Center for Internet Security®

Confidence in the Connected World

MS-ISAC®

Multi-State Information Sharing & Analysis Center®

Contact Information

www.cisecurity.org/ms-isac
info@msisac.org
soc@msisac.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, FedVTE Training, SANS 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.

CIS Services®

CIS CyberMarket®

Functions Key

Identify Function

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 Function

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 Function

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 Function

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 National Cybersecurity and Communications Integration Center (NCCIC), which have dedicated resources to provide incident response at no cost to the victim.

Recover Function

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.

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
IDENTIFY	ID.AM-1	Physical devices and systems within the organization are inventoried				Nmap OpenVAS SnipeIT	• Cyber Risk Management for Managers; • CMaaS Overview; • CMaaS Technical Overview Course; • CMaaS Transition Classroom Sessions; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; • (ISC)2(TM) Systems Security Certified Practitioner;	
	ID.AM-2	Software platforms and applications within the organization are inventoried				SnipeIT	• Cyber Risk Management for Managers; • CMaaS Overview; • CMaaS Technical Overview Course; • CMaaS Transition Classroom Sessions; • D B Evaluations using AppDetectivePro & dbProtect; • Dynamic Testing using HPE WebInspect; • Static Code Analysis using HPE Fortify; • Static Code Analysis using Synopsis Coverity; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • CDM Module 3: Software Asset Management; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; • (ISC)2(TM) Systems Security Certified Practitioner;	
	ID.AM-3	Organizational communication and data flows are mapped				Draw.io	• Cyber Risk Management for Managers; • CompTIA Advanced Security Practitioner; • Cisco CCENT Self-Study Prep; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; • (ISC)2 (TM) CISSP Concentration: ISSEP Prep;	
	ID.AM-4	External information systems are catalogued					• Cyber Risk Management for Managers; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2(TM) Systems Security Certified Practitioner;	
	ID.AM-5	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value					• Cyber Risk Management for Managers; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • CDM Module 2: Hardware Asset; • CDM Module 3: Software Asset Management; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; • (ISC)2 (TM) CISSP Concentration: ISSEP Prep;	SANS: Acquisition Assessment
	ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established					• The Election Official as IT Manager; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Cybersecurity Overview for Managers; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; • (ISC)2 (TM) CISSP Concentration: ISSEP Prep; • (ISC)2 (TM) CISSP: ISSMP Prep 2018;	

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
IDENTIFY	ID.BE-1	The organization's role in the supply chain is identified and communicated					• ISACA Certified Information Security Manager (CISM) Prep;	
	ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated					• 101 - Critical Infrastructure Protection;	
	ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated					• Cyber Risk Management for Managers; • ISACA Certified Information Security Manager (CISM) Prep; • 101 - Critical Infrastructure Protection; • Cybersecurity Overview for Managers; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; • (ISC)2 (TM) CISSP Concentration: ISSEP Prep; • (ISC)2 (TM) CISSP: ISSMP Prep 2018;	
	ID.BE-4	Dependencies and critical functions for delivery of critical services are established					• Cyber Risk Management for Managers; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • 101 - Critical Infrastructure Protection; • CompTIA Security +; • (ISC)2 (TM) CISSP Concentration: ISSEP Prep;	
	ID.BE-5	Resilience requirements to support delivery of critical services are established					• 101 - Critical Infrastructure Protection; • CompTIA Security +; • (ISC)2 (TM) CISSP Concentration: ISSEP Prep;	
	ID.GV-1	Organizational information security policy is established					• ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Cybersecurity Overview for Managers; • Emerging Cybersecurity Threats; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; • (ISC)2 (TM) CISSP Concentration: ISSEP Prep; • (ISC)2 (TM) CISSP: ISSMP Prep 2018;	
	ID.GV-2	Information security roles & responsibilities are coordinated and aligned with internal roles and external partners				Eramba GRC	• Cyber Risk Management for Managers; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • 101 - Critical Infrastructure Protection; • Cybersecurity Overview for Managers; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; • (ISC)2 (TM) CISSP Concentration: ISSEP Prep; • (ISC)2 (TM) CISSP: ISSMP Prep 2018;	

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
IDENTIFY	ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed				Eramba GRC	• EC-Council Certified Ethical Hacker (CEHv9) Self-Study Prep; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Cybersecurity Overview for Managers; • Emerging Cybersecurity Threats; • 101 Reverse Engineering; • (ISC)2 (TM) CISSP Concentration: ISSEP Prep; • (ISC)2 (TM) CISSP: ISSMP Prep 2018;	
	ID.GV-4	Governace and risk management processes address cybersecurity risks				Eramba GRC	• Cyber Risk Management for Technicians; • Cyber Risk Management for Managers; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Cybersecurity Overview for Managers; • CompTIA Advanced Security Practitioner; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; • (ISC)2 (TM) CISSP Concentration: ISSEP Prep; • (ISC)2 (TM) CISSP: ISSMP Prep 2018; • (ISC)2 (TM) Systems Security Certified Practitioner;	
	ID.RA-1	Asset vulnerabilities are identified and documented	Vulnerability Management Program (VMP)	CIS-CAT Pro	Network Penetration Test Vulnerability Assessment Web Application Penetration Test	Nmap OpenVAS	• Cyber Risk Management for Technicians; • Cyber Risk Management for Managers; • EC-Council Certified Ethical Hacker (CEHv9) Self-Study Prep; • CMaaS Overview; • CMaaS Technical Overview Course; • CMaaS Transition Classroom Sessions; • DB Evaluations using AppDetectivePro & dbProtect; • Dynamic Testing using HPE WebInspect; • Introduction to Threat Hunting Teams; • Static Code Analysis using HPE Fortify; • Static Code Analysis using Synopsis Coverity; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • CDM Module 5: Vulnerability Management; • CompTIA Advanced Security Practitioner; • CompTIA Cybersecurity Analyst (CySA+) Prep; • Radio Frequency Identification (RFID) Security; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; • (ISC)2 (TM) CISSP: ISSMP Prep 2018;	

