BIA

- Complete the BIA templates (Excel worksheet and/or Word document):

a. Timing

b. Duration

c. Operational Imapct

d. Financial Impact

You can use the inventory list from your NMAP exercise (sample file or real inventory), or you can simply make up the information to populate the BIA template.

## Episode 3.2: Security Awareness

- How does your organization provide security awareness training (the modalities)?
- When does your organization provide security awareness training (the frequency)?

# NIST Cybersecurity & Risk Management

- What do you remember from it?
- On a scale of 1 – 10, 1 being the lowest/least effective & 10 being the highest/most effective, how would you rate the training?

## Episode 3.3: Access Control

- How do you ensure user access and authorization levels are appropriate when auditing a client?
- What about administrator (root) authority to access?
- Network
- Servers

- PCs/end-points

## Episode 3.6: Access Control

www.ssllabs.com

## Episode 5.1: Incident Report

Think about clients you have audited over the last year to answer the following questions:

- How many of them had a global pandemic response plan before the outbreak of COVID-19 at the end of 2019, beginning of 2020?
- How many of them have a global pandemic response plan as a result of COVID-19?

# NIST Cybersecurity & Risk Management

- Does your company have adequate incident response planning in place for non-I.T.-related incidents?
- What would you recommend to a client concerned about incident response planning and how to undertake it?
- Do you have a set of tools to help facilitate a conversation with a client about incident response planning?

## Episode 5.2: Digital Forensics

Think about clients you have audited over the last three years to answer the following questions:

# NIST Cybersecurity & Risk Management

- How many of them had an incident that required a digital forensics response component?
- How many of them had a digital forensics response capability internally as part of a Computer Security Incident Response Team (CSIRT)?
- What would you recommend to a client concerned about digital forensics response and how to undertake it?

- Do you have a set of tools to help facilitate a conversation with a client about digital forensics response planning?

## Episode 6.1: Business Continuity

Think about clients you have audited over the last three years to answer the following questions:

- How many of them had a Business Continuity Plan (BCP) before the outbreak of COVID-19 at the end of 2019, beginning of 2020?

# NIST Cybersecurity & Risk Management

- How many of them have a BCP as a result of COVID-19?
- Does your company have an adequate BCP in place?
- What would you recommend to a client concerned about business continuity planning and how to undertake it?
- Do you have a set of tools to help facilitate a conversation with a client about business continuity planning?

# NIST Cybersecurity & Risk Management

## Episode 7.3: A Tale of Two Lists

*Create two lists based on your current organization:*

Organization Level Tasks:

- Your organization’s roles and responsibilities for managing security and privacy risks. Is it a team or an individual?
- The control framework(s) your organization needs to follow. (Regulatory requirements or industry standards)

# NIST Cybersecurity & Risk Management

- How does your organization identify, analyze and manage risks.

**System-Level Tasks:**

- System function & stakeholders. What is the system? Where is it located? Who are its owners, operators, or other stakeholders?
- Specific assets – The specific computers, devices, applications, or technologies. Include as much information as you can (the manufacturer, make, model, and version number)

# NIST Cybersecurity & Risk Management

- Type of information stored, processed, or transmitted by the system. Focus on the most sensitive data that could harm the organization if there is unauthorized disclosure or modification.