NISTnow

NIST CSF 2.0

Cybersecurity Assessment Report

Prepared for The Internet Store

Assessment	2026 Cybersecurity Assessment
Scope	NISTquick, 44 controls
Coverage	Everything the business runs.
Submitted	October 22, 2026 by the CFO
Overall score	3.59 / 5

This self-guided assessment shows where you stand today and what to improve over the next 6 months to 2 years. It is built on the NIST Cybersecurity Framework 2.0, a voluntary framework. It is not a certification, an audit, or a determination of compliance.

Executive summary

This report is for a 50 to 249 person retail and ecommerce business on Microsoft 365 with a mix of in-house and outside IT. In the past year, a customer and an insurance company asked to see how the business handles security, so the roadmap favors steps it can show.

All 44 questions were answered. Overall maturity is Established (3.59 out of 5), and the next level is Advanced.

Recover and Govern score highest, at 4.00 and 3.80 out of 5. Respond and Identify have the most room to grow, at 3.25 and 3.50 out of 5.

Do these first

1. **List the providers that can reach your systems, subscribe to their security notices, and check each notice against that access.**
   Now 1 · DE.CM-06 · Detect
2. **Adopt a short written access policy that gives each person only the access their role needs, and limit administrator rights to a few named people.**
   Now 2 · PR.AA-05 · Protect
3. **List every software program and online subscription the business uses, and retire the ones nobody needs.**
   Now 3 · ID.AM-02 · Identify
4. **List every login to your business systems with a named owner, and disable any that belong to former staff or to nobody.**
   Now 4 · PR.AA-01 · Protect
5. **Prepare a short incident response plan naming a lead, a deputy, and the outside help to call, then practice it.**
   Now 5 · RS.MA-01 · Respond

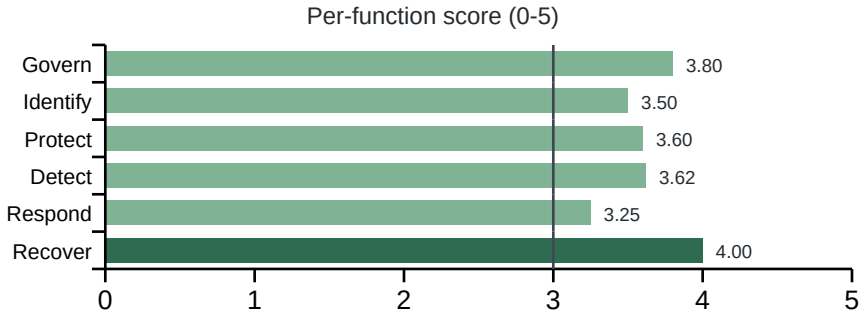
No step in this plan is a quick win: each one takes some planning.

If these five steps reach the next level, the projected score is 3.70. A retake confirms it.

The roadmap lists two more steps to take after these. Working steadily through the plan is what prepares the business for a formal assessment later.

The business's stated priority is keeping customer data safe. The answers show no gap there, so the roadmap does not need to turn to it.

All nine subjects that insurers commonly ask about are in place; see the insurance readiness page.



Context that shaped this report:

The business carries cyber insurance. Insurers commonly ask about multi-factor authentication (a second check at sign-in beyond the password), tested backups, and endpoint protection at renewal, and the insurance readiness page sets each subject beside the ratings in this assessment. The policy, and a question to the insurance broker, establish what the insurer expects. The business could run for only hours without its systems. The policy is worth rereading with that in mind, and the broker can say what it would pay for in a multi-day outage, business interruption included.

The business had a near miss in the last two years: a control, or a member of staff, caught it before it became an incident. A short record of what happened and what stopped it is training material drawn from the business's own experience, which no course provides, and it costs nothing to keep.

The business holds the administrator access to its email and accounts, and a second person can reach it. That arrangement is worth protecting with a yearly check that the second person can still sign in and that the recovery codes are held somewhere other than the account they unlock.

Card details reach the business through a payment page or payment link the payment provider hosts, so they never enter the business's own systems. That keeps the exposure on the payment path small, and it is worth protecting. If a member of staff begins taking card numbers by phone, by email, or on paper, the exposure changes and this part of the report needs rereading.

Your action plan

A one-page checklist of the Now items. Print it, put it where the staff working on these items can see it, and mark each item off as it is completed.

