Annual Cybersecurity Self-Assessment

Internal Audit · Based on NIST CSF v1.1

Use this assessment to honestly evaluate your own organization's cybersecurity posture.

IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER

ORGANIZATION NAME

COMPLETED BY

TITLE / ROLE

EMAIL ADDRESS

PHONE NUMBER

DATE OF ASSESSMENT

Purpose

This is an internal audit to help your organization honestly evaluate its cybersecurity posture. Use it to understand where you stand, identify gaps, and track progress over time. This is not a vendor evaluation, it is a mirror you hold up to yourselves.

Frequency

Complete this once per year, or after any major change to your technology environment. Insurance renewals, compliance reviews, or building good habits are all valid triggers.

Why NIST?

SOC 2 and ISO 27001 are excellent but require significant investment. NIST CSF is a practical, widely respected framework appropriate for organizations of any size.

Response Options

Yes / No / I Don't Know / N/A. "I don't know" is useful, it tells you where to look. Use the Notes column to add context. For help: macktez.com

NIST CSF — IDENTIFY

INVENTORY AND WORKFLOW

QUESTION	YES	NO	IDK	N/A	NOTES
1 Does your organization have a complete inventory of hardware?	☐	☐	☐	☐	
2 Does your organization have a complete inventory of software licenses?	☐	☐	☐	☐	
3 Does your organization have a complete inventory of online (cloud) services?	☐	☐	☐	☐	
4 Does your organization have a complete staff list and org chart?	☐	☐	☐	☐	
5 Does your organization have a defined set of apps & tools for internal communication?	☐	☐	☐	☐	

Additional notes — Inventory and Workflow:

NEW HIRES AND NEW COMPUTERS

QUESTION	YES	NO	IDK	N/A	NOTES
6 Does your organization have an onboarding checklist for assigning hardware, software, and services?	☐	☐	☐	☐	
7 Does your organization employ a standard base configuration for user hardware?	☐	☐	☐	☐	
8 Are there special configurations defined for different departments (e.g., Finance)?	☐	☐	☐	☐	
9 Are there special configurations defined for individual users (e.g., CFO)?	☐	☐	☐	☐	

Additional notes — New Hires and New Computers:

ROLES AND RESPONSIBILITIES

QUESTION	YES	NO	IDK	N/A	NOTES
10 Does your organization have a staff member responsible for cybersecurity?	☐	☐	☐	☐	
11 Are their cybersecurity responsibilities clearly defined?	☐	☐	☐	☐	

	QUESTION	YES	NO	IDK	N/A	NOTES
12	Does any third party (suppliers, customers, partners) have cybersecurity responsibility at your company?	☐	☐	☐	☐	
13	Are third party cybersecurity responsibilities clearly defined?	☐	☐	☐	☐	
14	Are users allowed to act as admin on their computers?	☐	☐	☐	☐	
15	Are there protections in place to deny admin access to those not authorized?	☐	☐	☐	☐	

Additional notes — Roles and Responsibilities:

SUPPLY CHAIN

	QUESTION	YES	NO	IDK	N/A	NOTES
16	Do you have a complete list of suppliers and customers with contact information?	☐	☐	☐	☐	
17	Has the importance of each third party been assessed and communicated with them?	☐	☐	☐	☐	
18	Has the importance of your organization to suppliers/customers been assessed and communicated?	☐	☐	☐	☐	
19	Does your organization qualify as Critical Infrastructure (see CISA guidance)?	☐	☐	☐	☐	

Additional notes — Supply Chain:

RESILIENCE

	QUESTION	YES	NO	IDK	N/A	NOTES
20	Are your organization's critical activities identified and prioritized?	☐	☐	☐	☐	
21	Do you know what business systems directly impact those critical activities?	☐	☐	☐	☐	
22	Have you established the cost of failure to perform critical activities if systems fail?	☐	☐	☐	☐	
23	Can you operate in a degraded state (partial systems failure)?	☐	☐	☐	☐	
24	Do you know how long it would take to restore critical business activities after a failure?	☐	☐	☐	☐	

