Center for Internet Security®

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

CIS Services®

CIS CyberMarket®

Contact Information

cisecurity.org/ms-isac
info@msisac.org
soc@msisac.org
ncsr@cisecurity.org
518.266.3460

In an effort to assist State, Local, Tribal & Territorial (SLTT) governments in advancing their cybersecurity practices, the Multi-State Information Sharing & Analysis Center (MS-ISAC) has mapped the following services and resources to the NIST Cybersecurity Framework (NIST CSF): MS-ISAC Services, CIS Services, Policy Templates, and additional open source documents. Some services and resources are free to MS-ISAC members (MS-ISAC membership is always free to all SLTTs) and others are affordable for-fee services for SLTTs available through CIS Services and CIS CyberMarket.

MS-ISAC is offering this guide to the SLTT community, as a resource to assist with the application and advancement of establishing best practices, implementing cybersecurity policies, and increasing overall cybersecurity maturity. This resource guide can also be used after completing the Nationwide Cybersecurity Review (NCSR) to identify and prioritize improvements. In addition, a library of free training is available to all SLTT governments as part of the Federal Virtual Training Environment (FedVTE): https://fedvte.usalearning.gov.

Functions Key

Identify

The activities under this functional area are key for an organization's understanding of their current internal culture, infrastructure, and risk tolerance. This functional area tends to be one of the lowest-rated functions for many organizations. Immature capabilities in the Identify Function may hinder an organization's ability to effectively apply risk management principles for cybersecurity. By incorporating sound risk management principles into cybersecurity programs, organizations will be able to continuously align their efforts towards protecting their most valuable assets against the most relevant risks.

Protect

The activities under the Protect Function pertain to different methods and activities that reduce the likelihood of cybersecurity events from happening and ensure that the appropriate controls are in place to deliver critical services. These controls are focused on preventing cybersecurity events from occurring through common attack vectors, including attacks targeting users and attacks leveraging inherent weakness in applications and network communication.

Detect

The quicker an organization is able to detect a cybersecurity incident, the better positioned it is to be able to remediate the problem and reduce the consequences of the event. Activities found within the Detect Function pertain to an organization's ability to identify incidents. These controls are becoming more important as the quantity of logs and events occurring within an environment can be overwhelming to handle and can make it difficult to identify the key concerns. This function continues to represent the largest maturity gap between state and local governments.

Respond

An organization's ability to quickly and appropriately respond to an incident plays a large role in reducing the incident's consequences. As such, the activities within the Respond Function examine how an organization plans, analyzes, communicates, mitigates, and improves its response capabilities. For many organizations, integration and cooperation with other entities is key. Many organizations do not have the internal resources to handle all components of incident response. One example is the ability to conduct forensics after an incident, which helps organizations identify and remediate the original attack vector. This gap can be addressed through resource sharing within the SLTT community and leveraging organizations such as MS-ISAC and DHS's Cybersecurity and Infrastructure Security Agency (CISA), which have dedicated resources to provide incident response at no cost to the victim.

Recover

Activities within the Recover Function pertain to an organization's ability to return to its baseline after an incident has occurred. Such controls are focused not only on activities to recover from the incident, but also on many of the components dedicated to managing response plans throughout their lifecycle.

Category	Subcategory	MS-ISAC Service or Resource Guide (No Cost)	CIS Service or Resource Guide (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	Policy Template
Function: Identify						
ID.AM-1	Physical devices and systems within the organization are inventoried	↗ First Steps in Establishing Essential Cyber Hygiene			↗ Nmap ↗ OpenVAS ↗ SnipeIT	↗ Acceptable Use of Information Technology Resource Policy ↗ Access Control Policy ↗ Account Management/Access Control Standard ↗ Identification and Authentication Policy ↗ Information Security Policy ↗ Security Assessment and Authorization Policy ↗ Security Awareness and Training Policy
ID.AM-2	Software platforms and applications within the organization are inventoried	↗ First Steps in Establishing Essential Cyber Hygiene			↗ SnipeIT	↗ Acceptable Use of Information Technology Resource Policy ↗ Access Control Policy ↗ Account Management/Access Control Standard ↗ Identification and Authentication Policy ↗ Information Security Policy ↗ Security Assessment and Authorization Policy ↗ Security Awareness and Training Policy
ID.AM-3	Organizational communication and data flows are mapped	↗ First Steps in Establishing Essential Cyber Hygiene			↗ Draw.io	
ID.AM-4	External information systems are catalogued	↗ First Steps in Establishing Essential Cyber Hygiene				↗ System and Communications Protection Policy
ID.AM-5	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	↗ First Steps in Establishing Essential Cyber Hygiene				↗ Information Classification Standard ↗ Information Security Policy
ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	↗ First Steps in Establishing Essential Cyber Hygiene				↗ Acceptable Use of Information Technology Resource Policy ↗ Information Security Policy ↗ Security Awareness and Training Policy
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					

Category	Subcategory	MS-ISAC Service or Resource Guide (No Cost)	CIS Service or Resource Guide (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	Policy Template
ID.GV-1	Organizational information security policy is established					
ID.GV-2	Information security roles and responsibilities are coordinated and aligned with internal roles and external partners				↗ Eramba GRC	
ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed				↗ Eramba GRC	
ID.GV-4	Governance and risk management processes address cybersecurity risks	↗ Malicious Domain Blocking and Reporting (MDBR) ↗ MS-ISAC Risk Assessment Guide			↗ Eramba GRC	
ID.RA-1	Asset vulnerabilities are identified and documented	↗ First Steps in Establishing Essential Cyber Hygiene ↗ MS-ISAC Risk Assessment Guide	↗ CIS-CAT Pro	↗ Network Penetration Test ↗ Vulnerability Assessment ↗ Web Application Penetration Test	↗ Nmap ↗ OpenVAS	
ID.RA-2	Threat and vulnerability information is received from information sharing forums and sources	↗ MS-ISAC Membership ↗ Malicious Domain Blocking and Reporting (MDBR) ↗ First Steps in Establishing Essential Cyber Hygiene ↗ MS-ISAC Risk Assessment Guide			↗ Nmap ↗ OpenVAS	
ID.RA-3	Threats, both internal and external, are identified and documented	↗ MS-ISAC Membership ↗ Malicious Domain Blocking and Reporting (MDBR) ↗ First Steps in Establishing Essential Cyber Hygiene ↗ MS-ISAC Risk Assessment Guide		↗ Network Penetration Test ↗ Vulnerability Assessment		
ID.RA-4	Potential business impacts and likelihoods are identified	↗ MS-ISAC Membership ↗ First Steps in Establishing Essential Cyber Hygiene ↗ MS-ISAC Risk Assessment Guide	↗ CIS-RAM	↗ Network Penetration Test ↗ Vulnerability Assessment ↗ Web Application Penetration Test		
ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	↗ MS-ISAC Membership ↗ First Steps in Establishing Essential Cyber Hygiene ↗ MS-ISAC Risk Assessment Guide	↗ CIS-CAT Pro ↗ CIS Benchmarks	↗ Network Penetration Test ↗ Vulnerability Assessment ↗ Web Application Penetration Test		
ID.RA-6	Risk responses are identified and prioritized	↗ Malicious Domain Blocking and Reporting (MDBR) ↗ First Steps in Establishing Essential Cyber Hygiene ↗ MS-ISAC Risk Assessment Guide	↗ CIS-RAM			

Category	Subcategory	MS-ISAC Service or Resource Guide (No Cost)	CIS Service or Resource Guide (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	Policy Template
ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders	↗ MS-ISAC Risk Assessment Guide				↗ Information Security Policy ↗ Information Security Risk Management Standard ↗ Risk Assessment Policy
ID.RM-2	Organizational risk tolerance is determined and clearly expressed					
ID.RM-3	The organization's determination of risk tolderance is informed by its role in critical infrastructure and sector specific risk analysis					
ID.SC-1	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	↗ Supply Chain Cybersecurity Resources Guide	↗ Guide for Ensuring Security in Election Technology Procurements ↗ Managing Cybersecurity Supply Chain Risks in Election Technology: A Guide for Election Technology Providers			
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	↗ Supply Chain Cybersecurity Resources Guide	↗ Guide for Ensuring Security in Election Technology Procurements ↗ Managing Cybersecurity Supply Chain Risks in Election Technology: A Guide for Election Technology Providers			↗ Identification and Authentication Policy ↗ Security Assessment and Authorization Policy ↗ Systems and Services Acquisition Policy ↗ Monitoring Vendor Performance and Compliance Policy Template ↗ Vendor Acquisition and Selection Policy Template
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.	↗ Supply Chain Cybersecurity Resources Guide	↗ Guide for Ensuring Security in Election Technology Procurements ↗ Managing Cybersecurity Supply Chain Risks in Election Technology: A Guide for Election Technology Providers			
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.	↗ Supply Chain Cybersecurity Resources Guide	↗ Guide for Ensuring Security in Election Technology Procurements ↗ Managing Cybersecurity Supply Chain Risks in Election Technology: A Guide for Election Technology Providers			↗ Identification and Authentication Policy ↗ Security Assessment and Authorization Policy ↗ Systems and Services Acquisition Policy ↗ Monitoring Vendor Performance and Compliance Policy Template ↗ Vendor Acquisition and Selection Policy Template
ID.SC-5	Response and recovery planning and testing are conducted with suppliers and third-party providers	↗ Supply Chain Cybersecurity Resources Guide	↗ Guide for Ensuring Security in Election Technology Procurements ↗ Managing Cybersecurity Supply Chain Risks in Election Technology: A Guide for Election Technology Providers			↗ Computer Security Threat Response Policy ↗ Cyber Incident Response Standard ↗ Incident Response Policy ↗ Systems and Services Acquisition Policy ↗ Monitoring Vendor Performance and Compliance Policy Template ↗ Vendor Acquisition and Selection Policy Template