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
IDENTIFY	ID.RA-2	Threat and vulnerability information is received from information sharing forums and sources	MS-ISAC Membership			Nmap OpenVAS	• Foundations of Incident Management; • Introduction to Threat Hunting Teams; • 101 - Critical Infrastructure Protection; • CompTIA Cybersecurity Analyst (CySA+) Prep; • CDM Module 5: Vulnerability Management; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; • (ISC)2 (TM) CISSP: ISSMP Prep 2018;	
	ID.RA-3	Threats, both internal and external, are identified and documented	MS-ISAC Membership		Network Penetration Test Vulnerability Assessment		• Cyber Risk Management for Technicians; • Cyber Risk Management for Managers; • EC-Council Certified Ethical Hacker; (CEHv9) Self-Study Prep; • CMaaS Overview; • CMaaS Technical Overview Course; • CMaaS Transition Classroom Sessions; • Foundations of Incident Management; • Introduction to Threat Hunting Teams; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • CompTIA Cybersecurity Analyst (CySA+) Prep; • Cisco CCENT Self-Study Prep; • Cisco CCNA Security Self-Study Prep; • Cyber Awareness Challenge 2019; Cybersecurity Overview for Managers; Emerging Cybersecurity Threats; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; • (ISC)2 (TM) CISSP: ISSMP Prep 2018;	
	ID.RA-4	Potential business impacts and likelihoods are identified	MS-ISAC Membership	CIS-RAM	Network Penetration Test Vulnerability Assessment Web Application Penetration Test		• The Election Official as IT Manager; • Cyber Risk Management for Managers; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • 101 - Critical Infrastructure Protection; CompTIA Advanced Security Practitioner; • Cloud Computing Security; • CompTIA Security +; • Cybersecurity Overview for Managers; (ISC)2 (TM) CISSP (R) Certification Prep 2018; • (ISC)2 (TM) CISSP: ISSMP Prep 2018;	

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
IDENTIFY	ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	MS-ISAC Membership	CIS-CAT Pro CIS Benchmarks	Network Penetration Test Vulnerability Assessment Web Application Penetration Test		• The Election Official as IT Manager; • Cyber Risk Management for Managers; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Cloud Computing Security; • CompTIA Security +; • Cybersecurity Overview for Managers; Emerging Cybersecurity Threats; • 101 - Critical Infrastructure Protection; CompTIA Advanced Security Practitioner; • CompTIA Cybersecurity Analyst (CySA+) Prep; • (ISC)2 (TM) CISSP (R) Certification Prep 2018;	
	ID.RA-6	Risk responses are identified and prioritized		CIS-RAM			• The Election Official as IT Manager; Cyber Risk Management for Managers; ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • CompTIA Advanced Security Practitioner; • CompTIA Cybersecurity Analyst (CySA+) Prep; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; • (ISC)2 (TM) CISSP: ISSMP Prep 2018;	
	ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders					• The Election Official as IT Manager; Cyber Risk Management for Managers; ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Cybersecurity Overview for Managers; CompTIA Advanced Security Practitioner; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; • (ISC)2 (TM) CISSP Concentration: ISSEP Prep; • (ISC)2 (TM) CISSP: ISSMP Prep 2018;	
	ID.RM-2	Organizational risk tolerance is determined and clearly expressed					• The Election Official as IT Manager; Cyber Risk Management for Managers; ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Cybersecurity Overview for Managers; CompTIA Advanced Security Practitioner; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; • (ISC)2 (TM) CISSP Concentration: ISSEP Prep; • (ISC)2 (TM) CISSP: ISSMP Prep 2018;	
	ID.RM-3	The organization's determination of risk tolderance is informed by its role in critical infrastructure and sector specific risk analysis					• The Election Official as IT Manager; Cyber Risk Management for Managers; ISACA Certified Information Security Manager (CISM) Prep; • 101 - Critical Infrastructure Protection; CompTIA Advanced Security Practitioner; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; • (ISC)2 (TM) CISSP Concentration: ISSEP Prep;	

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
IDENTIFY	ID.SC-1	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders					• The Election Official as IT Manager; Cyber Risk Management for Managers; ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • CompTIA Advanced Security Practitioner; • Cyber Supply Chain Risk Management; (ISC)2 (TM) CISSP Concentration: ISSEP Prep;	
	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					• CompTIA Advanced Security Practitioner; • Cyber Supply Chain Risk Management; (ISC)2 (TM) CISSP Concentration: ISSEP Prep;	SANS: Acquisition Assessment
	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.					• Cyber Supply Chain Risk Management; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; • (ISC)2 (TM) CISSP: ISSMP Prep 2018;	
	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.					• EC-Council Certified Ethical Hacker (CEHv9) Self-Study Prep; • Cyber Supply Chain Risk Management; CompTIA Advanced Security Practitioner; • Supply Chain Assurance using Sonatype Nexus;	SANS: Acquisition Assessment
	ID.SC-5	Response and recovery planning and testing are conducted with suppliers and third-party providers					• Foundations of Incident Management; CompTIA Advanced Security Practitioner; • Cyber Supply Chain Risk Management; (ISC)2 (TM) CISSP Concentration: ISSEP Prep;	SANS: Security Response Plan

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
PROTECT	PR.AC-1	Identities and credentials are managed for authorized devices and users					• Cyber Risk Management for Managers; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • CompTIA Advanced Security Practitioner; Securing Infrastructure Devices; Cisco CCNA Security Self-Study Prep; • CompTIA Security +; • Windows Operating System Security; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) Systems Security Certified Practitioner; • (ISC)2(TM) Systems Security Certified Practitioner; • Linux Operating System Security;	
	PR.AC-2	Physical access to assets is managed and protected					• Cyber Risk Management for Managers; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • CompTIA Advanced Security Practitioner; CompTIA A+ 220-902 Certification Prep; • CDM Module 2: Hardware Asset; • Securing Infrastructure Devices; • CompTIA Security +; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) Systems Security Certified Practitioner; • (ISC)2(TM) Systems Security Certified Practitioner; • Mobile and Device Security;	
	PR.AC-3	Remote access is managed				⇢ OpenVPN	• CMaaS Technical Overview Course; • Cyber Risk Management for Managers; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • CompTIA Advanced Security Practitioner; CompTIA Network+ N10-007; • Cisco CCNA Security Self-Study Prep; • CompTIA Security +; • Cybersecurity Overview for Managers; Emerging Cybersecurity Threats; • Windows Operating System Security; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) Systems Security Certified Practitioner; • (ISC)2(TM) Systems Security Certified Practitioner; • Mobile and Device Security;	⇢ SANS: Remote Access

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
PROTECT	PR.AC-4	Access permissions are managed, incorporating the principles of least privilege and separation of duties				⇢ OpenNAC ⇢ PacketFence	• Cyber Risk Management for Managers; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • CompTIA Advanced Security Practitioner; CompTIA Network+ N10-007; Securing Infrastructure Devices; • Cisco CCNA Security Self-Study Prep; • CompTIA Security +; • Cybersecurity Overview for Managers; Windows Operating System Security; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) Systems Security Certified Practitioner; • (ISC)2(TM) Systems Security Certified Practitioner; • Linux Operating System Security; • Mobile and Device Security;	
	PR.AC-5	Network integrity is protected, incorporating network segregation where appropriate				⇢ pfSense ⇢ Snort ⇢ Suricata ⇢ OpenNAC ⇢ PacketFence	• CMaaS Technical Overview Course, CMaaS Overview; • CMaaS Technical Overview Course; • CMaaS Transition Classroom Sessions; Demilitarized Zone (DMZ) with IDS/IPS; DNSSEC Training Workshop; IPv6 Security Essentials Course; • ISACA Certified Information Security Manager (CISM) Prep; • Cyber Risk Management for Managers; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • CompTIA Security +; • Cybersecurity Overview for Managers; Emerging Cybersecurity Threats; • Advanced PCAP Analysis and Signature Development (APA); • CompTIA Advanced Security Practitioner; Securing the Network Perimeter; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; LAN Security Using Switch Features;	⇢ SANS: Lab Security ⇢ SANS: Router and Switch Security
	PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions					• ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Windows Operating System Security; • CompTIA Advanced Security Practitioner; (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) Systems Security Certified Practitioner; • (ISC)2(TM) Systems Security Certified Practitioner; • Linux Operating System Security;	

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
PROTECT	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)					• ISACA Certified Information Security Manager (CISM) Prep; • Cyber Risk Management for Managers; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • CompTIA Security +; • Cybersecurity Overview for Managers; Emerging Cybersecurity Threats; • CDM Module 2: Hardware Asset; • CompTIA A+ 220-902 Certification Prep; CompTIA Advanced Security Practitioner; (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) Systems Security Certified Practitioner;	
	PR.AT-1	All users are informed and trained	⇢ MS-ISAC Membership				• Foundations of Incident Management; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Cyber Awareness Challenge 2019; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP: ISSMP Prep 2018;	
	PR.AT-2	Privileged users understand roles & responsibilities				⇢ Eramba GRC	• ISACA Certified Information Security Manager (CISM) Prep; • Cybersecurity Overview for Managers; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; (ISC)2 (TM) CISSP: ISSMP Prep 2018;	
	PR.AT-3	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities					• ISACA Certified Information Security Manager (CISM) Prep; • Cybersecurity Overview for Managers; • (ISC)2 (TM) CISSP Concentration: ISSEP Prep;	
	PR.AT-4	Senior executives understand roles & responsibilities				⇢ Eramba GRC	• The Election Official as IT Manager; • Cyber Risk Management for Managers; • ISACA Certified Information Security Manager (CISM) Prep; • Cybersecurity Overview for Managers; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; (ISC)2 (TM) CISSP: ISSMP Prep 2018;	
	PR.AT-5	Physical and information security personnel understand roles & responsibilities				⇢ Eramba GRC	• The Election Official as IT Manager; • Cyber Risk Management for Managers; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Cybersecurity Overview for Managers; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; (ISC)2 (TM) CISSP: ISSMP Prep 2018;	⇢ SANS: Router and Switch Security

