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		

1. Incident Response Guide and Tabletop Seminar

A good Incident Response Guide (IRG) is required for cybersecurity compliance as well as many cyber insurance carriers. A best practice is to have an IRG in place and review it annually. For this session, attendees will be provided with the best documents needed to gather information prior to the workshop. When attending the workshop, bring your documents to complete the IRG template. This "Make and Take" session is designed to assist you in leaving with a workable guide. Then an IR Tabletop exercise walks you through different scenarios while referencing the IRG.

- Incident Response Guide TEMPLATE
- IR Tabletop 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 Incident Response Plan in the following areas:

1. Identify ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers
2. Protect PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
3. Protect PR.IP-10: Response and recovery plans are tested
4. Respond RS.AN-3: Forensics are performed
5. Respond RS.AN-4: Incidents are categorized consistent with response plans
6. Respond RS.CO-1: Personnel know their roles and order of operations when a response is needed
7. Respond RS. CO-2: Incidents are reported consistent with established criteria
8. Respond RS.CO-3: Information is shared consistent with response plans
9. Respond RS.CO-4: Coordination with stakeholders occurs consistent with response plans
10. Respond RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
11. Respond RS.IM-1: Response plans incorporate lessons learned
12. Respond RS.IM-2: Response strategies are updated
13. Respond RS.MI-1: Incidents are contained
14. Respond RS.MI-2: Incidents are mitigated
15. Respond RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks
16. Respond RS.RP-1: Response plan is executed during or after an incident
17. Recover RC.CO-2: Reputation is repaired after an incident
18. Recover RC.CO-1: Public relations are managed
19. Recover RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams
20. Recover RC.IM-1: Recovery plans incorporate lessons learned
21. Recover RC.IM-2: Recovery strategies are updated
22. Recover RC.RP-1: Recovery plan is executed during or after a cybersecurity incident