Category	Subcategory	MS-ISAC Service or Resource Guide (No Cost)	CIS Service or Resource Guide (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	Policy Template
Function: Protect						
PR.AC-1	Identities and credentials are managed for authorized devices and users	↗ First Steps in Establishing Essential Cyber Hygiene				↗ Access Control Policy ↗ Account Management/Access Control Policy ↗ Authentication Tokens Standard ↗ Configuration Management Policy ↗ Identification and Authentication Policy ↗ Sanitization Secure Disposal Standard ↗ Secure Configuration Standard ↗ Secure System Development Life Cycle Standard
PR.AC-2	Physical access to assets is managed and protected	↗ First Steps in Establishing Essential Cyber Hygiene				
PR.AC-3	Remote access is managed	↗ First Steps in Establishing Essential Cyber Hygiene			↗ OpenVPN	↗ Access Control Policy ↗ Account Management/Access Control Policy ↗ Authentication Tokens Standard ↗ Configuration Management Policy ↗ Identification and Authentication Policy ↗ Sanitization Secure Disposal Standard ↗ Secure Configuration Standard ↗ Secure System Development Life Cycle Standard
PR.AC-4	Access permissions are managed, incorporating the principles of least privilege and separation of duties	↗ First Steps in Establishing Essential Cyber Hygiene			↗ OpenNAC ↗ PacketFence	↗ Access Control Policy ↗ Account Management/Access Control Standard ↗ Configuration Management Policy ↗ Identification and Authentication Policy ↗ Sanitization Secure Disposal Standard ↗ Secure Configuration Standard ↗ Secure System Development Life Cycle Standard
PR.AC-5	Network integrity is protected, incorporating network segregation where appropriate	↗ First Steps in Establishing Essential Cyber Hygiene			↗ pfSense ↗ Snort ↗ Suricata ↗ OpenNAC ↗ PacketFence	↗ 802.11 Wireless Network Security Standard ↗ Mobile Device Security ↗ System and Information Integrity Policy
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	↗ First Steps in Establishing Essential Cyber Hygiene				
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	↗ First Steps in Establishing Essential Cyber Hygiene				

Category	Subcategory	MS-ISAC Service or Resource Guide (No Cost)	CIS Service or Resource Guide (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	Policy Template
PR.AT-1	All users are informed and trained	↗ MS-ISAC Membership				↗ Acceptable Use of Information Technology Resources Policy ↗ Information Security Policy ↗ Personnel Security Policy ↗ Physical and Environmental Protection Policy ↗ Security Awareness and Training Policy
PR.AT-2	Privileged users understand roles & responsibilities				↗ Eramba GRC	
PR.AT-3	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities					
PR.AT-4	Senior executives understand roles & responsibilities				↗ Eramba GRC	
PR.AT-5	Physical and information security personnel understand roles & responsibilities				↗ Eramba GRC	
PR.DS-1	Data-at-rest is protected	↗ First Steps in Establishing Essential Cyber Hygiene				
PR.DS-2	Data-in-transit is protected	↗ First Steps in Establishing Essential Cyber Hygiene				↗ Computer Security Threat Response Policy ↗ Cyber Incident Response Standard ↗ Encryption Standard ↗ Incident Response Policy ↗ Information Security Policy ↗ Maintenance Policy ↗ Media Protection Policy ↗ Mobile Device Security ↗ Patch Management Standard
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	↗ First Steps in Establishing Essential Cyber Hygiene				↗ Access Control Policy ↗ Account Management/Access Control Standard ↗ Authentication Tokens Standard ↗ Configuration Management Policy ↗ Identification and Authentication Policy ↗ Sanitization Secure Disposal Standard ↗ Secure Configuration Standard ↗ Secure System Development Life Cycle Standard
PR.DS-4	Adequate capacity to ensure availability is maintained	↗ First Steps in Establishing Essential Cyber Hygiene				
PR.DS-5	Protections against data leaks are implemented	↗ First Steps in Establishing Essential Cyber Hygiene			↗ OpenDLP	
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	↗ First Steps in Establishing Essential Cyber Hygiene			↗ Tripwire ↗ AIDE	
PR.DS-7	The development and testing environment(s) are separate from the production environment	↗ First Steps in Establishing Essential Cyber Hygiene			↗ Agnito ↗ W3AF ↗ Wapiti	

