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		

4. **Organizational and Third-Party Access Control and Compliance as well as Training Seminar**

   In this session, the OhCR team and you will examine the journey to NIST Cybersecurity Compliance to meet your contractual obligations and Board policies. Our training will focus on Access Control in your School District that protects student, teacher, and staff data using processes, and decision-making exercises. Are you trying to protect everything but risking critical data? The OhCR and you will learn to identify the critical data and those who access it, to reduce your attack surface. Together, the OhCR and you will expand into the Cloud space and supply chain to assure that your vendors are also compliant. You will finish the seminar with a robust look at the districtwide Cyber Security Awareness training program.

   - NIST and Data Security Training and your Policies
   - Access Control Process Template and Exercise
   - Identify Critical Staff for Access Control Exercise
   - Supplier Control Process
   - Vendor Data Privacy Control Make and Take

- Security Awareness Training Exercise

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. Identify ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
2. Identify ID.BE-1: The organization's role in the supply chain is identified and communicated
3. Identify ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated
4. Identify ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated
5. Identify ID.GV-1: Organizational cybersecurity policy is established and communicated
6. Identify ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
7. Identify ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
8. Identify ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
9. Protect PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
10. Protect PR.AC-2: Physical access to assets is managed and protected
11. Protect PR.AC-3: Remote access is managed
12. Protect PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
13. Protect PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)
14. Protect PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions
15. Protect PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
16. Protect PR.AT-1: All users are informed and trained
17. Protect PR.AT-2: Privileged users understand their roles and responsibilities
18. Protect PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
19. Protect PR.AT-4: Senior executives understand their roles and responsibilities
20. Protect PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities
21. Protect PR.DS-5: Protections against data leaks are implemented
22. Protect PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
23. Protect PR.PT-2: Removable media is protected and its use restricted according to policy
24. Protect PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities