INFO ADVANTAGE

Cybersecurity Self-Assessment

This **Cybersecurity Self-Assessment** is designed to provide insight to those responsible for achieving regulatory compliance and protecting assets. The assessment is a high-level evaluation that will help determine the cybersecurity preparedness level of the organization based on the widely adopted National Institute of Standards and Technology (NIST) Cybersecurity Framework.

The NIST Cybersecurity Framework requires adopters to; (1) have the capability to **Identify** cyber threats and vulnerabilities, (2) **Protect** themselves accordingly with security controls and defenses, (3) have the capability to **Detect** if security controls have been compromised, (4) **Respond** to cyberattacks, incidents and breaches and lastly, (5) **Recover** from cyber-attacks, incidents and breaches.

The assessment is segmented into five Sections (Identify, Protect, Detect, Respond, Recover). Each section contains several statements. Read each statement carefully and then assign a numeric value using the assessment scale below. The numeric value assigned to the statement should be most representative of your organization's current capability or status.

Numeric Value	Statement Compliance
1	Disagree
2	Somewhat Disagree
3	Somewhat Agree
4	Agree

After assigning a numeric value to all statements for a section, add all numeric values for a section total and refer to the results recommendation section.

INFO ADVANTAGE

Section 1: Identify

DISAGREE TO AGREE

1.	All physical systems and devices within the organization are inventoried.	1 ☐	2 ☐	3 ☐	4 ☐
2.	All software platforms and applications within the organization are inventoried.	1 ☐	2 ☐	3 ☐	4 ☐
3.	All systems, devices, software platforms and applications are classified & prioritized based on their criticality & business value.	1 ☐	2 ☐	3 ☐	4 ☐
4.	The organization has clearly defined cybersecurity roles and responsibilities for internal users, external vendors, customers and partners.	1 ☐	2 ☐	3 ☐	4 ☐
5.	The organization has a written information security policies and procedures.	1 ☐	2 ☐	3 ☐	4 ☐
6.	The organization clearly understands all legal and regulatory requirements regarding cybersecurity.	1 ☐	2 ☐	3 ☐	4 ☐
7.	Cybersecurity risks are identified and managed by a governance and risk management process.	1 ☐	2 ☐	3 ☐	4 ☐
8.	Cybersecurity risk tolerance is determined, expressed in policy & agreed upon by all stakeholders.	1 ☐	2 ☐	3 ☐	4 ☐

_____ Total Score

Total Score	Recommendations
8 – 16	The overall ability to identify cybersecurity threats is relatively low. The organization should work to develop a library of information security policies and procedures that will provide the rules and guidance necessary to build and effective cybersecurity program. An inventory all hardware and software assets should be completed. Once the inventory of assets exists and there is a clear understanding of scope, a formal risk management process should be implemented to that cybersecurity risks are identified, assigned a risk rating and then responded to accordingly. The risk management process will help to prioritize the implementation of protective controls and defenses based on overall risk appetite. It is important for the organization to clearly understand what regulatory requirements exists regarding cybersecurity so that there is an appreciation for what will need to be accomplished to achieve compliance.

17 – 30	The overall ability to identify cybersecurity threats is inconsistent. The organization may have an incomplete set of information security policies and procedures or, the policies and procedures may not be used properly to govern the cybersecurity program. There may be a partial asset inventory, or an inventory that is not current and needs to be refreshed. A risk management process may exist but one of several issues may need to be addressed to make the process effective. Potential opportunities to improve the risk management process include (1) increase participation amongst data owners and executive stakeholders, (2) increase the frequency of the risk management exercise, (3) be sure that qualified and credentialed experts perform the risk management exercise, and (4) use the results of the risk management exercise to take actionable steps in improving the overall cybersecurity program. The organization may have partial awareness of regulatory requirements that exist regarding its cybersecurity program and should commit to learning about any and all regulatory requirements.
31 – 40	The overall ability to identify cybersecurity threats is very good. The organization has a library of information security policies and procedures that effectively governs the cybersecurity program. There may be an opportunity to review policies and procedures more frequently to ensure they remain current and relevant. The organization maintains a comprehensive inventory of information technology assets. The organization has a formal risk management program and they use the results of this program to prioritize improvements made to the cybersecurity program. The organization has a very good understanding of regulatory requirements regarding cybersecurity.