Category	Subcategory	MS-ISAC Service or Resource Guide (No Cost)	CIS Service or Resource Guide (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	Policy Template
PR.DS-8	Integrity checking mechanisms are used to verify hardware integrity	↗ First Steps in Establishing Essential Cyber Hygiene				↗ System and Information Integrity Policy
PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained	↗ First Steps in Establishing Essential Cyber Hygiene	↗ CIS-CAT Pro		↗ DMARC	↗ Access Control Policy ↗ Account Management/Access Control Standard ↗ Authentication Tokens Standard ↗ Configuration Management Policy ↗ Identification and Authentication Policy ↗ Sanitization Secure Disposal Standard ↗ Secure Configuration Standard ↗ Secure System Development Life Cycle Standard
PR.IP-2	A System Development Life Cycle to manage systems is implemented	↗ First Steps in Establishing Essential Cyber Hygiene				
PR.IP-3	Configuration change control processes are in place	↗ First Steps in Establishing Essential Cyber Hygiene	↗ CIS-CAT Pro			
PR.IP-4	Backups of information are conducted, maintained, and tested periodically	↗ First Steps in Establishing Essential Cyber Hygiene				↗ Computer Security Threat Response Policy ↗ Cyber Incident Response Standard ↗ Encryption Standard ↗ Incident Response Policy ↗ Information Security Policy ↗ Maintenance Policy ↗ Media Protection Policy ↗ Mobile Device Security ↗ Patch Management Standard
PR.IP-5	Policy and regulations regarding the physical operating environment for organizational assets are met	↗ First Steps in Establishing Essential Cyber Hygiene				
PR.IP-6	Data is destroyed according to policy	↗ First Steps in Establishing Essential Cyber Hygiene				↗ Maintenance Policy ↗ Media Protection Policy ↗ Sanitization Secure Disposal Standard
PR.IP-7	Protection processes are continuously improved	↗ First Steps in Establishing Essential Cyber Hygiene				
PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties	↗ First Steps in Establishing Essential Cyber Hygiene				
PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	↗ First Steps in Establishing Essential Cyber Hygiene				↗ Computer Security Threat Response Policy ↗ Cyber Incident Response Standard ↗ Incident Response Policy ↗ Planning Policy
PR.IP-10	Response and recovery plans are tested	↗ First Steps in Establishing Essential Cyber Hygiene				↗ Computer Security Threat Response Policy ↗ Cyber Incident Response Standard ↗ Incident Response Policy ↗ Planning Policy
PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	↗ First Steps in Establishing Essential Cyber Hygiene				

Category	Subcategory	MS-ISAC Service or Resource Guide (No Cost)	CIS Service or Resource Guide (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	Policy Template
PR.IP-12	A vulnerability management plan is developed and implemented	↗ First Steps in Establishing Essential Cyber Hygiene			↗ OpenVAS	
PR.MA-1	Maintenance and repair of organizational assets is performed and logged in a timely manner, 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				↗ Snort ↗ Suricata	↗ Maintenance Policy ↗ Remote Access Standard ↗ Security Logging Standard
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	↗ First Steps in Establishing Essential Cyber Hygiene	↗ CIS SecureSuite		↗ OSSIM	↗ Access Control Policy ↗ Account Management/Access Control Standard ↗ Authentication Tokens Standard ↗ Configuration Management Policy ↗ Identification and Authentication Policy ↗ Sanitization Secure Disposal Standard ↗ Secure Configuration Standard ↗ Secure System Development Life Cycle Standard ↗ Security Logging Standard
PR.PT-2	Removable media is protected and its use restricted according to policy	↗ First Steps in Establishing Essential Cyber Hygiene				↗ Acceptable Use of Technology Resources Policy ↗ Media Protection Policy ↗ Mobile Device Security
PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality	↗ First Steps in Establishing Essential Cyber Hygiene				
PR.PT-4	Communications and control networks are protected	↗ First Steps in Establishing Essential Cyber Hygiene			↗ Nmap ↗ OpenVAS	↗ Encryption Standard ↗ Information Security Policy ↗ Maintenance Policy ↗ Media Protection Policy ↗ Mobile Device Security ↗ System and Communications Protection Policy
PR.PT-5	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	↗ First Steps in Establishing Essential Cyber Hygiene				