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
PROTECT	PR.DS-1	Data-at-rest is protected					• DB Evaluations using AppDetectivePro & dbProtect; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • CompTIA Advanced Security Practitioner; CompTIA Security +; • Windows Operating System Security; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) Systems Security Certified Practitioner;	
	PR.DS-2	Data-in-transit is protected					• IPv6 Security Essentials Course; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Advanced PCAP Analysis and Signature Development (APA); • Analysis Pipeline; • CompTIA Advanced Security Practitioner; CompTIA Network+ N10-007; • Cloud Computing Security; • CompTIA Security +; • Emerging Cybersecurity Threats; • Windows Operating System Security; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) Systems Security Certified Practitioner; • LAN Security Using Switch Features;	
	PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition					• CMaaS Overview; • CMaaS Technical Overview Course; • CMaaS Transition Classroom Sessions; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • CDM Module 2: Hardware Asset; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; (ISC)2 (TM) Systems Security Certified Practitioner; • (ISC)2(TM) Systems Security Certified Practitioner;	→ SANS: Acquisition Assessment → SANS: Technology Equipment Disposal
	PR.DS-4	Adequate capacity to ensure availability is maintained					• (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep;	

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
PROTECT	PR.DS-5	Protections against data leaks are implemented				⇢ OpenDLP	• CMaaS Overview; • CMaaS Technical Overview Course; • CMaaS Transition Classroom Sessions; • Static Code Analysis using HPE Fortify; • Static Code Analysis using Synopsis Coverity; ISACA Certified Information Security Manager (CISM) Prep; • Advanced PCAP Analysis and Signature Development (APA); • Analysis Pipeline; • CompTIA Advanced Security Practitioner; CompTIA Network+ N10-007;	
	PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity				⇢ Tripwire ⇢ AIDE	• DNSSEC Training Workshop; • Static Code Analysis using HPE Fortify; • Static Code Analysis using Synopsis Coverity; ISACA Certified Information Security Manager (CISM) Prep; • Advanced Windows Scripting; • (ISC)2(TM) Systems Security Certified Practitioner;	
	PR.DS-7	The development and testing environment(s) are separate from the production environment				⇢ Agnito ⇢ W3AF ⇢ Wapiti	• DB Evaluations using AppDetectivePro & dbProtect; • Dynamic Testing using HPE WebInspect; • Static Code Analysis using HPE Fortify; • Static Code Analysis using Synopsis Coverity; Supply Chain Assurance using Sonatype Nexus; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP: ISSMP Prep 2018; • Software Assurance Executive Course (SAE);	⇢ SANS: Lab Security ⇢ SANS: Router and Switch Security
	PR.DS-8	Integrity checking mechanisms are used to verify hardware integrity					• (ISC)2(TM) Systems Security Certified Practitioner;	⇢ SANS: Acquisition Assessment
	PR.IP-1	A baseline configuration of information technology/ industrial control systems is created and maintained		⇢ CIS-CAT Pro			• CMaaS Overview; CMaaS Technical Overview Course; • CMaaS Transition Classroom Sessions; Advanced Windows Scripting; • CompTIA A+ 220-901 Certification Prep; CompTIA A+ 220-902 Certification Prep; CompTIA Advanced Security Practitioner; • CDM Module 4: Configuration Settings Mgt;	

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
PROTECT	PR.IP-2	A System Development Life Cycle to manage systems is implemented					• DB Evaluations using AppDetectivePro & dbProtect; • ISACA Certified Information Security Manager (CISM) Prep; • CompTIA Advanced Security Practitioner; (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; (ISC)2 (TM) CISSP: ISSMP Prep 2018; • (ISC)2 (TM) CISSP: ISSMP Prep 2018; • (ISC)2 (TM) Systems Security Certified Practitioner; • (ISC)2(TM) Systems Security Certified Practitioner; • Software Assurance Executive Course (SAE);	
	PR.IP-3	Configuration change control processes are in place		⇢ CIS-CAT Pro			• CMaaS Overview; • CMaaS Technical Overview Course; • CMaaS Transition Classroom Sessions; • Static Code Analysis using HPE Fortify; • Static Code Analysis using Synopsis Coverity; ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Cybersecurity Overview for Managers; CompTIA Advanced Security Practitioner; Securing Infrastructure Devices; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; (ISC)2 (TM) Systems Security Certified Practitioner; (ISC)2(TM) Systems Security Certified Practitioner; • Software Assurance Executive Course (SAE);	
	PR.IP-4	Backups of information are conducted, maintained, and tested periodically					• Foundations of Incident Management; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Cybersecurity Overview for Managers; CompTIA Security +; • CompTIA Network+ N10-007; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) Systems Security Certified Practitioner;	⇢ SANS: Disaster Recovery Plan
	PR.IP-5	Policy and regulations regarding the physical operating environment for organizational assets are met					• ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • CompTIA Security +; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP: ISSMP Prep 2018; • (ISC)2(TM) Systems Security Certified Practitioner;	