Section 2: Protect

DISAGREE TO AGREE

1.	A security awareness training program is in place & all users are provided training at least annually.	1 ☐	2 ☐	3 ☐	4 ☐
2.	Critical or sensitive data is protected by encryption technology at rest and in transit.	1 ☐	2 ☐	3 ☐	4 ☐
3.	Network segmentation is used logically or physical separate systems according to policy.	1 ☐	2 ☐	3 ☐	4 ☐
4.	The organization has a formal change management process.	1 ☐	2 ☐	3 ☐	4 ☐
5.	There is a formal process documented for conducting, maintaining & testing data backups.	1 ☐	2 ☐	3 ☐	4 ☐
6.	Data backups of critical systems have at least 3 copies, 2 of which are located on different mediums and at least one of which is physically located offsite.	1 ☐	2 ☐	3 ☐	4 ☐
7.	All systems are secured and hardened using industry best practices or according to policy.	1 ☐	2 ☐	3 ☐	4 ☐
8.	There is a formal Vulnerability and Patch Management program in which systems, devices, software and applications are regularly scanned for known vulnerabilities and then patched or upgraded accordingly.	1 ☐	2 ☐	3 ☐	4 ☐
9.	Removable media and / or mobile devices are protected and restricted in accordance with policy.	1 ☐	2 ☐	3 ☐	4 ☐
10.	Access permissions & authorizations are managed, incorporating the principles of least privilege & separation of duties.	1 ☐	2 ☐	3 ☐	4 ☐
11.	Physical access to critical systems and devices is managed.	1 ☐	2 ☐	3 ☐	4 ☐
12.	Multi-Factor authentication is used to authenticate to critical systems or applications.	1 ☐	2 ☐	3 ☐	4 ☐
13.	There is a formal, written Disaster Recovery (DR) and Business Continuity Plan (BCP).	1 ☐	2 ☐	3 ☐	4 ☐

14. There is a formal, written Incident Response and Recovery Plan.	1 ☐	2 ☐	3 ☐	4 ☐
15. Perimeter defenses such as Firewalls and Intrusion Detection / Prevention systems are implemented and managed.	1 ☐	2 ☐	3 ☐	4 ☐
16. Endpoint protection such as Anti-Virus and Anti-Malware defenses are implemented and managed.	1 ☐	2 ☐	3 ☐	4 ☐

_____ Total Score

Total Score	Recommendations
16 – 32	The overall ability of the organization to protect itself against cybersecurity threats and attacks is very low. Many security controls that are required to effectively protect the organization and reduce overall risk are either absent or not configured correctly. The organization should immediately look for opportunities to add security controls or modify existing security controls according the to the results of the risk management process.
33 – 65	The organization can protect itself against certain types of cybersecurity threats and attacks, others it cannot. There are several types of existing security controls implemented effectively but there is also a real opportunity to improves the overall cybersecurity program by looking for opportunities to add security controls or modify existing security controls according the to the results of the risk management process.
65 – 80	The organization is in an excellent position to protect itself from most cybersecurity threats and attacks. Many security controls are implemented and are effective. There is a need to frequently review existing security controls and look for ways to make minor improvements.

Section 3: Detect

DISAGREE TO AGREE

1.	The organization has a clear definition of normal network operations & expected data flows for users & systems.	1 ☐	2 ☐	3 ☐	4 ☐
2.	The organization has the capability to collect & correlate events & logs from multiple sources, systems, devices, or applications.	1 ☐	2 ☐	3 ☐	4 ☐
3.	The network, physical environment & user activity is actively monitored to detect potential cybersecurity events.	1 ☐	2 ☐	3 ☐	4 ☐
4.	The organization always knows when a security control has been comprised.	1 ☐	2 ☐	3 ☐	4 ☐

