Nationwide Cyber Security Review 2018 & 2019: 482593

Created Date: 9/10/2019 8:52 AM Last Updated: 9/10/2019 8:52 AM

Instructions

Review the following steps to complete this questionnaire:

1) Utilize the save button found in the upper left hand corner periodically throughout the survey.

2) Answer the required questions in the **General Information** section of the survey.

3) Complete the survey by answering **all** of the questions in the following tabs listed below: Demographics, Identify, Protect, Detect, Respond, Recover, Privacy, Cybersecurity Automation & Orchestration Capabilities, and Post Survey Questions.

4) You can add comments or attach supporting evidence to each question by clicking on the sticky note icon located to the right of the question.

5) You can view question clarification by selecting the question mark icon located to the left of the question. Also included within this icon is a link to a policy template, if applicable.

6) When you have completed the assessment, change the Status within the Submit Self-Assessment section to Submit.

7) After you have completed the survey, you will be able to gain access to various reports specific to your entity. To access your results, utilize the dashboard found on the main homepage.

General Information

Questionnaire ID:	482593	**Year:**	2019
Organization:	2019 Test Organization		
Progress:	0 of 141 Completed	**Due Date:**	12/31/2019
Progress Status:	0%	What does your organization need to comply with? (Can select multiple answers below)	
Entity Type:		**Compliance Drivers:**	
Industry:		**ISAC Monitoring Services:**	
		Admin Findings:	

Submit Self-Assessment

Submit Self-Assessment:	Please note: It's important to make sure the survey is completed in full prior to changing the status to "Submit". Once the status is changed, your findings are generated and the survey is locked.	In Progress

Maturity Scale

The Nationwide Cyber Security Review utilizes the below response scale which allows participants to indicate how formalized the cybersecurity activities are within their organization.

Optimized: Your organization has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.

Tested and Verified: Your organization has formally documented policies. standards, and procedures. Implementation is tested and verified.

Implementation in Process: Your organization has formally documented policies, standards, and procedures and are in the process of implementation.

Risk Formally Accepted: Your organization has chosen not to implement based on a risk assessment.

Partially Documented Standards and/or Procedures: Your organization has a formal policy in place and began the process of developing documented standards and/or procedures to support the policy.

Documented Policy: Your organization has a formal policy in place.

Informally Performed: Activities and processes may be substantially performed and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by management.

Not Performed: Activities, processes and technologies are not in place to achieve the referenced objective.

Completion Tracking

Completion Tracking (ID):	0 %	**Completion Tracking (RC):**	0 %
Completion Tracking (PR):	0 %	**Completion Tracking (PC):**	0 %
Completion Tracking (DE):	0 %	**Completion Tracking (Post-Survey):**	0 %
Completion Tracking (RS):	0 %		

Demographics

(CSF) Demographics

(NCSR)Demo 1: Cybersecurity Governance:	How would you categorize your cybersecurity governance structure?
(NCSR)Demo 2: Cybersecurity Governance:	How would you categorize your cybersecurity implementation and operations?
(NCSR)Demo 3: Cybersecurity Governance:	Who are you answering the NCSR on behalf of?
(NCSR)Demo 4: Executive Reporting:	Do your top-level decision-makers receive periodic (at least annual) reports on the status of information risks, controls, and/or security from the departments, divisions, and/or agencies within your organization?
(NCSR)Demo 5: Cyber Security Executive Mandates:	Has your organization adopted or established a set of cybersecurity executive mandates, laws, statutes, approved legislation, policies, or standards to help guide the implementation of information security controls across your organization?
(NCSR)Demo 6: Security Framework:	Which control frameworks and/or security methodologies are your organization's information security controls based on? Select all that apply.
(NCSR)Demo 7: FTE Size:	How many full-time equivalent (FTEs) employees/contractors are there in your organization?
(NCSR)Demo 8: IT FTE:	How many full-time equivalent employees are there in your IT?
(NCSR)Demo 9: Security FTE:	How many full-time equivalent employees have security related duties?
(NCSR)Demo 10: IT Outsourcing:	What part of your IT operation is outsourced?
(NCSR)Demo 11: Security Outsourcing:	What part of your security operation is outsourced?