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
PROTECT	PR.IP-6	Data is destroyed according to policy					• ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • CompTIA Security +; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2(TM) Systems Security Certified Practitioner;	SANS: Technology Equipment Disposal
	PR.IP-7	Protection processes are continuously improved					• Static Code Analysis using HPE Fortify; • Static Code Analysis using Synopsis Coverity; ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP: ISSMP Prep 2018; • (ISC)2 (TM) Systems Security Certified Practitioner;	
	PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties					• ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • 101 - Critical Infrastructure Protection; • (ISC)2 (TM) CISSP (R) Certification Prep 2018;	
	PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed					• Foundations of Incident Management; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • 101 - Critical Infrastructure Protection; CompTIA Network+ N10-007; • 101 - Critical Infrastructure Protection; • Cisco CCNA Security Self-Study Prep; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; (ISC)2 (TM) CISSP: ISSMP Prep 2018; • (ISC)2 (TM) Systems Security Certified Practitioner; • (ISC)2(TM) Systems Security Certified Practitioner;	SANS: Data Breach Response SANS: Disaster Recovery Plan SANS: Pandemic Response Planning SANS: Security Response Plan
	PR.IP-10	Response and recovery plans are tested					• EC-Council Certified Ethical Hacker (CEHv9) Self-Study Prep; • Foundations of Incident Management; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • CompTIA Network+ N10-007; • CompTIA Advanced Security Practitioner; (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; (ISC)2 (TM) Systems Security Certified Practitioner; • (ISC)2(TM) Systems Security Certified Practitioner;	SANS: Data Breach Response SANS: Disaster Recovery Plan SANS: Pandemic Response Planning SANS: Security Response Plan

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
PROTECT	PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)					• ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Cybersecurity Overview for Managers; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; (ISC)2 (TM) CISSP: ISSMP Prep 2018;	
	PR.IP-12	A vulnerability management plan is developed and implemented				⇢ OpenVAS	• EC-Council Certified Ethical Hacker (CEHv9) Self-Study Prep; • CMaaS Overview; • CMaaS Technical Overview Course; • CMaaS Transition Classroom Sessions; Dynamic Testing using HPE WebInspect; • ISACA Certified Information Security Manager (CISM) Prep; • Cybersecurity Overview for Managers; • Radio Frequency Identification (RFID) Security; CDM Module 5: Vulnerability Management; (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP: ISSMP Prep 2018;	
	PR.MA-1	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools					• ISACA Certified Information Security Manager (CISM) Prep; CompTIA Advanced Security Practitioner	
	PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access				⇢ Snort ⇢ Suricata	• CompTIA Advanced Security Practitioner; CompTIA Network+ N10-007;	⇢ SANS: Remote Access ⇢ SANS: Remote Access Tools
	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy		⇢ CIS SecureSuite		⇢ OSSIM	• Foundations of Incident Management; • ISACA Certified Information Security Manager (CISM) Prep; • CompTIA Advanced Security Practitioner; • Cisco CCNA Security Self-Study Prep; • CompTIA Security +; • Windows Operating System Security; • (ISC)2 (TM) CISSP (R) Certification Prep 2018;	⇢ SANS: Information Logging Standard
	PR.PT-2	Removable media is protected and its use restricted according to policy					• ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • CompTIA Security +; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) Systems Security Certified Practitioner;	⇢ SANS: Acceptable Use

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
PROTECT	PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality					• ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Emerging Cybersecurity Threats; CompTIA Security +; • Cybersecurity Overview for Managers; CompTIA Advanced Security Practitioner; CompTIA Network+ N10-007; • Securing Infrastructure Devices; • Securing the Network Perimeter; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) Systems Security Certified Practitioner; • (ISC)2(TM) Systems Security Certified Practitioner;	
	PR.PT-4	Communications and control networks are protected				Nmap OpenVAS	• CMaaS Overview; • CMaaS Technical Overview Course; • CMaaS Transition Classroom Sessions; Demilitarized Zone (DMZ) with IDS/IPS; DNSSEC Training Workshop; • ISACA Certified Information Security Manager (CISM) Prep; • Securing Infrastructure Devices; • Securing the Network Perimeter; • Wireless Network Security; • CompTIA Advanced Security Practitioner; CompTIA Network+ N10-007; • Analysis Pipeline; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; Mobile and Device Security;	SANS: Router and Switch Security
	PR.PT-5	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations					• DNSSEC Training Workshop; • Foundations of Incident Management; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Emerging Cybersecurity Threats; • Securing the Network Perimeter; • CompTIA Advanced Security Practitioner; CompTIA Network+ N10-007; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2(TM) Systems Security Certified Practitioner;	SANS: Disaster Recovery Plan SANS: Security Response Plan