	Item	What to do
☐	Now 1	List the providers that can reach your systems, subscribe to their security notices, and check each notice against that access.
☐	Now 2	Adopt a short written access policy that gives each person only the access their role needs, and limit administrator rights to a few named people.
☐	Now 3	List every software program and online subscription the business uses, and retire the ones nobody needs.
☐	Now 4	List every login to your business systems with a named owner, and disable any that belong to former staff or to nobody.
☐	Now 5	Prepare a short incident response plan naming a lead, a deputy, and the outside help to call, then practice it.

When these are done, retake your assessment to see your new score.

Insurance readiness

Wording varies by insurer, but cyber-insurance questionnaires keep returning to the same subjects. Each subject below is matched to the ratings recorded in this assessment, so you can answer from evidence rather than from memory.

This page sets the answers you have already given beside the subjects insurers most often ask about. It does not determine whether an insurer will offer cover, at what price, or on what terms, and it is not an application. Read the questionnaire as written and put anything uncertain to your insurance broker.

What the insurer asks	Controls	Where you stand
Is multi-factor authentication required on email, on cloud sign-in, and on any remote access into your network?	PR.AA-03: Advanced PR.AA-01: Established PR.IR-01: Advanced	**In place**
Do backups run automatically, is at least one copy held where an intruder cannot delete it, and has a restore been tested?	PR.DS-11: Advanced RC.RP-03: Advanced	**In place**
Do your computers run endpoint detection software, and does a named person read the alerts it raises?	DE.CM-09: Advanced DE.CM-03: Advanced	**In place**
Is your email filtered for phishing and for malicious links or attachments?	PR.DS-02: Advanced DE.CM-09: Advanced	**In place**
Do staff receive security awareness training, and does it cover phishing?	PR.AT-01: Advanced	**In place**
Is there a written incident response plan, and is one person named as its owner?	ID.IM-04: Advanced RS.MA-01: Established	**In place**
How quickly is software updated, and is anything reachable from the internet kept current?	PR.PS-02: Advanced ID.RA-01: Advanced	**In place**
Are administrator accounts limited to the people who need them, and separated from everyday logins?	PR.AA-05: Established PR.AA-01: Established	**In place**
Are logs kept from your systems, and would a person notice something unusual in them?	PR.PS-04: Established DE.AE-03: Established	**In place**

Practices to keep

Not every finding in this report is a gap. For the controls below, your answers show a practice that is working. A practice like this weakens unnoticed once the checking stops, so each one is listed with what it takes to maintain it.

Govern: GV.PO-01

Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced

Rated Advanced.

To keep this level: That written policy still fits your business, is still seen by all staff, and is still applied consistently. On top of that, you review it on a schedule and check whether staff follow it, using evidence such as sign-offs.

Govern: GV.RR-02

Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced

Rated Advanced.

To keep this level: Each task still has a named owner in writing, and the assignments still hold in practice. On top of that, you review the assignments on a schedule and check whether the tasks happen.

Identify: ID.AM-01

Inventories of hardware managed by the organization are maintained

Rated Advanced.

To keep this level: That written inventory still covers all your hardware, stays owned, and is kept current. On top of that, you review it on a schedule and check it against the devices in use.

Your roadmap

The roadmap is grouped into what to do now and what to do next. Each tier assumes the one before it is under way, and each item is stated as a move on one control from your current level to the next.

Now: do these first

These are your first five priorities. They rank highest for a business of your size, weighing how much risk each gap carries against how far your answers sit from the next level. The six baseline safeguards come first wherever one is rated below Established, and any other practice rated below Established comes next. The Now tier always holds an item from the weakest function and no more than three from any one function. Treat them as the priorities for the coming quarter.

Now 1 Detect DE.CM-06 2 to 3



External service provider activities and services are monitored to find potentially adverse events

List the providers that can reach your systems, subscribe to their security notices, and check each notice against that access.

A provider's breach or mistake becomes your incident, because outside providers such as IT support, cloud services, and software vendors often hold real access to your systems and data. With no watch on that access, the first you hear of their trouble is a customer telling you about it.

Aim for: Provider trouble that reaches you from the provider, not from a customer: their access known, their notices read, and their incidents checked against your own exposure.

1. **1.** List your key providers, what each does for you, and what access each one holds, marking any with administrator rights to your systems.
2. **2.** Subscribe to the status page and security notices of each one, so an outage or a breach on their side reaches you from them rather than from a customer.
3. **3.** Treat every provider security notice as potentially yours: check what it touched in your systems, and write the answer down, even when the answer is nothing.