Category	Subcategory	MS-ISAC Service or Resource Guide (No Cost)	CIS Service or Resource Guide (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	Policy Template
Function: Detect						
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	↗ First Steps in Establishing Essential Cyber Hygiene			↗ Snort ↗ Suricata	
DE.AE-2	Detected events are analyzed to understand attack targets and methods	↗ First Steps in Establishing Essential Cyber Hygiene ↗ Malicious Domain Blocking and Reporting (MDBR)		↗ Albert Network Monitoring ↗ Endpoint Security Services (ESS)		
DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors	↗ First Steps in Establishing Essential Cyber Hygiene			↗ OSSIM	↗ Auditing and Accountability Standard ↗ Security Logging Standard ↗ System and Information Integrity Policy ↗ Vulnerability Scanning Standard
DE.AE-4	Impact of events is determined	↗ First Steps in Establishing Essential Cyber Hygiene			↗ OSSIM	
DE.AE-5	Incident alert thresholds are established	↗ First Steps in Establishing Essential Cyber Hygiene			↗ Logstash ↗ Graylog	
DE.CM-1	The network is monitored to detect potential cybersecurity events	↗ First Steps in Establishing Essential Cyber Hygiene		↗ Albert Network Monitoring ↗ Endpoint Security Services (ESS)	↗ Zeek ↗ Snort ↗ Suricata ↗ Quad9	↗ Encryption Standard ↗ Information Security Policy ↗ Maintenance Policy ↗ Media Protection Policy ↗ Mobile Device Security ↗ Patch Management Standard ↗ Security Assessment and Authorization Policy ↗ Vulnerability Scanning Standard
DE.CM-2	The physical environment is monitored to detect potential cybersecurity events	↗ First Steps in Establishing Essential Cyber Hygiene				
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	↗ First Steps in Establishing Essential Cyber Hygiene ↗ Malicious Domain Blocking and Reporting (MDBR)			↗ Zabbix	
DE.CM-4	Malicious code is detected	↗ First Steps in Establishing Essential Cyber Hygiene		↗ Albert Network Monitoring	↗ ClamAV	↗ Auditing and Accountability Standard ↗ Secure Coding Standard ↗ Security Logging Standard ↗ System and Information Integrity Policy ↗ Vulnerability Scanning Standard
DE.CM-5	Unauthorized mobile code is detected	↗ First Steps in Establishing Essential Cyber Hygiene				
DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	↗ First Steps in Establishing Essential Cyber Hygiene		↗ Albert Network Monitoring		
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	↗ First Steps in Establishing Essential Cyber Hygiene ↗ Malicious Domain Blocking and Reporting (MDBR)			↗ Quad9	↗ Auditing and Accountability Standard ↗ Security Logging Standard ↗ System and Information Integrity Policy ↗ Vulnerability Scanning Standard

Category	Subcategory	MS-ISAC Service or Resource Guide (No Cost)	CIS Service or Resource Guide (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	Policy Template
DE.CM-8	Vulnerability scans are performed	↗ First Steps in Establishing Essential Cyber Hygiene	↗ CIS-CAT Pro	↗ Vulnerability Management Program (VMP)	↗ Nmap, OpenVAS	
DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability					↗ Computer Security Threat Response Policy ↗ Cyber Incident Response Standard ↗ Incident Response Policy ↗ Information Security Risk Management Standard
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 to appropriate parties	↗ Malicious Domain Blocking and Reporting (MDBR)		↗ Albert Network Monitoring		↗ Computer Security Threat Response Policy ↗ Cyber Incident Response Standard ↗ Incident Response Policy ↗ Information Security Risk Management Standard
DE.DP-5	Detection processes are continuously improved			↗ Albert Network Monitoring		