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
DETECT	DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed				Snort Suricata	• Cyber Risk Management for Managers; • DB Evaluations using AppDetectivePro & dbProtect; • Dynamic Testing using HPE WebInspect; • ISACA Certified Information Security Manager (CISM) Prep; • Emerging Cybersecurity Threats; • Analysis Pipeline; • (ISC)2 (TM) CISSP Concentration: ISSEP Prep;	
	DE.AE-2	Detected events are analyzed to understand attack targets and methods			Albert Network Monitoring		• EC-Council Certified Ethical Hacker (CEHv9) Self-Study Prep; • Demilitarized Zone (DMZ) with IDS/IPS; • DB Evaluations using AppDetectivePro & dbProtect; • Foundations of Incident Management; • Static Code Analysis using HPE Fortify; • Static Code Analysis using Synopsis Coverity; ISACA Certified Information Security Manager (CISM) Prep; • Emerging Cybersecurity Threats; • Advanced PCAP Analysis and Signature Development (APA); • Analysis Pipeline; • Root Cause Analysis; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) Systems Security Certified Practitioner; • SiLK Traffic Analysis;	
	DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors				OSSIM	• EC-Council Certified Ethical Hacker (CEHv9) Self-Study Prep; • Demilitarized Zone (DMZ) with IDS/IPS; Dynamic Testing using HPE WebInspect; Foundations of Incident Management; • ISACA Certified Information Security Manager (CISM) Prep; • Analysis Pipeline; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; SiLK Traffic Analysis;	SANS: Information Logging Standard
	DE.AE-4	Impact of events is determined				OSSIM	• DB Evaluations using AppDetectivePro & dbProtect; Dynamic Testing using HPE WebInspect; Foundations of Incident Management; CompTIA Advanced Security Practitioner; Root Cause Analysis; (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep;	
	DE.AE-5	Incident alert thresholds are established				Logstash Graylog	• Foundations of Incident Management; Cybersecurity Overview for Managers; • (ISC)2 (TM) CISSP (R) Certification Prep 2018;	

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
DETECT	DE.CM-1	The network is monitored to detect potential cybersecurity events			Albert Network Monitoring	Zeek Snort Suricata	• Cyber Risk Management for Technicians; Cyber Risk Management for Managers; • Demilitarized Zone (DMZ) with IDS/IPS; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Advanced PCAP Analysis and Signature Development (APA); • Analysis Pipeline; • CompTIA Advanced Security Practitioner; (ISC)2 (TM) CISSP (R) Certification Prep 2018;	
	DE.CM-2	The physical environment is monitored to detect potential cybersecurity events					• ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • CompTIA A+ 220-902 Certification Prep; (ISC)2 (TM) CISSP (R) Certification Prep 2018;	
	DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events				Zabbix	• ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • (ISC)2 (TM) CISSP (R) Certification Prep 2018;	
	DE.CM-4	Malicious code is detected			Albert Network Monitoring	ClamAV	• Demilitarized Zone (DMZ) with IDS/IPS; • DB Evaluations using AppDetectivePro & dbProtect; • Dynamic Testing using HPE WebInspect; • Static Code Analysis using HPE Fortify; • Static Code Analysis using Synopsis Coverity; Advanced PCAP Analysis and Signature Development (APA); • Analysis Pipeline; • CompTIA A+ 220-902 Certification Prep; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; SiLK Traffic Analysis;	
	DE.CM-5	Unauthorized mobile code is detected					• DB Evaluations using AppDetectivePro & dbProtect; • Static Code Analysis using HPE Fortify; • Static Code Analysis using Synopsis Coverity; Advanced PCAP Analysis and Signature Development (APA); • Analysis Pipeline; • CompTIA A+ 220-902 Certification Prep; • (ISC)2 (TM) CISSP Concentration: ISSEP Prep; Mobile and Device Security;	
	DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events			Albert Network Monitoring		• Demilitarized Zone (DMZ) with IDS/IPS	

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
DETECT	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed					• Demilitarized Zone (DMZ) with IDS/IPS; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Analysis Pipeline; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2(TM) Systems Security Certified Practitioner;	
	DE.CM-8	Vulnerability scans are performed		⇢ CIS-CAT Pro	⇢ Vulnerability Management Program (VMP)	⇢ Nmap, OpenVAS	• EC-Council Certified Ethical Hacker (CEHv9) Self-Study Prep; • CMaaS Overview; • CMaaS Technical Overview Course; • CMaaS Transition Classroom Sessions; • DB Evaluations using AppDetectivePro & dbProtect; • Dynamic Testing using HPE WebInspect; Introduction to Threat Hunting Teams; • Static Code Analysis using HPE Fortify; • Static Code Analysis using Synopsis Coverity; ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Supply Chain Assurance using Sonatype Nexus; • Cybersecurity Overview for Managers; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP: ISSMP Prep 2018;	
	DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability					• Cyber Risk Management for Managers; • The Election Official as IT Manager; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Cybersecurity Overview for Managers; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; (ISC)2 (TM) CISSP: ISSMP Prep 2018;	
	DE.DP-2	Detection activities comply with all applicable requirements					• ISACA Certified Information Security Manager (CISM) Prep; • Cyber Risk Management for Managers; Analysis Pipeline; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; (ISC)2 (TM) CISSP: ISSMP Prep 2018;	
	DE.DP-3	Detection processes are tested					• Demilitarized Zone (DMZ) with IDS/IPS; • DB Evaluations using AppDetectivePro & dbProtect; • ISACA Certified Information Security Manager (CISM) Prep;	

