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		

2. Risk Management Guide, Tools & Assessment Seminar

In this session, the OhCR team will take your school district through the K-12 Risk Management Plan and make the necessary changes to build your scheme to respond to a cybersecurity threat. When the plan is verified, it will meet the ID.GV-4, ID.RA-1 to ID.RA-6, ID.RM-1 to ID.RM-3, ID.SC-1 to ID.SC-3 data security controls.

- Risk Management Plan TEMPLATE
- Risk Management Worksheet 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 a Risk Management Plan in the following areas:

1. Identify ID.GV-4: Governance and risk management processes address cybersecurity risks
2. Identify ID.RA-1: Asset vulnerabilities are identified and documented
3. Identify ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources
4. Identify ID.RA-3: Threats, both internal and external, are identified and documented

5. Identify ID.RA-4: Potential business impacts and likelihoods are identified
6. Identify ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
7. Identify ID. RA-6: Risk responses are identified and prioritized
8. Identify ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders
9. Identify ID.RM-2: Organizational risk tolerance is determined and clearly expressed
10. Identify ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis
11. Identify ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
12. Identify ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process
13. 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.