_____ Total Score

Total Score	Recommendations
4 – 8	The overall ability to detect cybersecurity events and incident is very low. The organization does not have the capability to know when security controls have been compromised causing an extreme delay in any detection of an incident and the ability to invoke an incident response plan. The organization should immediately work to understand the normal behaviors of the network and data flow then work to implement the capability to detect events and incidents.
9 – 12	The organization may be able to detect certain types of cybersecurity security events and incidents, but not all of them. The ability to know when security controls have been compromised is inconsistent and reactive. The organization should immediately work to understand the normal behaviors of the network and data flow then work to implement the capability to detect events and incidents.
13 – 16	The organization can effectively detect cybersecurity events and incidents. There may be an opportunity to fine tune the detection process, procedure and related technologies to reduce the overall number of false positive detections.

Section 4: Response

DISAGREE TO AGREE

1.	Roles and responsibilities for incident response personnel are thoroughly defined and communicated.	1 ☐	2 ☐	3 ☐	4 ☐
2.	Cybersecurity incidents are properly communicated throughout the organization when they occur. Information related to the event is shared in a manner consistent with the Incident Response Plan.	1 ☐	2 ☐	3 ☐	4 ☐
3.	Formal, documented processes and procedures for investigating notifications of suspicious activity are executed and maintained by the incident response team.	1 ☐	2 ☐	3 ☐	4 ☐
4.	Formal, documented process & procedures exist to ensure preservation of forensic evidence during or after an event.	1 ☐	2 ☐	3 ☐	4 ☐
5.	The organization has the capability to quickly contain and mitigate cybersecurity incidents.	1 ☐	2 ☐	3 ☐	4 ☐
6.	The Incident Response Plan is regularly reviewed and updated based on test results or actual events.	1 ☐	2 ☐	3 ☐	4 ☐

_____ Total Score

Total Score	Recommendations
6 – 12	The overall ability to respond to cybersecurity events and incidents is very low. The organization should immediately (1) develop a formal Incident Response Plan, (2) establish an incident response team and (3) be sure that the organization can effectively mitigate attacks, communicate about incidents properly and effectively preserve forensic evidence.
13 – 24	The organization has some elements of an effective Incident Response Plan in place, but there are opportunities for overall improvement. Employees must understand what their role is in responding to a cybersecurity incident and how to effectively communicate with the organization during a response effort. The organization may also need to improve the overall process used to investigate the cybersecurity event or incident and properly preserve forensic evidence.

25 – 30	The organization can respond effectively to most cybersecurity events and incidents. There may be minor opportunities for improvement to the overall incident response plan, typically in the areas of event or incident investigation and preservation of forensic evidence.

INFO ADVANTAGE

Section 5: Recover

DISAGREE TO AGREE

1.	The Disaster Recovery (DR) and Business Continuity Plan (BCP) is tested regularly, at least annually.	1 ☐	2 ☐	3 ☐	4 ☐
2.	The organization is capable of recovering from a cybersecurity event or incident in accordance with desire Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).	1 ☐	2 ☐	3 ☐	4 ☐
3.	The organization maintains a crisis communication plan that manages the organization's reputation after a cybersecurity event or incident occurs.	1 ☐	2 ☐	3 ☐	4 ☐
4.	The Disaster Recovery (DR) and Business Continuity Plan (BCP) is reviewed and updated regularly, at least annually.	1 ☐	2 ☐	3 ☐	4 ☐

_____ Total Score

Total Score	Recommendations
4 – 8	The overall ability to recover from cybersecurity events and incidents is very low. The organization should immediately develop a formal Disaster Recovery (DR) and Business Continuity Plan (BCP). The plan should allow for prompt recovery of critical systems and should be reviewed and tested frequently, at least annually.
9 – 12	The organization has some elements of an effective DR / BCP plan but the plan may not be regularly reviewed and tested – or – the plan may not restore critical assets to an operational state within the desired Recovery Point Objective or Recovery Time Objective.
13 – 16	The organization can effectively recover from most cybersecurity events and incidents. There may be an opportunity to review the DR/BCP plan more frequently and test it for effectiveness, at least annually.

Questions? Please reach out to Info Advantage using the information below:

Website: www.info-adv.com

Phone: 585.254.8710