From your answers: A rough sense of provider access tends to understate it, because access granted for one project is rarely removed afterward. Ask the provider for a written list of every account they hold in your systems, what each one can do, and which of their staff use it, then keep that list. Asking is routine, and the list itself often prompts the removal of accounts nobody still needs.

Your note: Our monitoring provider covers Microsoft 365 and the laptops. Nobody watches what apps, the agency or platform support do in the storefront admin.

Tools to consider:

You told us you already pay for a service that watches for threats and raises alerts, so the step is the agreement with them rather than a new tool. Agree in writing what they will call you about, at what hour, and what you are expected to do when they call.

Now 2 Protect PR.AA-05 3 to 4



Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties

Adopt a short written access policy that gives each person only the access their role needs, and limit administrator rights to a few named people.

When everyone can reach everything, a single mistake or one stolen account can expose or destroy the whole business, because the compromised login inherits all that access. Least privilege, giving each person only the access their job needs, and separation of duties, so no one person controls a sensitive process end to end, shrink what any one account, or any one attacker, can touch.

Aim for: Access rights are reviewed on a schedule, and excess permissions and stale administrator accounts are removed, with evidence kept.

Your note: The quarterly access review covers Microsoft 365, the ERP and finance, but not the storefront admin, where several staff hold full permissions.

1. Set a review date in the calendar, name who runs the review, and file the dated result with the record below.

Record to keep: The record of your last access review, with the permissions and admin rights it removed.

Microsoft 365: In Microsoft 365, review who holds privileged roles such as Global Administrator in Entra ID, and pare them back to a small number of named admins, each with their own account. Have admins use a separate standard account for daily work, and where your plan supports it consider Privileged Identity Management to grant admin rights only when needed.

Your IT provider: Ask your IT provider for a list of who can access what, including their own admin accounts into your systems, and agree that all staff and the provider alike get only what their role needs. Ask how they separate their admin access from everyday use and how they remove access when your staff change roles.

Now 3 **Identify** **ID.AM-02** **3 to 4** 

Inventories of software, services, and systems managed by the organization are maintained

List every software program and online subscription the business uses, and retire the ones nobody needs.

Forgotten or unapproved software is a common way attackers get in: an unpatched application, a free tool anyone installed, or a cloud service holding company data that no one is watching.

Aim for: The software and subscription list is reviewed on a schedule and checked against what is installed and subscribed to.

Your note: IT keeps the inventory current for what it buys. Storefront apps get added when we notice them, so it trails what marketing installs.

1. Set a review date in the calendar, name who runs the review, and file the dated result with the record below.

Record to keep: Your software and subscription list, with the date it was last checked against statements and sign-ins.

Specialist software: List the industry or custom software you depend on with extra care: note the vendor, who maintains it, what data it holds, and anything old it forces you to keep, such as a specific operating system or browser version. That software is often the hardest to update and the simplest to overlook, and its dependencies are risks in their own right.

Microsoft 365: In the Microsoft 365 admin center, and under Enterprise Applications in Entra ID, you can see which applications and services are connected to your tenant and what data they can reach. Review that list, revoke anything unneeded, then add software bought outside Microsoft 365, such as a standalone accounting tool or a design application, that will not appear there.

From your answers: Knowing some of the connections means the rest hold access to your mail and documents with nobody accountable for them. Open the connected applications page in your platform: Enterprise applications in the Microsoft Entra admin center, or connected apps in the Google Workspace admin console. Read the list, and write each connection down with who uses it and why. Then require administrator approval before a new application is granted access, so that the list you have built stays short.

Now 4 **Protect** **PR.AA-01** **3 to 4**

Identities and credentials for authorized users, services, and hardware are managed by the organization

List every login to your business systems with a named owner, and disable any that belong to former staff or to nobody.

Orphaned accounts, logins left active after a member of staff leaves or changes role, are one of the most common ways an attacker gets a foothold, because a live credential no one is watching draws no attention. Every account and credential should be created deliberately, tracked in one place, and removed the moment it is no longer needed.

Aim for: You review accounts on a schedule and find and remove unused or leftover logins, with evidence kept.

Your note: Staff accounts come from the HR system and are reviewed each quarter in Entra ID. Storefront and marketplace logins are outside that review.

1. Set a review date in the calendar, name who runs the review, and file the dated result with the record below.

Record to keep: Your account inventory, with the date it was last reconciled against your staff roster.

