

Security Policy and Plan Review Checklist

33 items in 9 sections, mapped to the 6 NIST CSF 2.0 functions. Mark each item done, not done or not applicable, and give every item that is not done an owner and a date.

Organization	Policy set reviewed
Owner of the policy set	Reviewer
Date of this review	Date of the next review

How to use this checklist

- 1. Run it with 2 people: the owner of the policy set and a reviewer who did not write the policies.
- 2. Mark each item done, not done or not applicable, and give every item that is not done an owner and a date.
- 3. Run it at every scheduled review and after any major change, such as an acquisition, a new core system or a serious incident.
- 4. Keep each completed checklist with its date, because it is the evidence that the review happened.

How the sections map to NIST CSF 2.0

The NIST Cybersecurity Framework 2.0, published in February 2024, is organized around 6 functions: Govern, Identify, Protect, Detect, Respond and Recover. Each section below names the functions it serves, so a team that reports against CSF 2.0 can file the results under its own headings.

Section	NIST CSF 2.0 functions
1. Governance and ownership	Govern
2. Scope and currency	Govern, Identify
3. Access	Protect
4. Data	Identify, Protect
5. Incident response	Detect, Respond
6. Business continuity and recovery	Recover
7. Third parties	Govern, Identify
8. AI use	Govern
9. Evidence and review cycle	Govern, Identify

The checklist

1. Governance and ownership **Govern**

Item	Done	Not done	N/A	Owner and date
1 Every policy and plan names one accountable owner, by role and by name.	☐	☐	☐	
2 Senior leadership has approved the information security policy, and the approval is dated and recorded.	☐	☐	☐	
3 The roles that run security are written down, including who may accept a risk on the business's behalf.	☐	☐	☐	
4 An index lists every policy, standard and plan with its owner, version and next review date.	☐	☐	☐	

2. Scope and currency **Govern, Identify**

Item	Done	Not done	N/A	Owner and date
5 Each policy states the business units, locations, systems and data it covers, and that scope matches the business as it runs today.	☐	☐	☐	
6 Systems, cloud services and suppliers added since the last review are covered by the policies that apply to them.	☐	☐	☐	
7 Every reference to a standard or regulation names its current version, such as ISO/IEC 27001:2022 or NIST CSF 2.0.	☐	☐	☐	
8 The laws, regulations and contract terms that apply to the business are listed, and each one points to the policy that meets it.	☐	☐	☐	

3. Access **Protect**

Item	Done	Not done	N/A	Owner and date
9 The access policy requires multifactor authentication for remote access, email and every administrator account.	☐	☐	☐	
10 The policy lists the second factors that are allowed, and it treats one-time codes sent by SMS as a restricted authenticator, the status NIST SP 800-63B gives them.	☐	☐	☐	
11 Privileged access is granted only with a named approver, and privileged accounts are reviewed on a stated schedule.	☐	☐	☐	
12 Access is removed within a stated time when someone leaves or changes role, and recent leaver records show that it happened.	☐	☐	☐	

4. Data Identify, Protect

Item	Done	Not done	N/A	Owner and date
13 A data classification scheme exists, and each class says how that data is stored, shared and deleted.	☐	☐	☐	
14 The policy states where encryption is required at rest and in transit, and who holds and manages the keys.	☐	☐	☐	
15 Each class of data has a retention period, and deletion at the end of that period is recorded.	☐	☐	☐	

5. Incident response Detect, Respond

Item	Done	Not done	N/A	Owner and date
16 The incident response plan names the incident lead and a deputy, and says how to reach both outside working hours.	☐	☐	☐	
17 The plan defines severity levels and says who decides when an incident goes to senior leadership.	☐	☐	☐	
18 The plan lists every notification duty the business has, with its recipient and its deadline. For a US public company, the list includes disclosure of a material cybersecurity incident on SEC Form 8-K Item 1.05 within 4 business days of the materiality determination.	☐	☐	☐	
19 The logs the plan relies on are named, switched on and kept long enough to investigate an incident.	☐	☐	☐	
20 The plan has been exercised in the last 12 months, and what the exercise taught has been written into the plan.	☐	☐	☐	

6. Business continuity and recovery Recover

Item	Done	Not done	N/A	Owner and date
21 Each important service has a recovery time objective and a recovery point objective, set from a business impact analysis.	☐	☐	☐	
22 The continuity plan lists the people, systems, sites and suppliers that each important service depends on.	☐	☐	☐	
23 Backups are defined for each important system, including how often they run and where the copies are kept.	☐	☐	☐	
24 A restore or failover test has shown that each important service can be recovered within its recovery time objective, and the result is dated.	☐	☐	☐	

7. Third parties **Govern, Identify**

Item	Done	Not done	N/A	Owner and date
25 A register lists every supplier that holds company data or connects to company systems, with an owner for each.	☐	☐	☐	
26 Suppliers are tiered by the data they hold and the access they have, and each tier has a review frequency.	☐	☐	☐	
27 Contracts with high-tier suppliers cover security requirements, breach notification, audit rights and the return of data at exit.	☐	☐	☐	
28 The date of each high-tier supplier's latest security evidence is recorded, and evidence more than 12 months old has been requested again.	☐	☐	☐	

8. AI use **Govern**

Item	Done	Not done	N/A	Owner and date
29 An acceptable use policy for AI tools says which tools staff may use and which data may never be entered into them.	☐	☐	☐	
30 An inventory lists the AI tools and AI features in use, including AI built into existing software, with an owner for each.	☐	☐	☐	
31 The AI policy names the framework it follows, such as the NIST AI Risk Management Framework 1.0 or ISO/IEC 42001:2023, and records whether the EU AI Act, Regulation (EU) 2024/1689, applies to the business.	☐	☐	☐	

9. Evidence and review cycle **Govern, Identify**

Item	Done	Not done	N/A	Owner and date
32 Each policy has at least one piece of evidence that it is followed, such as an access review record or a restore test report, and staff acknowledgements of the current version are kept.	☐	☐	☐	
33 Exceptions to any policy are recorded with an owner, a reason and an expiry date, and expired exceptions have been closed or renewed.	☐	☐	☐	

What to do with the results

Every item marked not done becomes a task with an owner and a date. Carry the open tasks into the next review, so each completed checklist also shows what changed since the last one.

DigitalXForce published this checklist in October 2026, for Cybersecurity Awareness Month. The web version, with answers to common questions about policy reviews, is at digitalxforce.com/security-policy-review-checklist/. DigitalXForce, 230 W John Carpenter Fwy, Suite 100, Irving, TX 75039, USA.