Identify

(CSF) Identify.Asset Management

ID.AM-1:	Physical devices and systems within the organization are inventoried.
ID.AM-2:	Software platforms and applications within the organization are inventoried
ID.AM-3:	Organizational communication and data flows are mapped
ID.AM-4:	External information systems are catalogued
ID.AM-5:	Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value
ID.AM-6:	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

(CSF) Identify.Business Environment

ID.BE-1:	The organization's role in the supply chain is identified and communicated
ID.BE-2:	The organization's place in critical infrastructure and its industry sector is identified and communicated
ID.BE-3:	Priorities for organizational mission, objectives, and activities are established and communicated
ID.BE-4:	Dependencies and critical functions for delivery of critical services are established
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)

(CSF) Identify.Governance

ID.GV-1:	Organizational cybersecurity policy is established and communicated
ID.GV-2:	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
ID.GV-3:	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
ID.GV-4:	Governance and risk management processes address cybersecurity risks

(CSF) Identify.Risk Assessment

ID.RA-1:	Asset vulnerabilities are identified and documented
ID.RA-2:	Cyber threat intelligence and vulnerability information is received from information sharing forums and sources
ID.RA-3:	Threats, both internal and external, are identified and documented
ID.RA-4:	Potential business impacts and likelihoods are identified
ID.RA-5:	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
ID.RA-6:	Risk responses are identified and prioritized

(CSF) Identify.Risk Management Strategy

ID.RM-1:	Risk management processes are established, managed, and agreed to by organizational stakeholders
ID.RM-2:	Organizational risk tolerance is determined and clearly expressed
ID.RM-3:	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis

(CSF) Identify.Supply Chain Risk Management

ID.SC-1:	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
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
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.
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.
ID.SC-5:	Response and recovery planning and testing are conducted with suppliers and third-party providers

Protect

(CSF) Protect.Access Control	
PR.AC-1:	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes
PR.AC-2:	Physical access to assets is managed and protected
PR.AC-3:	Remote access is managed
PR.AC-4:	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
PR.AC-5:	Network integrity is protected (e.g., network segregation, network segmentation)
PR.AC-6:	Identities are proofed and bound to credentials and asserted in interactions
PR.AC-7:	Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)

(CSF) Protect.Awareness and Training	
PR.AT-1:	All users are informed and trained
PR.AT-2:	Privileged users understand roles & responsibilities
PR.AT-3:	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities
PR.AT-4:	Senior executives understand roles & responsibilities
PR.AT-5:	Physical and cybersecurity personnel understand their roles and responsibilities

(CSF) Protect.Data Security	
PR.DS-1:	Data-at-rest is protected
PR.DS-2:	Data-in-transit is protected
PR.DS-3:	Assets are formally managed throughout removal, transfers, and disposition
PR.DS-4:	Adequate capacity to ensure availability is maintained
PR.DS-5:	Protections against data leaks are implemented
PR.DS-6:	Integrity checking mechanisms are used to verify software, firmware, and information integrity
PR.DS-7:	The development and testing environment(s) are separate from the production environment
PR.DS-8:	Integrity checking mechanisms are used to verify hardware integrity

(CSF) Protect.Information Protection Process and Procedures

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)
PR.IP-2:	A System Development Life Cycle to manage systems is implemented
PR.IP-3:	Configuration change control processes are in place
PR.IP-4:	Backups of information are conducted, maintained, and tested
PR.IP-5:	Policy and regulations regarding the physical operating environment for organizational assets are met
PR.IP-6:	Data is destroyed according to policy
PR.IP-7:	Protection processes are improved
PR.IP-8:	Effectiveness of protection technologies is shared
PR.IP-9:	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
PR.IP-10:	Response and recovery plans are tested
PR.IP-11:	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
PR.IP-12:	A vulnerability management plan is developed and implemented

(CSF) Protect.Maintenance

PR.MA-1:	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
PR.MA-2:	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

(CSF) Protect.Protective Technology

PR.PT-1:	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
PR.PT-2:	Removable media is protected and its use restricted according to policy
PR.PT-3:	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
PR.PT-4:	Communications and control networks are protected
PR.PT-5:	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations

Detect

(CSF) Detect.Anomalies and Events

DE.AE-1:	A baseline of network operations and expected data flows for users and systems is established and managed
DE.AE-2:	Detected events are analyzed to understand attack targets and methods
DE.AE-3:	Event data are collected and correlated from multiple sources and sensors
DE.AE-4:	Impact of events is determined
DE.AE-5:	Incident alert thresholds are established

