Before scheduling a first time Cybersecurity Assessment and Gap Analysis, the customer's leaders and team should participate in five 3 to 4 hours 'Make and Take' exercises that cover the NIST Core V1.1 Cybersecurity Framework. The five training courses cover Incident Response, Risk Management, Vulnerability Management, Organizational and Third-Party Access Control and Training and Network System Controls.

The 5 NIST Training Exercises are:

1. Incident Response Guide and Tabletop Exercise
2. Risk Management Guide, Tools & Assessment Exercise
3. Vulnerability Management Detection & Analysis Exercise
4. Organization, Third Party Access Control, and Training Exercise
5. Network Systems Control Exercise

There are 108 Data Security Controls in the NIST Core V1.1 Cybersecurity Framework. The training covers all the data security controls in a relatable exercise to enhance understanding. The five exercises covers from 14 controls for Risk Management to 29 controls for Network System Controls.

	Identify	**Protect**	**Detect**	**Respond**	**Recover**
Data Security Controls	**29**	**39**	**18**	**16**	**6**
IR Guide and IR Tabletop Exercise	1	2		13	6
Risk Management Guide and Risk Management Worksheet	13				
Vulnerability Management Guide, Tools, and Analysis		1	17	3	
Organization, Third Party Access Control, and Training Exercise	8	16			
Network Systems Control Exercise	7	20	1		

3. Vulnerability Management Detection & Analysis Seminar

In this session, the OhCR team will take your school district through the Vulnerability Management (VM) Plan as well as expand your understanding of the VM process. We will examine the CISA Cyber Hygiene Program as well as placing a tap inside your network. We will review Windows server and Google Workspace log analysis and threshold settings. We will look at both open source and professional VM tools and their reports.

- Vulnerability Management Policy TEMPLATE exercise
- Sign up and use the CISA External Looking Cyber Hygiene Service with NMAP and NESSUS
- Acquire Tap, Install, and Collect Data inside the Network Exercise
- Log Analysis and Thresholds Setting Exercise
- SIEM Software Selection and Basic Training Syllabus Exercise
- Elevating an Event to an IR Incident Process

This seminar helps the organization to meet the following NIST Data Security controls.

The NIST Framework (National Institute of Standards of Technology) outlines the need for an Risk Management Plan in the following areas:

1. Protect PR.IP-12: A vulnerability management plan is developed and implemented
2. Detect DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed
3. Detect DE.AE-2: Detected events are analyzed to understand attack targets and methods
4. Detect DE.AE-3: Event data are collected and correlated from multiple sources and sensors
5. Detect DE.AE-4: Impact of events is determined
6. Detect DE.AE-5: Incident alert thresholds are established
7. Detect DE.CM-1: The network is monitored to detect potential cybersecurity events
8. Detect DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events
9. Detect DE.CM-4: Malicious code is detected
10. Detect DE.CM-5: Unauthorized mobile code is detected
11. Detect DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events
12. Detect DE.CM-7:: Monitoring for unauthorized personnel, connections, devices, and software is performed
13. Detect DE.CM-8:: Vulnerability scans are performed
14. Detect DE.DP-1:: Roles and responsibilities for detection are well defined to ensure accountability
15. Detect DE.DP-2:: Detection activities comply with all applicable requirements
16. Detect DE.DP-3:: Detection processes are tested
17. Detect DE.DP-4:: Event detection information is communicated
18. Detect DE.DP-5:: Detection processes are continuously improved
19. Respond RS.AN-1: Notifications from detection systems are investigated
20. Respond RS.AN-2: The impact of the incident is understood
21. Respond RA.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)