Microsoft 365: In the Microsoft 365 admin center, review Active users in one place, and block sign-in then delete accounts for anyone who has left. In Entra ID you can see last sign-in activity to spot dormant accounts, and reconcile the user list against your current staff roster.

Your IT provider: Ask your IT provider for a current export of all accounts, including service and admin logins, and confirm every one maps to a current staff member or a known service. Make disabling access on the departure day a defined step in your leaver process with them, and ask for evidence it was carried out.

From your answers: Knowing your non-human logins, such as the scanner that emails files, the backup tool, and the accounting integration, is what keeps them from sitting outside every check you run on staff accounts. Keep a named owner and a password-change date against each one, and remove any whose purpose nobody can name. These credentials rarely change and nobody thinks to review them, so a short owned list is the only check watching them.

Now 5 **Respond** **RS.MA-01** **3 to 4**

The incident response plan is executed in coordination with relevant third parties once an incident is declared

Prepare a short incident response plan naming a lead, a deputy, and the outside help to call, then practice it.

A response plan that sits in a drawer while everyone improvises does not help you, and improvising under pressure is how obvious steps get missed and time is lost.

Aim for: The incident response plan is walked through in practice runs, outside contacts included, and notes from each run are kept.

Your note: Our plan is written and was practised in the spring ransomware exercise. The platform, payment provider and agency have never been part of a practice run.

1. Set a review date in the calendar, name who runs the review, and file the dated result with the record below.

Record to keep: Your written response plan, with dated notes from its most recent walk-through.

Your IT provider: Agree with your IT provider in advance exactly what they do when you declare an incident: which actions they take, how fast they respond, their out-of-hours contact route, and who on your side is authorized to call them. Put that agreement and their emergency number in the plan so response does not wait on figuring out who to phone.

Your monitoring service: You told us a service watches for threats and raises alerts, which changes where your plan begins. For most incidents you will find out because they call, not because a member of staff notices, so the first line of the plan is who takes that call. Name the person, the number they will be reached on out of hours, and the deputy. They detect and advise; deciding to stop trading for the morning or to notify a customer stays with you, and the plan is where that split is written down.

From your answers: Practicing the plan is what turns it from a document into something people can run under pressure. Insurers and consultants call this a tabletop exercise, and an hour around a table with the people named in your plan is the whole of it. Keep practicing: walk through a likely incident, fix whatever confused people, then repeat it yearly and after any major change. Keep short dated notes from each run, because a note saying you ran it carries more weight with an insurer or a customer than the document alone.

Next

Start these once the Now items are under way. Several build on that work, so starting them first usually takes more effort for less return.

Next 1 **Protect** **PR.PS-04** **3 to 4** 

Log records are generated and made available for continuous monitoring

Turn on logging of sign-ins and system changes in your cloud services and servers, and aim to keep the records for at least ninety days.

When something goes wrong, logs are how you find out what genuinely happened, who signed in, what changed, and when, and without them an incident leaves no trail, so you cannot check up on it or contain it. Logs only help if they still exist and can be found weeks later, since many incidents surface long after they began.

Aim for: Log coverage and retention are checked on a schedule, and logs are sampled to confirm each one is usable.

Your note: Microsoft 365, Entra ID and laptop logs go to our monitoring provider for a year. Storefront and ERP audit logs stay in each platform and expire within days.

1. Set a review date in the calendar, name who runs the review, and file the dated result with the record below.

Record to keep: A retrieved sample, such as last week's sign-in records pulled from one key system, with the retention setting noted.

Next 2 **Review and evidence** **Practices in place, put on a review calendar** Covers eleven areas

Each practice below is in place but lacks a set review date and a dated record an insurer or assessor could ask to see. Practices drift once nobody checks them. For each, the step is a review date, a named reviewer and the dated result on file; the table shows what the review adds.

