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		

5. Network Configuration and Maintenance Control Seminar

In this session, you improve your inventory control by identifying assets as critical and non-critical. You and your team will work with School District leaders to create your data flows to identify all PII, PHI and PFI storage, locally and on the cloud. The OhCR, you and your team will build system design and maintenance skills to promote data security and efficiency. You will finish the seminar with a plan to sustain your Cybersecurity Framework.

- Identify Asset Inventory and Categorization Exercise
- How to Make a Data Flow Exercise
- Business Critical and Non-Critical Systems Exercise
- Developing Organizational Standards for Systems Architecture
- Information Technology System Maintenance Plan
- A CSF Sustainment Plan that Works.

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-1: Physical devices and systems within the organization are inventoried
2. Identify ID.AM-2: Software platforms and applications within the organization are inventoried
3. Identify ID.AM-3: Organizational communication and data flows are mapped
4. Identify ID.AM-4: External information systems are catalogued
5. Identify ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
6. Identify ID.BE-4: Dependencies and critical functions for delivery of critical services are established
7. Identify 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)
8. Protect PR.DS-1: Data-at-rest is protected
9. Protect PR.DS-2: Data-in-transit is protected
10. Protect PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition
11. Protect PR.DS-4: Adequate capacity to ensure availability is maintained
12. Protect PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity
13. Protect PR.DS-7: The development and testing environment(s) are separate from the production environment
14. Protect PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity
15. Protect PR.IP-1: A baseline configuration of information technology / industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
16. Protect PR.IP-2: A System Development Life Cycle to manage systems is implemented
17. Protect PR.IP-3: Configuration change control processes are in place
18. Protect PR.IP-4: Backups of information are conducted, maintained, and tested
19. Protect PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met
20. Protect PR.IP-6: Data is destroyed according to policy
21. Protect PR.IP-7: Protection processes are improved
22. Protect PR.IP-8: Effectiveness of protection technologies is shared
23. Protect PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
24. Protect PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
25. Protect PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
26. Protect PR.PT-4: Communications and control networks are protected
27. Protect PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations
28. Detect DE.CM-2: The physical environment is monitored to detect potential cybersecurity events