Category	Subcategory	MS-ISAC Service or Resource Guide (No Cost)	CIS Service or Resource Guide (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	Policy Template
Function: Respond						
RS.RP-1	Response plan is executed during or after an event				↗ TheHive	↗ Computer Security Threat Response Policy ↗ Cyber Incident Response Standard ↗ Incident Response Policy ↗ Planning Policy
RS.CO-1	Personnel know their roles and order of operations when a response is needed					↗ Computer Security Threat Response Policy ↗ Cyber Incident Response Standard ↗ Incident Response Policy
RS.CO-2	Events are reported consistent with established criteria	↗ Malicious Domain Blocking and Reporting (MDBR)				↗ Computer Security Threat Response Policy ↗ Cyber Incident Response Standard ↗ Incident Response Policy
RS.CO-3	Information is shared consistent with response plans					↗ Computer Security Threat Response Policy ↗ Cyber Incident Response Standard ↗ Incident Response Policy
RS.CO-4	Coordination with stakeholders occurs consistent with response plans	↗ Malicious Domain Blocking and Reporting (MDBR)				↗ Computer Security Threat Response Policy ↗ Cyber Incident Response Standard ↗ Incident Response Policy
RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	↗ Malicious Domain Blocking and Reporting (MDBR)				↗ Computer Security Threat Response Policy ↗ Cyber Incident Response Standard ↗ Incident Response Policy
RS.AN-1	Notifications from detection systems are investigated	↗ First Steps in Establishing Essential Cyber Hygiene				
RS.AN-2	The impact of the incident is understood	↗ 24/7 Security Operations Center (SOC) ↗ First Steps in Establishing Essential Cyber Hygiene				
RS.AN-3	Forensics are performed	↗ Computer Emergency Response Team (CERT) Forensic Analysis ↗ First Steps in Establishing Essential Cyber Hygiene				
RS.AN-4	Incidents are categorized consistent with response plans	↗ First Steps in Establishing Essential Cyber Hygiene				↗ Computer Security Threat Response Policy ↗ Cyber Incident Response Standard ↗ Incident Response Policy
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)	↗ First Steps in Establishing Essential Cyber Hygiene			↗ Nmap ↗ OpenVAS	

Category	Subcategory	MS-ISAC Service or Resource Guide (No Cost)	CIS Service or Resource Guide (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	Policy Template
RS.MI-1	Incidents are contained	↗ Computer Emergency Response Team (CERT) Incident Response ↗ First Steps in Establishing Essential Cyber Hygiene				
RS.MI-2	Incidents are mitigated	↗ Computer Emergency Response Team (CERT) Incident Response ↗ First Steps in Establishing Essential Cyber Hygiene				
RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks	↗ First Steps in Establishing Essential Cyber Hygiene	↗ CIS Controls ↗ CIS-CAT Pro			
RS.IM-1	Response plans incorporate lessons learned					↗ Computer Security Threat Response Policy ↗ Cyber Incident Response Standard ↗ Incident Response Policy
RS.IM-2	Response strategies are updated					↗ Computer Security Threat Response Policy ↗ Cyber Incident Response Standard ↗ Incident Response Policy

Category	Subcategory	MS-ISAC Service or Resource Guide (No Cost)	CIS Service or Resource Guide (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	Policy Template

Function: **Recover**

RC.RP-1	Recovery plan is executed during or after an event					↗ Computer Security Threat Response Policy ↗ Contingency Planning Policy ↗ Cyber Incident Response Standard ↗ Incident Response Policy
RC.IM-1	Recovery plans incorporate lessons learned					↗ Computer Security Threat Response Policy ↗ Contingency Planning Policy ↗ Cyber Incident Response Standard ↗ Incident Response Policy
RC.IM-2	Recovery strategies are updated					↗ Computer Security Threat Response Policy ↗ Contingency Planning Policy ↗ Cyber Incident Response Standard ↗ Incident Response Policy
RC.CO-1	Public relations are managed					↗ Computer Security Threat Response Policy ↗ Cyber Incident Response Standard ↗ Incident Response Policy
RC.CO-2	Reputation after an event is repaired					↗ Computer Security Threat Response Policy ↗ Cyber Incident Response Standard ↗ Incident Response Policy
RC.CO-3	Recovery activities are communicated to internal stakeholders and executive and management teams					↗ Computer Security Threat Response Policy ↗ Cyber Incident Response Standard ↗ Incident Response Policy