Control	What to add
Next 2.1 PR.DS-10 **Protect** Set every device to lock after a short idle time, keep real customer data out of test systems, and limit who can export records in bulk.	Protections for data in use are reviewed on a schedule, and violations, like real customer data in a test system, are caught.
Next 2.2 PR.IR-03 **Protect** List the servers, connections, applications, and people the business cannot operate without, and write and test a fallback for each.	Fallbacks for critical systems are tested on a schedule, for example by simulating the outage of a key system.
Next 2.3 ID.AM-03 **Identify** Draw a diagram of how your systems connect to each other and to the internet, and mark every route in from outside.	The network and data-flow diagram is reviewed on a schedule and checked against the real network.
Next 2.4 ID.AM-04 **Identify** List each supplier the business relies on, what service it provides, and what company data it can reach.	The list of supplier services is reviewed on a schedule and checked against invoices and contracts.
Next 2.5 RS.CO-03 **Respond** Name one person to send incident updates to staff, key customers, your IT provider, and your insurer.	Sharing incident updates with staff, customers, and partners is practiced in walk-throughs, and copies of what was sent are kept with the incident notes.
Next 2.6 RS.MA-04 **Respond** Write down when a problem goes to a senior person or outside help, and who to call, including after hours.	Escalation routes are practiced in walk-throughs, and each real escalation is recorded with its time and reason.
Next 2.7 GV.SC-03 **Govern** Rank supplier risks on the same list, by the same method, as your internal ones.	The treatment of supplier risks is reviewed on a schedule with the rest of the risk process, with evidence kept.
Next 2.8 ID.RA-07 **Identify** Keep a written log of changes to your systems and exceptions to your security rules, and give each exception an end date.	Change and exception records are reviewed on a schedule, and expired exceptions are closed.
Next 2.9 ID.RA-08 **Identify** Publish a way for outsiders to report a security flaw in your website or product, and name who answers each report.	Handling of reported security flaws is exercised on a schedule, and each report is tracked from receipt to resolution.

Control	What to add
Next 2.10 PR.PS-06 **Protect** If your business builds software, have a second person review code before release, update third-party components, and keep passwords out of the code.	Security checks run in the development pipeline, and adherence to the secure coding practices is reviewed on a schedule.
Next 2.11 DE.AE-03 **Detect** Name who compares alerts, sign-in records, and staff reports before judging whether something suspicious is real.	Clues from the business's alert and log sources are compared in one review on a schedule, with notes kept of each comparison.

What you can safely skip for now

Knowing what not to buy yet matters as much as knowing what to do. At your current stage, the items below are usually money and attention spent too early. Each one earns its cost at a later stage, and your answers do not place the business there yet.

A threat intelligence feed

A threat intelligence feed is a paid subscription that lists the attacks currently circulating. A paid feed still delivers more than a small team can act on. The advisories your software suppliers and your platform publish cover most of what you need.

Policy volume for its own sake

Depth serves you better than volume. Strengthen the policies you put into practice rather than adding documents for completeness.

What to get quotes for now

Alongside what you can safely skip, a few paid services have started to earn their price at your stage. None is urgent, and none replaces the roadmap. Each is worth a quote and a conversation this year, rather than a purchase this month.

A scoped penetration test

A penetration test is an authorized attempt by a specialist to break into your systems. You are past the point at which a test mostly reports what this assessment already shows, so a tester can spend the engagement on depth rather than on first steps. Limit the scope to whatever would hurt most to lose, and ask for a retest of the fixes to be included in the price.

A periodic check-in with an outside advisor

A few hours twice a year, spent on what has changed in the business and how that shifts your priorities, suit a business of your size better than a standing retainer. An arrangement of that kind can also be ended without a negotiation.

Device setup and updates belong in the agreement

Setting computers up and keeping them updated is outside what you told us your provider covers, so if it is not held in-house it falls to whoever has time. Late updates are a quiet way in for attackers using flaws that are already public, and a machine handed to a member of staff without being set up properly starts with the wrong settings. Ask at your next renewal what it would take for the provider to own the setup and the update schedule for every machine, including the ones that rarely come into the office. The evidence to ask for afterward is a device list showing the update status of each machine, refreshed monthly.

Your next formal assessment

You are ready to take real value from a formal assessment. At this level an assessor spends the engagement on depth and verification rather than on first steps, which is the work worth paying for. This report gives that assessor a documented starting position.

What to bring to the assessment

This report, so that the assessor starts from what you already know.

Your asset list: the systems, devices, and data the business runs on.

Notes from any incident or near miss, including any recorded informally.

The working documents you produced by following the roadmap, such as written policies, backup test results, and access reviews.

Questions to ask an outside firm

What exactly does the engagement cover, and what evidence will you want from the business?

Have you worked with businesses of this size, and what did those clients do with your report afterward?

What happens after the report: do you assist with the fixes, or deliver the report and step away?

