NIST Module

Category	Sub Category	Question	# Assessments	# NO	# YES
Detect	Anomalies and Events	Incident alert thresholds are established	196	54	142
Detect	Anomalies and Events	Impact of events is determined	196	33	163
Detect	Anomalies and Events	Detected events are analyzed to understand attack targets and methods	196	27	169
Detect	Anomalies and Events	Event data are aggregated and correlated from multiple sources and sensors	196	49	147
Detect	Anomalies and Events	A baseline of network operations and expected data flows for users and systems is established and managed	196	59	137
Detect	Detection Processes	Detection processes are continuously improved	196	38	158
Detect	Detection Processes	Detection activities comply with all applicable requirements	196	58	138
Detect	Detection Processes	Event detection information is communicated to appropriate parties	196	28	168
Detect	Detection Processes	Roles and responsibilities for detection are well defined to ensure accountability	196	61	135
Detect	Detection Processes	Detection processes are tested	196	70	126
Detect	Security Continuous Monitoring	Vulnerability scans are performed	196	33	163
Detect	Security Continuous Monitoring	Unauthorized mobile code is detected	196	57	139
Detect	Security Continuous Monitoring	External service provider activity is monitored to detect potential cybersecurity events	196	53	143
Detect	Security Continuous Monitoring	Personnel activity is monitored to detect potential cybersecurity events	196	43	153
Detect	Security Continuous Monitoring	Malicious code is detected	196	17	179
Detect	Security Continuous Monitoring	Monitoring for unauthorized personnel, connections, devices, and software is performed	196	46	150
Detect	Security Continuous Monitoring	The network is monitored to detect potential cybersecurity events	196	29	167
Detect	Security Continuous Monitoring	The physical environment is monitored to detect potential cybersecurity events	196	31	165
Identify	Asset Management	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	196	75	121
Identify	Asset Management	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	196	56	140
Identify	Asset Management	External information systems are catalogued	196	69	127
Identify	Asset Management	Organizational communication and data flows are mapped	196	66	130
Identify	Asset Management	Software platforms and applications within the organization are inventoried	196	34	162
Identify	Asset Management	Physical devices and systems within the organization are inventoried	196	15	181
Identify	Business Environment	The organization's role in the supply chain is identified and communicated	196	46	150
Identify	Business Environment	Resilience requirements to support delivery of critical services are established	196	38	158
Identify	Business Environment	The organization's place in critical infrastructure and its industry sector is identified and communicated	196	40	156
Identify	Business Environment	Dependencies and critical functions for delivery of critical services are established	196	29	167
Identify	Business Environment	Priorities for organizational mission, objectives, and activities are established and communicated	196	26	170
Identify	Governance	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	196	33	163
Identify	Governance	Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	196	52	144
Identify	Governance	Governance and risk management processes address cybersecurity risks	196	48	148
Identify	Governance	Organizational information security policy is established	196	41	155
Identify	Risk Assessment	Threat and vulnerability information is received from information sharing forums and sources	196	23	173
Identify	Risk Assessment	Risk responses are identified and prioritized	196	49	147
Identify	Risk Assessment	Threats, both internal and external, are identified and documented	196	46	150
Identify	Risk Assessment	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	196	46	150
Identify	Risk Assessment	Asset vulnerabilities are identified and documented	196	53	143

Identify	Risk Assessment	Potential business impacts and likelihoods are identified	196	40	156
Identify	Risk Management	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.	196	101	95
Identify	Risk Management	Response and recovery planning and testing are conducted with suppliers and third-party providers	196	120	76
Identify	Risk Management	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.	196	72	124
Identify	Risk Management	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	196	95	101
Identify	Risk Management	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	196	89	107
Identify	Risk Management Strategy	Risk management processes are established, managed, and agreed to by organizational stakeholders	196	81	115
Identify	Risk Management Strategy	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	196	79	117
Identify	Risk Management Strategy	Organizational risk tolerance is determined and clearly expressed	196	93	103
Protect	Access Control	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)	196	17	179
Protect	Access Control	Identities are proofed and bound to credentials and asserted in interactions	196	20	176
Protect	Access Control	Access permissions are managed, incorporating the principles of least privilege and separation of duties	196	13	183
Protect	Access Control	Physical access to assets is managed and protected	196	8	188
Protect	Access Control	Identities and credentials are managed for authorized devices and users	196	6	190
Protect	Access Control	Remote access is managed	196	8	188
Protect	Access Control	Network integrity is protected, incorporating network segregation where appropriate	196	16	180
Protect	Awareness and Training	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	196	35	161
Protect	Awareness and Training	Senior executives understand roles & responsibilities	196	27	169
Protect	Awareness and Training	All users are informed and trained	196	25	171
Protect	Awareness and Training	Physical and information security personnel understand roles & responsibilities	196	10	186
Protect	Awareness and Training	Privileged users understand roles & responsibilities	196	16	180
Protect	Data Security	Integrity checking mechanisms are used to verify hardware integrity	196	71	125
Protect	Data Security	Protections against data leaks are implemented	196	51	145
Protect	Data Security	Integrity checking mechanisms are used to verify software, firmware, and information integrity	196	61	135
Protect	Data Security	Adequate capacity to ensure availability is maintained	196	18	178
Protect	Data Security	Assets are formally managed throughout removal, transfers, and disposition	196	16	180
Protect	Data Security	Data-in-transit is protected	196	17	179
Protect	Data Security	Data-at-rest is protected	196	29	167
Protect	Data Security	The development and testing environment(s) are separate from the production environment	196	34	162
Protect	Information Protection Processes and Procedures	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	196	41	155
Protect	Information Protection Processes and Procedures	Data is destroyed according to policy	196	18	178