(CSF) Detect.Security Continuous Monitoring

DE.CM-1:	The network is monitored to detect potential cybersecurity events
DE.CM-2:	The physical environment is monitored to detect potential cybersecurity events
DE.CM-3:	Personnel activity is monitored to detect potential cybersecurity events
DE.CM-4:	Malicious code is detected
DE.CM-5:	Unauthorized mobile code is detected
DE.CM-6:	External service provider activity is monitored to detect potential cybersecurity events
DE.CM-7:	Monitoring for unauthorized personnel, connections, devices, and software is performed
DE.CM-8:	Vulnerability scans are performed

(CSF) Detect.Detection Process

DE.DP-1:	Roles and responsibilities for detection are well defined to ensure accountability
DE.DP-2:	Detection activities comply with all applicable requirements
DE.DP-3:	Detection processes are tested
DE.DP-4:	Event detection information is communicated
DE.DP-5:	Detection processes are continuously improved

Respond

(CSF) Respond.Response Planning

RS.RP-1:	Response plan is executed during or after an event

(CSF) Respond.Communications

RS.CO-1:	Personnel know their roles and order of operations when a response is needed
RS.CO-2:	Incidents are reported consistent with established criteria
RS.CO-3:	Information is shared consistent with response plans
RS.CO-4:	Coordination with stakeholders occurs consistent with response plans
RS.CO-5:	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness

(CSF) Respond.Analysis

RS.AN-1:	Notifications from detection systems are investigated
RS.AN-2:	The impact of the incident is understood
RS.AN-3:	Forensics are performed
RS.AN-4:	Incidents are categorized consistent with response plans
RS.AN-5:	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)

(CSF) Respond.Mitigation

RS.MI-1:	Incidents are contained
RS.MI-2:	Incidents are mitigated
RS.MI-3:	Newly identified vulnerabilities are mitigated or documented as accepted risks

(CSF) Respond.Improvements

RS.IM-1:	Response plans incorporate lessons learned
RS.IM-2:	Response strategies are updated

Recover

(CSF) Recover.Recovery Planning

RC.RP-1:	Recovery plan is executed during or after a cybersecurity incident

(CSF) Recover.Improvements

RC.IM-1:	Recovery plans incorporate lessons learned
RC.IM-2:	Recovery strategies are updated

(CSF) Recover.Communications

RC.CO-1:	Public relations are managed
RC.CO-2:	Reputation is repaired after an incident
RC.CO-3:	Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

Privacy

Privacy

PC - 1:	Does your organization have a privacy officer?
PC - 2:	Does your organization have clearly defined processes to report a breach of PII/PHI?

Cybersecurity Automation & Orchestration Capabilities

Cybersecurity Automation & Orchestration

(Automation) Question 1:	Security Information and Event Management (SIEM) tools are fully implemented, monitored, and managed.
(Automation) Question 2:	Identity and Access Management (IAM) tools are fully implemented, monitored, and managed.
(Automation) Question 3:	Two factor authentication has been fully implemented.
(Automation) Question 4:	Mobile Device Management (MDM) tools are fully implemented for the administration of mobile devices.
(Automation) Question 5:	Vulnerability assessment tools are fully implemented, monitored, and managed.
(Automation) Question 6:	Intrusion Defense System (IDS) tools are fully implemented.
(Automation) Question 7:	Intrusion Prevention System (IPS) tools are fully implemented.
(Automation) Question 8:	End point protection tools are fully implemented to monitor and analyze network endpoints.
(Automation) Question 9:	Automated tools are used to manage physical IT assets (i.e., inventory and tracking of all software or hardware within an IT environment).
(Automation) Question 10:	Automated tools are used to manage and control removable media.
(Automation) Question 11:	Automated tools are used to encrypt sensitive data in transit between networks.
(Automation) Question 12:	Automated tools are used to create and maintain baseline configuration/change control information.
(Automation) Question 13:	Automated tools are used to conduct and test system backups.
(Automation) Question 14:	Penetration tests are performed to exploit identified vulnerabilities.
(Automation) Question 15:	Antiviral tools are implemented, monitored, and managed.
(Automation) Question 16:	Automated methods are used to integrate disparate security systems.

Post Survey Questions

General

(Post Survey) Question 1:	What are your top 5 security concerns?
(Post Survey) Question 2:	Were you able to answer all of the assessment questions?
(Post Survey) Question 3:	How long did it take you to complete this assessment (including time spent researching answers off-line)
(Post Survey) Question 4:	Are you completing the 2019 NCSR to meet the Homeland Security Grant Program (HGSP) requirement?

History Log

View History Log

Comments

Question Name	Submitter	Date	Comment	Attachment
No Records Found				