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
DETECT	DE.DP-4	Event detection information is communicated to appropriate parties			Albert Network Monitoring		• ISACA Certified Information Security Manager (CISM) Prep; • Cyber Risk Management for Managers; • 101 - Critical Infrastructure Protection; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; (ISC)2 (TM) CISSP: ISSMP Prep 2018;	
	DE.DP-5	Detection processes are continuously improved			Albert Network Monitoring		• Demilitarized Zone (DMZ) with IDS/IPS; • DB Evaluations using AppDetectivePro & dbProtect; • ISACA Certified Information Security Manager (CISM) Prep; • Cyber Risk Management for Managers; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep;	
RESPOND	RS.RP-1	Response plan is executed during or after an event				TheHive	• Foundations of Incident Management; • The Election Official as IT Manager; Introduction to Investigation of Digital Assets; ISACA Certified Information Security Manager (CISM) Prep; • Cyber Risk Management for Managers; Cybersecurity Overview for Managers; CompTIA A+ 220-902 Certification Prep; • Root Cause Analysis; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; (ISC)2 (TM) CISSP: ISSMP Prep 2018;	SANS: Security Response Plan
	RS.CO-1	Personnel know their roles and order of operations when a response is needed					• Foundations of Incident Management; Introduction to Investigation of Digital Assets; ISACA Certified Information Security Manager (CISM) Prep; • Cyber Risk Management for Managers; Cybersecurity Overview for Managers; Offensive and Defensive Network Operations; CompTIA A+ 220-902 Certification Prep; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; (ISC)2 (TM) CISSP: ISSMP Prep 2018;	SANS: Data Breach Response SANS: Pandemic Response Planning SANS: Security Response Plan
	RS.CO-2	Events are reported consistent with established criteria					• Foundations of Incident Management; • ISACA Certified Information Security Manager (CISM) Prep; • Cybersecurity Overview for Managers; Offensive and Defensive Network Operations; (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; (ISC)2 (TM) CISSP: ISSMP Prep 2018; • (ISC)2(TM) Systems Security Certified Practitioner;	SANS: Data Breach Response SANS: Pandemic Response Planning SANS: Security Response Plan

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
RESPOND	RS.CO-3	Information is shared consistent with response plans					• Foundations of Incident Management; Introduction to Investigation of Digital Assets; ISACA Certified Information Security Manager (CISM) Prep; • Cybersecurity Overview for Managers; Offensive and Defensive Network Operations; (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; (ISC)2 (TM) CISSP: ISSMP Prep 2018;	→ SANS: Data Breach Response → SANS: Pandemic Response Planning → SANS: Security Response Plan
	RS.CO-4	Coordination with stakeholders occurs consistent with response plans					• Foundations of Incident Management; Introduction to Investigation of Digital Assets; ISACA Certified Information Security Manager (CISM) Prep; • Cybersecurity Overview for Managers; Offensive and Defensive Network Operations; (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; (ISC)2 (TM) CISSP: ISSMP Prep 2018;	→ SANS: Data Breach Response → SANS: Pandemic Response Planning → SANS: Security Response Plan
	RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness					• Foundations of Incident Management; Introduction to Investigation of Digital Assets; ISACA Certified Information Security Manager (CISM) Prep; • Cybersecurity Overview for Managers; Offensive and Defensive Network Operations;	→ SANS: Data Breach Response → SANS: Pandemic Response Planning → SANS: Security Response Plan
	RS.AN-1	Notifications from detection systems are investigated					• Foundations of Incident Management; Introduction to Investigation of Digital Assets; ISACA Certified Information Security Manager (CISM) Prep; • Cyber Risk Management for Managers; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Cybersecurity Overview for Managers; Advanced PCAP Analysis and Signature Development (APA); • Root Cause Analysis; (ISC)2 (TM) CISSP (R) Certification Prep 2018; • SiLK Traffic Analysis;	
	RS.AN-2	The impact of the incident is understood	→ 24/7 Security Operations Center (SOC) → Vulnerability Management Program (VMP) → Computer Emergency Response Team (CERT)				• Dynamic Testing using HPE WebInspect; Foundations of Incident Management; Introduction to Investigation of Digital Assets; ISACA Certified Information Security Manager (CISM) Prep; • Cyber Risk Management for Managers; Cybersecurity Overview for Managers; • (ISC)2 (TM) CISSP Concentration: ISSEP Prep; (ISC)2 (TM) CISSP: ISSMP Prep 2018;	