What a reasonable first assessment looks like

A formal assessment can be run in two ways. A member of staff can run it, if the business has a person with the time, the independence, and the security background to answer honestly about work that person may own. More often, a business of your size brings in an outside firm or an independent consultant, which provides that independence and a second opinion. Either way, a reasonable first assessment is limited in scope and length: a gap assessment against a framework you name, a written report you own, and a working session in which the assessor walks you and your leadership through it. Be cautious of open-ended retainers as a first step, and of reports that arrive without a conversation.

Appendix

This appendix holds reference material and the notes and exceptions recorded against individual controls. Nothing in it changes the roadmap above. It is included so that the report is complete and any detail can be looked up when needed.

Records to keep

These are the records worth keeping as you close the gaps in the roadmap. An advisor, an auditor or an insurer may ask to see any of them, and having them ready turns that request into a single exchange. Keep a copy where you can find it, and record where it is kept and the date you last checked it, so that the next assessment goes faster than this one.

Roadmap item	Record	Where it is kept	Date last checked
Now 1	Your provider list showing what access each holds, with the date it was last reviewed.		
Now 2	The record of your last access review, with the permissions and admin rights it removed.		
Now 3	Your software and subscription list, with the date it was last checked against statements and sign-ins.		
Now 4	Your account inventory, with the date it was last reconciled against your staff roster.		
Now 5	Your written response plan, with dated notes from its most recent walk-through.		
Next 1	A retrieved sample, such as last week's sign-in records pulled from one key system, with the retention setting noted.		

When you bring in outside help, hand these records over first. They show the work behind your answers and let the assessor start from what you hold rather than from nothing.

For whoever releases payments

This page is for whoever releases the money. The cyber loss that appears in the accounts rather than in the systems rarely arrives as a technical breach. It arrives as an ordinary email about a supplier's new bank details, and it is paid because no step in the payment process was built to question it. Nothing on this page needs budget, technical access, or a change to your systems. Each item is a rule you can put in writing this week. A written rule does not depend on a member of staff noticing a forged request under time pressure.

A written approval threshold

You told us a second member of staff approves payments above a set amount. What remains is keeping that threshold from being bypassed when a payment is urgent. State in the rule that the second approval still applies when the request comes from the owner, and name a deputy, so an absence never becomes a reason to skip it.

A callback rule for bank-detail changes

You told us staff call a known number to check any change to a supplier's bank details. Write that rule down if it is currently an unwritten habit. State in it that the number comes from your own records rather than from the request, so a new member of staff under time pressure applies it the same way you would.

A payment run reviewed by a member of staff other than the preparer

A payment run prepared and released by the same person carries nothing that would surface an added supplier or an altered account number. Errors of that kind usually appear on a bank statement weeks later. Have a member of staff other than the preparer review the run before it is released: ten minutes, once a cycle, checked against your supplier list rather than against the invoices. Checking the run against the supplier list is what identifies a supplier you never had, because a forged invoice agrees with itself and so proves nothing.

What to do if a fraudulent payment gets through

If a payment goes to a fraudster, call your bank the moment you know. A recall is most likely to work in the first hours, and the chance falls away sharply after that. Then report the payment at ic3.gov, the FBI's reporting site for cyber-enabled crime, which can help the bank act.

Notes and exceptions

These are the controls where the business recorded a note, answered a follow-up question, or gave a reason for a not applicable rating. A note or answer that already prints on a roadmap card is not repeated in this table.

Control	Rating	Note
PR.AA-03	Advanced	Conditional Access enforces MFA for all staff; admins and finance use hardware keys.
PR.DS-11	Advanced	Restores are tested every quarter, and the backup copies cannot be altered.
DE.AE-03	Established	The monitoring provider correlates laptops, Microsoft 365 and the firewalls. The storefront and ERP are not connected to it.

Control	Rating	Note
RS.CO-03	Established	The spring exercise covered internal updates only, never the wholesale customer, the marketplace or the payment provider.
RS.MA-04	Established	Escalation to the CFO, counsel and the insurer is written down. Escalating to the platform or payment provider has never been practised.

Every control and its rating

Every control in this assessment appears below with its rating, in framework order. The assessment on the web gives the full text of each control.