Protect	Information Protection Processes and Procedures	Effectiveness of protection technologies is shared with appropriate parties	196	28	168
Protect	Information Protection Processes and Procedures	Protection processes are continuously improved	196	26	170
Protect	Information Protection Processes and Procedures	Policy and regulations regarding the physical operating environment for organizational assets are met	196	20	176
Protect	Information Protection Processes and Procedures	A vulnerability management plan is developed and implemented	196	67	129
Protect	Information Protection Processes and Procedures	A System Development Life Cycle to manage systems is implemented	196	77	119
Protect	Information Protection Processes and Procedures	Response and recovery plans are tested	196	80	116
Protect	Information Protection Processes and Procedures	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	196	43	153
Protect	Information Protection Processes and Procedures	Configuration change control processes are in place	196	52	144
Protect	Information Protection Processes and Procedures	A baseline configuration of information technology/industrial control systems is created and maintained	196	63	133
Protect	Information Protection Processes and Procedures	Backups of information are conducted, maintained, and tested periodically	196	15	181
Protect	Maintenance	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	196	29	167
Protect	Maintenance	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	196	21	175
Protect	Protective Technology	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	196	58	138
Protect	Protective Technology	Removable media is protected and its use restricted according to policy	196	55	141
Protect	Protective Technology	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	196	21	175
Protect	Protective Technology	Access to systems and assets is controlled, incorporating the principle of least functionality	196	20	176
Protect	Protective Technology	Communications and control networks are protected	196	11	185
Recover	Improvements	Recovery strategies are updated	196	35	161
Recover	Improvements	Recovery plans incorporate lessons learned	196	30	166
Recover	Recovery Communications	Reputation after an event is repaired	196	19	177
Recover	Recovery Communications	Public relations are managed	196	17	179
Recover	Recovery Communications	Recovery activities are communicated to internal stakeholders and executive and management teams	196	21	175
Recover	Recovery Planning	Recovery plan is executed during or after an event	196	25	171
Respond	Analysis	Incidents are categorized consistent with response plans	196	48	148
Respond	Analysis	Forensics are performed	196	56	140
Respond	Analysis	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)	196	39	157
Respond	Analysis	The impact of the incident is understood	196	22	174
Respond	Analysis	Notifications from detection systems are investigated	196	20	176
Respond	Improvements	Response strategies are updated	196	42	154
Respond	Improvements	Response plans incorporate lessons learned	196	33	163

Respond	Mitigation	Newly identified vulnerabilities are mitigated or documented as accepted risks	196	34	162
Respond	Mitigation	Incidents are mitigated	196	17	179
Respond	Mitigation	Incidents are contained	196	16	180
Respond	Response Communications	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	196	42	154
Respond	Response Communications	Information is shared consistent with response plans	196	38	158
Respond	Response Communications	Events are reported consistent with established criteria	196	39	157
Respond	Response Communications	Coordination with stakeholders occurs consistent with response plans	196	34	162
Respond	Response Communications	Personnel know their roles and order of operations when a response is needed	196	41	155
Respond	Response Planning	Response plan is executed during or after an event	196	35	161