Additional notes — Resilience:

GOVERNANCE

	QUESTION	YES	NO	IDK	N/A	NOTES
25	Does your organization have any form of documented cybersecurity policy?	☐	☐	☐	☐	
26	Is the policy regularly reviewed and approved?	☐	☐	☐	☐	
27	Is the policy known to employees and contractors?	☐	☐	☐	☐	
28	Are you aware of the legal and regulatory requirements for cybersecurity at your organization?	☐	☐	☐	☐	
29	Are these regulations regularly reviewed?	☐	☐	☐	☐	
30	Are you aware of the legal ramifications for not being in compliance?	☐	☐	☐	☐	
31	Are these legal requirements regularly reviewed?	☐	☐	☐	☐	

Additional notes — Governance:

RISK ASSESSMENT

	QUESTION	YES	NO	IDK	N/A	NOTES
32	Has your company evaluated vulnerabilities (internal and external) to each type of asset?	☐	☐	☐	☐	
33	Are these vulnerabilities regularly reviewed and updated?	☐	☐	☐	☐	
34	Has your organization identified the likelihood of cybersecurity failures impacting operations?	☐	☐	☐	☐	
35	Are these likelihoods regularly reviewed and updated?	☐	☐	☐	☐	
36	Does your organization identify and prioritize the impacts of cybersecurity vulnerabilities?	☐	☐	☐	☐	
37	Are these impacts regularly reviewed and updated?	☐	☐	☐	☐	
38	Have threats, vulnerabilities, likelihoods, and impacts been used to determine overall risk?	☐	☐	☐	☐	

	QUESTION	YES	NO	IDK	N/A	NOTES
39	Is this risk assessment regularly reviewed and updated?	☐	☐	☐	☐	

Additional notes — Risk Assessment:

RISK MANAGEMENT STRATEGY

	QUESTION	YES	NO	IDK	N/A	NOTES
40	Has your organization defined risk tolerance and management strategy? (What risk is accepted, transferred, avoided, remediated?)	☐	☐	☐	☐	
41	Is this strategy regularly reviewed and updated?	☐	☐	☐	☐	
42	Is this strategy communicated to staff?	☐	☐	☐	☐	
43	Is this strategy communicated to suppliers and customers?	☐	☐	☐	☐	
44	Are procedures in place to support this strategy?	☐	☐	☐	☐	
45	Does your cybersecurity risk management strategy extend to supply chain risk?	☐	☐	☐	☐	
46	Do you know the status of critical suppliers' own risk assessment and risk management strategy?	☐	☐	☐	☐	
47	Do your contracts with vendors include terms that allow them to meet your cybersecurity standards?	☐	☐	☐	☐	
48	Do your contracts with customers add requirements to your risk management strategy?	☐	☐	☐	☐	
49	Are contracts regularly reviewed and updated along with updated risk assessments?	☐	☐	☐	☐	

Additional notes — Risk Management Strategy:

NIST CSF — PROTECT

IDENTITY MANAGEMENT, AUTHENTICATION, AND ACCESS CONTROL

QUESTION	YES	NO	IDK	N/A	NOTES
50 Does your organization have a process to assign identities and access credentials to employees?	☐	☐	☐	☐	
51 Is the credential assignment process manual?	☐	☐	☐	☐	
52 Is the process using single sign-on (SSO)?	☐	☐	☐	☐	
53 Is the process using identity and access management (IdAM)?	☐	☐	☐	☐	
54 Does anyone regularly review credentials?	☐	☐	☐	☐	
55 Does your organization have a process to manage physical access to assets?	☐	☐	☐	☐	
56 Is someone responsible for approving an employee's physical access?	☐	☐	☐	☐	
57 Is someone responsible for reclaiming assets during job changes?	☐	☐	☐	☐	
58 Does your organization have a process to manage remote access?	☐	☐	☐	☐	
59 Is someone responsible for approving an employee's remote access?	☐	☐	☐	☐	
60 Are employees trained on remote access security (authentication, encryption, VPN, social engineering)?	☐	☐	☐	☐	
61 Is remote access monitored for suspicious events?	☐	☐	☐	☐	
62 Can security appliances block or disable remote devices attempting unauthorized tasks?	☐	☐	☐	☐	
63 Does your organization have a process for managing access permissions?	☐	☐	☐	☐	
64 Are least privilege and separation of duties applied? (No unnecessary admin access; data only accessible to those who need it?)	☐	☐	☐	☐	
65 Do employees have physical access only to specific floors or offices?	☐	☐	☐	☐	