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
RESPOND	RS.AN-3	Forensics are performed	Computer Emergency Response Team (CERT) Forensic Analysis				• EC-Council Certified Ethical Hacker (CEHv9) Self-Study Prep; • Foundations of Incident Management; Introduction to Investigation of Digital Assets; ISACA Certified Information Security Manager (CISM) Prep; • 101 Reverse Engineering; • Advanced PCAP Analysis and Signature Development (APA); • Cyber Fundamentals for LE Investigators; Cybersecurity Overview for Managers; Offensive and Defensive Network Operations; (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP: ISSMP Prep 2018; • (ISC)2 (TM) Systems Security Certified Practitioner; • (ISC)2(TM) Systems Security Certified Practitioner; • Mobile Forensics;	
	RS.AN-4	Incidents are categorized consistent with response plans					• Foundations of Incident Management; Introduction to Investigation of Digital Assets; ISACA Certified Information Security Manager (CISM) Prep; • Cybersecurity Overview for Managers; CompTIA A+ 220-902 Certification Prep; • (ISC)2 (TM) CISSP: ISSMP Prep 2018; • (ISC)2(TM) Systems Security Certified Practitioner;	SANS: Data Breach Respons SANS: Pandemic Response Planning SANS: Security Response Plan
	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)				Nmap OpenVAS	• EC-Council Certified Ethical Hacker (CEHv9) Self-Study Prep; • CMaaS Overview; • CMaaS Technical Overview Course; • CMaaS Transition Classroom Sessions; Foundations of Incident Management; Introduction to Investigation of Digital Assets; ISACA Certified Information Security Manager (CISM) Prep; • Cyber Risk Management for Managers; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Cybersecurity Overview for Managers; • 101 - Critical Infrastructure Protection; • Supply Chain Assurance using Sonatype Nexus; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP: ISSMP Prep 2018;	
	RS.MI-1	Incidents are contained	Computer Emergency Response Team (CERT) Incident Response				• Foundations of Incident Management; Introduction to Investigation of Digital Assets; ISACA Certified Information Security Manager (CISM) Prep; • Cybersecurity Overview for Managers; Offensive and Defensive Network Operations; CompTIA A+ 220-902 Certification Prep; • Root Cause Analysis; • (ISC)2(TM) Systems Security Certified Practitioner; • Mobile Forensics;	

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
RESPOND	RS.MI-2	Incidents are mitigated	Computer Emergency Response Team (CERT) Incident Response				• Dynamic Testing using HPE WebInspect; Foundations of Incident Management; Introduction to Investigation of Digital Assets; Cybersecurity Overview for Managers; Offensive and Defensive Network Operations; CompTIA A+ 220-902 Certification Prep; • Root Cause Analysis; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) Systems Security Certified Practitioner; • (ISC)2(TM) Systems Security Certified Practitioner; • Mobile Forensics; • SiLK Traffic Analysis;	
	RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks		CIS Controls CIS-CAT Pro			• EC-Council Certified Ethical Hacker (CEHv9) Self-Study Prep; • CMaaS Overview; • CMaaS Technical Overview Course; • CMaaS Transition Classroom Sessions; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Cybersecurity Overview for Managers; • 101 - Critical Infrastructure Protection; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP: ISSMP Prep 2018;	
	RS.IM-1	Response plans incorporate lessons learned					• Foundations of Incident Management; Introduction to Investigation of Digital Assets; ISACA Certified Information Security Manager (CISM) Prep; • Cybersecurity Overview for Managers; CompTIA A+ 220-902 Certification Prep; • (ISC)2 (TM) CISSP (R) Certification Prep 2018;	SANS: Data Breach Response SANS: Pandemic Response Planning SANS: Security Response Plan
	RS.IM-2	Response strategies are updated					• Foundations of Incident Management; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Cybersecurity Overview for Managers; CompTIA Advanced Security Practitioner; (ISC)2 (TM) CISSP (R) Certification Prep 2018;	SANS: Data Breach Response SANS: Pandemic Response Planning SANS: Security Response Plan

Function	Category	Subcategory	MS-ISAC Service (No Cost)	CIS Service (No Cost)	CIS or MS-ISAC Service (Fee-Based)	Open Source	FedVTE	Policy Template
RECOVER	RC.RP-1	Recovery plan is executed during or after an event					• Foundations of Incident Management; • Cyber Risk Management for Managers; • ISACA Certified Information Security Manager (CISM) Prep; • Cybersecurity Overview for Managers; CompTIA Advanced Security Practitioner; (ISC)2 (TM) CISSP (R) Certification Prep 2018;	SANS: Disaster Recovery Plan
	RC.IM-1	Recovery plans incorporate lessons learned					• Foundations of Incident Management; • ISACA Certified Information Security Manager (CISM) Prep; • Cybersecurity Overview for Managers; CompTIA Advanced Security Practitioner; (ISC)2 (TM) CISSP (R) Certification Prep 2018;	SANS: Disaster Recovery Plan
	RC.IM-2	Recovery strategies are updated					• Foundations of Incident Management; • ISACA Certified Information Security Manager (CISM) Prep; • (ISC)2 (TM) CAP Certification Prep Self Study 2014; • Cybersecurity Overview for Managers; CompTIA Advanced Security Practitioner; (ISC)2 (TM) CISSP (R) Certification Prep 2018;	SANS: Disaster Recovery Plan
	RC.CO-1	Public relations are managed					• Cybersecurity Overview for Managers; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep;	SANS: Disaster Recovery Plan
	RC.CO-2	Reputation after an event is repaired					• Cybersecurity Overview for Managers; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep;	SANS: Disaster Recovery Plan
	RC.CO-3	Recovery activities are communicated to internal stakeholders and executive and management teams					• Foundations of Incident Management; • ISACA Certified Information Security Manager (CISM) Prep; • Cybersecurity Overview for Managers; • (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; (ISC)2(TM) Systems Security Certified Practitioner;	SANS: Disaster Recovery Plan