Ransomware Readiness Module

Category	Sub Category	Question	# NO	# YES
Application Integrity and Allowlist (AI)	Advanced	Has the organization documented a list of known approved software (an Allowlist) organized by software publisher and version number, and is that list used to allow only approved software to run on organizational systems?	117	79
Application Integrity and Allowlist (AI)	Basic	Is there a list of known bad software (a “Blocklist”), and is the software on that list being blocked?	66	130
Application Integrity and Allowlist (AI)	Intermediate	Has the organization documented a list of known approved software (an “Allowlist”)?	94	102
Application Integrity and Allowlist (AI)	Intermediate	Is the Allowlist organized by software publisher, and is that list used to allow only approved software to run on organizational systems?	117	79
Asset Management (AM)	Advanced	Does the organization quarantine and/or remove all rogue hardware?	57	139
Asset Management (AM)	Advanced	Does the organization manage system configurations using security hardening guides?	70	126
Asset Management (AM)	Basic	Have the organization’s hardware and software assets been inventoried and is the inventory managed?	32	164
Asset Management (AM)	Basic	Has the organization removed all unsupported hardware and software from its operating environment?	88	108
Asset Management (AM)	Basic	Are documented and approved secure configurations used to manage the organization’s hardware and software assets?	57	139
Asset Management (AM)	Intermediate	Does the organization detect rogue hardware and alert key stakeholders?	72	124
Asset Management (AM)	Intermediate	Are standard baseline images used to control hardware and software configurations?	40	156
Incident Response (IR)	Advanced	Are physical incident response exercises performed at least twice a year?	147	49
Incident Response (IR)	Advanced	Have redundant and resilient systems and data been implemented throughout the organization?	51	145
Incident Response (IR)	Basic	Has the organization developed an incident response plan?	58	138
Incident Response (IR)	Basic	Does the organization conduct annual incident response tabletop exercises that include ransomware response scenarios?	108	88
Incident Response (IR)	Intermediate	Are cybersecurity incidents reported and escalated to the appropriate stakeholders?	17	179
Incident Response (IR)	Intermediate	Have disaster recovery procedures been developed?	42	154
Incident Response (IR)	Intermediate	Are incident response tabletop exercises performed at least twice a year?	142	54
Incident Response (IR)	Intermediate	Is a physical incident response exercise performed at least once a year?	118	78
Incident Response (IR)	Intermediate	Has the organization implemented redundant systems where appropriate for the purpose of resiliency?	24	172
Network Perimeter Monitoring (NM)	Advanced	Has the organization established a baseline of network traffic and is it used to identify anomalous activity?	75	121
Network Perimeter Monitoring (NM)	Basic	Is perimeter network traffic monitored?	24	172
Network Perimeter Monitoring (NM)	Intermediate	Is internal network traffic monitored?	38	158
Network Perimeter Monitoring (NM)	Intermediate	Are networks segmented to protect mission critical assets?	36	160
Patch and Update Management (PM)	Advanced	Are all software and firewalls patched for vulnerabilities within 3 days for vulnerabilities rated as “Critical” and 7 days for vulnerabilities rated as “High”?	81	115
Patch and Update Management (PM)	Basic	Is all public-facing software patched for vulnerabilities within 15 days for vulnerabilities rated as “Critical” and 30 days for vulnerabilities rated as “High”?	45	151
Patch and Update Management (PM)	Basic	Are all internal-facing software and firewalls patched for vulnerabilities within 30 days for both vulnerabilities rated as “Critical” and for vulnerabilities rated as “High”?	48	148

Patch and Update Management (PM)	Intermediate	Are all software and firewalls patched for vulnerabilities within 15 days for vulnerabilities rated as “Critical” and 30 days for vulnerabilities rated as “High”?	50	146
Phishing Prevention and Awareness (PP)	Basic	Are annual tabletop exercises that include phishing response scenarios conducted?	79	117
Phishing Prevention and Awareness (PP)	Basic	Are users trained to recognize cyber threats like phishing?	15	181
Phishing Prevention and Awareness (PP)	Basic	Is email filtered to protect against malicious content?	7	189
Risk Management (RM)	Advanced	Has the organization defined organizational risk criteria and tolerances?	101	95
Risk Management (RM)	Advanced	Does the organization consider risk inheritance and exposure between its various interconnected systems?	68	128
Risk Management (RM)	Advanced	Does the organization apply quantitative risk analysis to remediation activities?	123	73
Risk Management (RM)	Intermediate	Does the organization perform business impact assessments?	100	96
Robust Data Backup (DB)	Basic	Are important systems and data backed up daily to an offsite location with the ability to restore multiple versions back at least 30 days?	25	171
Robust Data Backup (DB)	Basic	Are data backups tested annually?	47	149
User and Access Management (UM)	Advanced	Is two-factor authentication implemented for all users?	108	88
User and Access Management (UM)	Advanced	Is role-based security training conducted?	101	95
User and Access Management (UM)	Advanced	Are users who attempt to install rogue hardware counseled against installing rogue hardware?	35	161
User and Access Management (UM)	Basic	Are strong and unique passwords implemented throughout the entire organization?	28	168
User and Access Management (UM)	Basic	Is the principle of least privilege enforced through policies and procedures?	40	156
User and Access Management (UM)	Intermediate	Is two-factor authentication implemented for all privileged (e.g. system administrators) and remote users	73	123
User and Access Management (UM)	Intermediate	Is least privilege enforced through technical (technology based) restrictions?	42	154
User and Access Management (UM)	Intermediate	Are audit logs maintained for all privileged (e.g. system administrator) accounts?	47	149
User and Access Management (UM)	Intermediate	Is rogue hardware being detected?	73	123
Web Browser Management and DNS Filtering (BM)	Basic	Is malicious web content being blocked using DNS filtering via methods like DNS resolvers and DNS firewalls?	12	184
Web Browser Management and DNS Filtering (BM)	Basic	Are web browser security settings managed?	34	162