66	Is the person approving access permissions different from the person processing access control?	☐	☐	☐	☐
67	Does your organization have documentation of your network configuration?	☐	☐	☐	☐
68	Does documentation cover security zones or network segmentation?	☐	☐	☐	☐
69	Does documentation cover VLAN configuration?	☐	☐	☐	☐
70	Do guests have full access to the local network?	☐	☐	☐	☐
71	Do guests have partial (restricted) access to the local network?	☐	☐	☐	☐
72	Does your organization have a process to validate user identities?	☐	☐	☐	☐
73	Is multi-factor authentication (MFA) required for all critical systems?	☐	☐	☐	☐
74	Is user authentication managed by a central directory service?	☐	☐	☐	☐
75	Is access limited by device or IP address?	☐	☐	☐	☐

Additional notes — Identity Management, Authentication, and Access Control:

AWARENESS AND TRAINING

	QUESTION	YES	NO	IDK	N/A	NOTES
76	Is there a cybersecurity awareness training plan at your organization?	☐	☐	☐	☐	
77	Is this training planned, scheduled, and designed for different employee roles?	☐	☐	☐	☐	
78	Are roles and responsibilities for privileged users documented and communicated?	☐	☐	☐	☐	
79	Are roles and responsibilities for clients and vendors documented and communicated?	☐	☐	☐	☐	
80	Are roles and responsibilities for executives documented and communicated?	☐	☐	☐	☐	
81	Are roles and responsibilities for cybersecurity and physical security personnel documented?	☐	☐	☐	☐	

Additional notes — Awareness and Training:

DATA SECURITY

	QUESTION	YES	NO	IDK	N/A	NOTES
82	Is company data protected at rest (e.g., disk encryption)?	☐	☐	☐	☐	
83	Are there exceptions to at-rest protection?	☐	☐	☐	☐	
84	Is company data protected in transit (e.g., over file sharing)?	☐	☐	☐	☐	
85	Are endpoints verified with certificates?	☐	☐	☐	☐	
86	Are there exceptions to in-transit protection?	☐	☐	☐	☐	
87	Is wireless access to your network protected with encryption or authentication?	☐	☐	☐	☐	
88	Does your organization have policies for hardware transfer or disposal to protect data?	☐	☐	☐	☐	
89	Does your organization monitor for data leaks?	☐	☐	☐	☐	
90	Are system software security patches applied regularly?	☐	☐	☐	☐	
91	Is there a system in place to verify the level of software security?	☐	☐	☐	☐	
92	Are device firmware security patches applied regularly?	☐	☐	☐	☐	
93	Is there a system in place to verify the level of hardware security?	☐	☐	☐	☐	
94	Can users install software on their own workstations?	☐	☐	☐	☐	
95	Are they restricted to authorized app stores?	☐	☐	☐	☐	
96	Do workstations have a TPM (Trusted Platform Module) installed?	☐	☐	☐	☐	

Additional notes — Data Security:

INFORMATION PROTECTION PROCESSES AND PROCEDURES

QUESTION	YES	NO	IDK	N/A	NOTES
97 Does your organization have a baseline system configuration that incorporates security policies?	☐	☐	☐	☐	
98 Are principles of least functionality observed? (e.g., no SSH on a server that does not need it?)	☐	☐	☐	☐	
99 Does hardware have a defined lifecycle?	☐	☐	☐	☐	
100 Are there any end-of-life devices in use?	☐	☐	☐	☐	
101 Does your organization have a staff member responsible for making changes to devices?	☐	☐	☐	☐	
102 Are their change management responsibilities clearly defined?	☐	☐	☐	☐	
103 Are data backups maintained?	☐	☐	☐	☐	
104 Are backups monitored regularly?	☐	☐	☐	☐	
105 Are backups tested for viability (restorability)?	☐	☐	☐	☐	
106 Is data purposefully destroyed at end of life?	☐	☐	☐	☐	
107 Does your organization have a staff member responsible for authorizing data destruction?	☐	☐	☐	☐	
108 Is data destruction verified?	☐	☐	☐	☐	
109 Does your organization have a plan to respond to a cybersecurity incident and maintain continuity?	☐	☐	☐	☐	
110 Does your organization have a plan to recover from a cybersecurity incident or natural disaster?	☐	☐	☐	☐	
111 Does a staff member own responsibility for maintaining these plans?	☐	☐	☐	☐	
112 Are these plans regularly reviewed?	☐	☐	☐	☐	
113 Are these plans regularly tested?	☐	☐	☐	☐	

Additional notes — Information Protection Processes and Procedures:

MAINTENANCE

	QUESTION	YES	NO	IDK	N/A	NOTES
114	Does your organization have a process for maintaining and updating company assets?	☐	☐	☐	☐	
115	Does your organization have a process for the repair of company assets?	☐	☐	☐	☐	
116	Are repairs and maintenance approved and logged?	☐	☐	☐	☐	
117	Is remote access to a user's machine approved and logged?	☐	☐	☐	☐	
118	Is remote access restricted to only authorized users?	☐	☐	☐	☐	

Additional notes — Maintenance:

PROTECTIVE TECHNOLOGY

	QUESTION	YES	NO	IDK	N/A	NOTES
119	Is device logging enabled on security devices?	☐	☐	☐	☐	
120	Are logs maintained for more than 90 days?	☐	☐	☐	☐	
121	Are logs maintained for more than 180 days?	☐	☐	☐	☐	
122	Does anyone at your organization have permission to overwrite or delete logs?	☐	☐	☐	☐	
123	Has your organization implemented system redundancy for internet service?	☐	☐	☐	☐	
124	Has your organization implemented system redundancy for electrical power?	☐	☐	☐	☐	
125	Has your organization implemented system redundancy for firewalls?	☐	☐	☐	☐	
126	Has your organization implemented system redundancy for network switches?	☐	☐	☐	☐	
127	Has your organization implemented system redundancy for wireless access points?	☐	☐	☐	☐	
128	Has your organization implemented system redundancy for physical servers?	☐	☐	☐	☐	
129	Has your organization implemented system redundancy for cloud servers?	☐	☐	☐	☐	

	QUESTION	YES	NO	IDK	N/A	NOTES
130	Has your organization implemented system redundancy for virtual appliances?	☐	☐	☐	☐	
131	Has your organization implemented system redundancy for remote access tools?	☐	☐	☐	☐	
132	Has your organization implemented system redundancy for workstations?	☐	☐	☐	☐	

Additional notes — Protective Technology:

NIST CSF — DETECT

ANOMALIES AND EVENTS

	QUESTION	YES	NO	IDK	N/A	NOTES
133	Does your organization have a documented plan for responding to a security event?	☐	☐	☐	☐	
134	Can event data (e.g., logs) be collected?	☐	☐	☐	☐	
135	Can event data be collected from multiple sources?	☐	☐	☐	☐	
136	Are detected events analyzed to understand vulnerabilities?	☐	☐	☐	☐	
137	Are vulnerabilities documented and updated?	☐	☐	☐	☐	
138	Does your organization have a process to analyze events and assess their business impact?	☐	☐	☐	☐	
139	Have you determined and documented what activity should trigger a response?	☐	☐	☐	☐	

Additional notes — Anomalies and Events:

SECURITY CONTINUOUS MONITORING

	QUESTION	YES	NO	IDK	N/A	NOTES
140	Is your organization's local network monitored?	☐	☐	☐	☐	
141	Can unauthorized devices on the network be detected?	☐	☐	☐	☐	
142	Is network equipment installed in a locked cabinet or closet?	☐	☐	☐	☐	