Control	Rating	Control	Rating	Control	Rating
GV: Govern					
GV.OC-03	Advanced	**GV.PO-01**	Advanced	**GV.RM-01**	Advanced
GV.RR-02	Advanced	**GV.SC-03**	Established		
ID: Identify					
ID.AM-01	Advanced	**ID.AM-02**	Established	**ID.AM-03**	Established
ID.AM-04	Established	**ID.AM-05**	Advanced	**ID.IM-04**	Advanced
ID.RA-01	Advanced	**ID.RA-06**	Advanced	**ID.RA-07**	Established
ID.RA-08	Established				
PR: Protect					
PR.AA-01	Established	**PR.AA-03**	Advanced	**PR.AA-05**	Established
PR.AT-01	Advanced	**PR.DS-01**	Advanced	**PR.DS-02**	Advanced
PR.DS-10	Established	**PR.DS-11**	Advanced	**PR.IR-01**	Advanced
PR.IR-03	Established	**PR.IR-04**	Advanced	**PR.PS-01**	Advanced
PR.PS-02	Advanced	**PR.PS-04**	Established	**PR.PS-06**	Established
DE: Detect					
DE.AE-02	Advanced	**DE.AE-03**	Established	**DE.AE-06**	Advanced
DE.AE-08	Advanced	**DE.CM-01**	Advanced	**DE.CM-03**	Advanced

Control	Rating	Control	Rating	Control	Rating
DE.CM-06	Developing	**DE.CM-09**	Advanced		
RS: Respond					
RS.CO-02	Advanced	**RS.CO-03**	Established	**RS.MA-01**	Established
RS.MA-04	Established				
RC: Recover					
RC.RP-01	Advanced	**RC.RP-03**	Advanced		

Scale definitions

Level	Value	Description
Not Applicable	N/A	This practice genuinely doesn't apply to how your business runs, so it won't count for or against your score. Use this sparingly. If you're unsure, it usually applies in some form.
None	0	You don't do this yet. There's no process and no one owns it. That's completely normal when you're starting out; it just marks a place to begin. Sounds like: "We've never really looked at this."
Informal	1	It happens, but in an ad-hoc way that lives in someone's head rather than on paper. It works until that person is busy or leaves. Sounds like: "Our office manager usually handles that."
Developing	2	You've started making this repeatable. Some of it is written down and most people follow it, but there are gaps and it isn't applied everywhere yet. Sounds like: "We have a rough checklist and most of the team uses it."
Established	3	This is written down, clearly owned, and done the same way every time across the business. This is the healthy baseline most small companies should aim for first. Sounds like: "We have a policy, everyone knows it, and we follow it."
Advanced	4	You don't just do this. You also check that it's actually working, review it on a schedule, and catch issues early. It's managed with evidence, not just good intentions. Sounds like: "We review this every quarter and can prove it works."
Leading	5	This is a genuine strength you keep improving, using data and how leaders in your industry operate. Few small companies need every area at this level. Sounds like: "We measure it, benchmark it, and keep raising the bar."

Methodology

This assessment is a Test of Design: it rates how the business's practices are designed and documented, not whether they were tested in operation. Each in-scope NIST CSF 2.0 subcategory is rated on the scale defined above. A function score and the overall score are the average of the ratings that were answered and are not N/A (not applicable), with every subcategory weighted equally. Items marked N/A or left unanswered are left out, and a group with nothing to score is reported as N/A.

In this report, a control is one NIST CSF 2.0 subcategory: a single practice or outcome the framework lists.

The roadmap puts a baseline safeguard first whenever it is rated below Established. The six are multi-factor authentication (a second check at sign-in beyond the password), backups, administrator access, software updates, account management and staff awareness. Any other practice rated below Established comes next, ahead of every practice already Established. Within each group, every item is ordered by its importance to a business like this one, then by how far it sits below the next level. No practice rated Advanced is on the roadmap, because the step to Leading takes the staff and spending of a much larger organization. The Now tier then takes at most three items from any one function, and always at least one from the weakest function with a gap. An item that gives up its Now place moves down into Next.

Where several smaller gaps share a subject, such as suppliers or risk decisions, the roadmap lists them together under one finding. Each one keeps its own row and rating.

The insurance readiness page rates each subject at the level of the weakest control mapped to it, because a question asked as a single yes or no can only be answered honestly at that level. The mapping of subjects to controls is this report's own judgment, not a NIST statement.

Your answers about the business adjusted the priority order of the roadmap. Without those answers, the order would rest on importance and on your scores alone.

Generated from your answers at the time of download. Assessment ID: 01SAMPLEASSESS. Template version: 01SAMPLETMPL.