	QUESTION	YES	NO	IDK	N/A	NOTES
143	Does your organization have a system in place for monitoring user machines?	☐	☐	☐	☐	
144	Does your organization maintain antivirus software on all computers?	☐	☐	☐	☐	
145	Are organization-owned mobile devices enrolled in Mobile Device Management (MDM)?	☐	☐	☐	☐	
146	Does this MDM solution monitor vulnerabilities in the OS?	☐	☐	☐	☐	
147	Are users permitted to install apps outside of MDM?	☐	☐	☐	☐	
148	Are all non-MDM installed apps documented?	☐	☐	☐	☐	
149	Does your organization monitor vendors for potential security concerns?	☐	☐	☐	☐	

Additional notes — Security Continuous Monitoring:

DETECTION PROCESSES

	QUESTION	YES	NO	IDK	N/A	NOTES
150	Does your organization have a staff member responsible for detecting network vulnerabilities?	☐	☐	☐	☐	
151	Are the processes for detecting and monitoring devices recorded?	☐	☐	☐	☐	
152	Are these processes being followed?	☐	☐	☐	☐	
153	Are your processes being tested to ensure they are effective?	☐	☐	☐	☐	
154	Are these processes regularly reviewed and updated?	☐	☐	☐	☐	
155	Does your organization have a staff member responsible for communication during a cybersecurity event?	☐	☐	☐	☐	
156	Has a communications plan been documented?	☐	☐	☐	☐	
157	Is this plan regularly reviewed and updated?	☐	☐	☐	☐	

Additional notes — Detection Processes:

NIST CSF — RESPOND

RESPONSE PLANNING

	QUESTION	YES	NO	IDK	N/A	NOTES
158	Does your organization have a response plan to address cybersecurity events?	☐	☐	☐	☐	
159	Does the plan include specific steps for typical events (rogue employees, exploits, data leaks, ransomware)?	☐	☐	☐	☐	
160	Does the response plan include explicit delegation of responsibilities?	☐	☐	☐	☐	
161	Are staff members aware of their responsibilities in case of a cybersecurity event?	☐	☐	☐	☐	
162	Does the plan outline what information can be shared and with whom (staff, vendors, clients)?	☐	☐	☐	☐	
163	Is the response plan regularly reviewed and updated?	☐	☐	☐	☐	

Additional notes — Response Planning:

ANALYSIS AND MITIGATION

	QUESTION	YES	NO	IDK	N/A	NOTES
164	Are security alerts recorded and investigated when detected?	☐	☐	☐	☐	
165	Does your organization have a staff member responsible for analysis of detected threats?	☐	☐	☐	☐	
166	Does your organization have a staff member responsible for determining technical response actions?	☐	☐	☐	☐	
167	Are your systems regularly audited for vulnerabilities?	☐	☐	☐	☐	
168	Are accepted risks discussed and documented?	☐	☐	☐	☐	

Additional notes — Analysis and Mitigation:

NIST CSF — RECOVER

RECOVERY

QUESTION	YES	NO	IDK	N/A	NOTES
169 Does your organization have a plan for recovery after a cybersecurity event?	☐	☐	☐	☐	
170 Does this plan include prioritized points of recovery within your data set and infrastructure?	☐	☐	☐	☐	
171 Does this plan define an expected recovery timeline?	☐	☐	☐	☐	
172 Is the recovery plan regularly reviewed and updated?	☐	☐	☐	☐	

Additional notes — Recovery:

COMMUNICATION

QUESTION	YES	NO	IDK	N/A	NOTES
173 Does your organization have a plan for communication after a cybersecurity event?	☐	☐	☐	☐	
174 Does this plan include methods of communicating with internal personnel?	☐	☐	☐	☐	
175 Does this plan include methods of communicating with vendors and clients?	☐	☐	☐	☐	

Additional notes — Communication:

Summary: Priority Actions by Section

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER