NISTnow

NIST CSF 2.0

Cybersecurity Assessment Report

Prepared for The Internet Store

Assessment	2026 Cybersecurity Assessment
Scope	Full NIST CSF 2.0, 106 controls
Coverage	Everything the business runs.
Submitted	October 22, 2026 by the CFO
Overall score	3.43 / 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 106 questions were answered. Overall maturity is Established (3.43 out of 5), and the next level is Advanced.

All six functions sit at about the same level, Established, so no single area stands out as stronger or weaker than the rest.

Do these first

1. **List the types of sensitive data the business holds, such as customer records, and where each type is stored.**
   Now 1 · ID.AM-07 · Identify
2. **Give extra security training to the staff who pay invoices or hold administrator rights, matched to the risks of their role.**
   Now 2 · PR.AT-02 · Protect
3. **Name who approves public statements about an incident, choose the channels in advance, and draft template wording to adapt.**
   Now 3 · RC.CO-04 · Recover · Quick win
4. **Risk judgments written down.**
   Now 4 · Risk decisions · covers two areas
5. **Suppliers checked, watched, and offboarded.**
   Now 5 · Suppliers and third parties · covers four areas

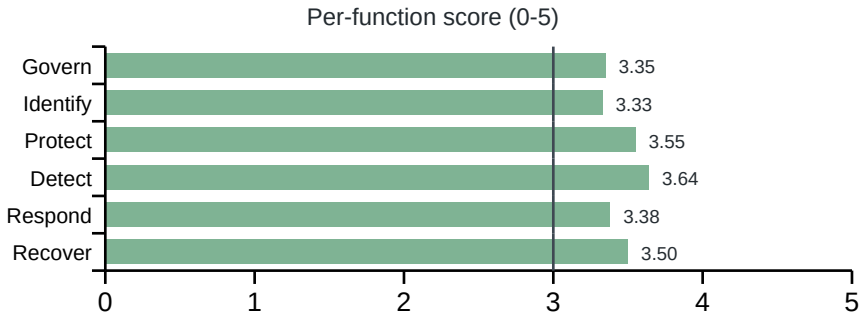
Quick wins (low effort, each closes a gap): Now 3 RC.CO-04, Now 4.1 GV.RM-07, Next 1 RS.AN-07, Next 7 RS.MA-02

If these five steps reach the next level, the projected score is 3.52. A retake confirms it.

The roadmap lists eight 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. Step 1 serves it directly.

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 and the quick wins. 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 types of sensitive data the business holds, such as customer records, and where each type is stored.
☐	Now 2	Give extra security training to the staff who pay invoices or hold administrator rights, matched to the risks of their role.
☐	Now 3	Name who approves public statements about an incident, choose the channels in advance, and draft template wording to adapt. **Quick win**
	Now 4	**Risk judgments written down**
☐	Now 4.1	GV.RM-07 List the business opportunities good security could support, such as winning larger customers, and name one person to assess which to pursue. **Quick win**
☐	Now 4.2	GV.RM-02 Write a short statement of which risks you will fix promptly, which you will insure against, and which you will accept for now.
	Now 5	**Suppliers checked, watched, and offboarded**
☐	Now 5.1	GV.SC-10 Create an exit checklist for important suppliers: get your data back or confirm it is deleted, and remove their access.
☐	Now 5.2	GV.SC-06 Before signing, ask each new supplier with access to your data or systems how it protects them, and keep the answers on file.
☐	Now 5.3	ID.RA-10 Ask each critical supplier a short list of security questions before you sign, and keep their answers on file.
☐	Now 5.4	DE.CM-06 List the providers that can reach your systems, subscribe to their security notices, and check each notice against that access.
☐	Next 1	Preserve the emails, logs, and machines an incident touched before anything is cleaned up. **Quick win**
☐	Next 7	Appoint one person to receive reports of a possible security problem, decide whether each is real, and record the outcome. **Quick win**

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 PR.PS-05: 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.OC-01

The organizational mission is understood and informs cybersecurity risk management

Rated Advanced.

To keep this level: That written statement still links your mission to your top priorities and stays owned and current. On top of that, you revisit it on a schedule and can point to choices it drove, such as where protection money goes.

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-01

Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving

Rated Advanced.

To keep this level: A named leader still owns cybersecurity risk and still backs it with decisions and budget. On top of that, leadership reviews security on a schedule, and its commitment shows in recorded decisions and follow-through.

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.

Quick wins

These are the low-effort steps in Now and Next, most important first. Each one closes a real gap, so it is worth doing early.

- **Now 3, RC.CO-04**: Name who approves public statements about an incident, choose the channels in advance, and draft template wording to adapt. **Quick**
- **Now 4.1, GV.RM-07**: List the business opportunities good security could support, such as winning larger customers, and name one person to assess which to pursue. **Quick**
- **Next 1, RS.AN-07**: Preserve the emails, logs, and machines an incident touched before anything is cleaned up. **Quick**

- **Next 7, RS.MA-02**: Appoint one person to receive reports of a possible security problem, decide whether each is real, and record the outcome. **Quick**

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. Items tagged "Serves the stated priority" are the ones that do the most to protect the priority you named.

Now 1 **Identify** **ID.AM-07** **2 to 3**  **Serves the stated priority**

Inventories of data and corresponding metadata for designated data types are maintained

List the types of sensitive data the business holds, such as customer records, and where each type is stored.

You cannot protect data or meet privacy obligations if you do not know what you hold and where it lives, and sensitive data has a habit of scattering into email, spreadsheets, and cloud applications unnoticed. This data map underpins nearly everything else: access control, backups, breach response, and privacy duties.

Aim for: For any sensitive record the business holds, a ready answer to where it lives and who can reach it, including the copies that drifted into inboxes and shared drives.

1. List the important data types the business holds, such as customer records, employee data, and financial information, and note for each where it lives, who can reach it, and roughly how sensitive it is.

2. Ask staff where they keep customer and financial information in practice, and include the copies in email, shared drives, and on laptops, not just the main system.

3. Cut access back where it is not justified, starting with the most sensitive types, so each store is reachable only by people who need it.

4. Update the map each time you adopt a new tool or service, and reread it yearly to catch what has drifted.

Hosted checkout: You told us card payments go through a checkout page your payment provider hosts, so card details go straight to the provider. Record that on the map: name the provider as the place card data is held, and note that the business keeps none of it. Then look for card numbers that arrive by accident, such as in a customer's email, a phone order, or a note on an order. Delete any copy you find, and agree with staff to send the customer a payment link instead.

From your answers: A rough sense held in memory is hard to act on when you need to lock a system down quickly or answer where a breach reached. Write down where your customer, employee, and financial data sits, including cloud applications, shared drives, email, and staff laptops. Note who can reach each place. It is a modest effort, and it turns vague awareness into a record you can use in a real incident and to tighten access.

Your note: Customer data lives in the platform and the ERP, and copies sit in the email marketing tool, the help desk, analytics and exported campaign spreadsheets.

Now 2 **Protect** **PR.AT-02** **2 to 3**

Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind

Give extra security training to the staff who pay invoices or hold administrator rights, matched to the risks of their role.

People in sensitive roles make higher-stakes decisions, so general awareness is not enough for them, and a single mistake by whoever administers your systems or approves payments can affect the whole business. A mistake there is also the one an attacker is trying hardest to cause.

Aim for: Specialist knowledge in the seats attackers single out: whoever pays invoices able to name the current scams, whoever holds admin rights able to read a security alert and act on it.

1. Name the roles that carry extra security responsibility, whoever manages IT and admin accounts, handles payroll or payments, or holds access to customer data, and match each one's training to the risks that role faces in practice.

2. Train payment handlers on invoice-fraud and payment-change scams, and on verifying a request through a second channel before money moves.

3. Train system administrators on secure configuration, patching, managing access, and reading security alerts, and refresh both when duties, tools, or threats change.

From your answers: If you have not singled out your higher-risk roles, the staff making the highest-stakes decisions may be getting only general awareness. A single mistake by whoever runs your systems or approves payments can affect everyone. List the roles with extra security responsibility, such as IT and admin, payments and payroll, and access to customer data, and give each training matched to its risks. That targets your effort where a mistake would cost the most.

Your note: Finance was coached on invoice fraud after the 2025 near miss. Developers, customer service agents handling account recovery and storefront admins get no traini [...] The full note is in the assessment on the web.

Tools to consider:

Microsoft Defender attack simulation training (works with your Microsoft 365): Runs simulated phishing campaigns and assigns follow-up lessons to staff who click, managed from the Microsoft Defender portal. It comes with certain Microsoft 365 security plans and fits a business already on Microsoft that wants to test and train users in one place.

KnowBe4: Delivers security awareness lessons and simulated phishing campaigns, with a library of content and reporting on who has completed each course. It suits a business that wants a broad set of material to run regular training and phishing tests.

Proofpoint ZenGuide: Provides security awareness lessons and phishing simulations and can tailor training to the threats a team actually sees; formerly sold as Proofpoint Security Awareness. It suits a business that wants training tied to the risks its staff encounter.

Hoxhunt: Runs continuous, personalized phishing simulations and short lessons that adapt to how each person responds. It suits a business that wants training to adjust to individual staff rather than a fixed annual course.

These tools are examples, not endorsements. Check that a tool still suits your business before you buy it.

Now 3 **Recover** **RC.CO-04** **2 to 3** **Quick**

Public updates on incident recovery are shared using approved methods and messaging

Name who approves public statements about an incident, choose the channels in advance, and draft template wording to adapt.

In an incident, an off-the-cuff public statement, or several contradicting each other, causes confusion and can create claims you later regret or cannot stand behind. Anything published during a bad week is quoted back at you for years, usually by whoever is least sympathetic.

Aim for: A public account of an incident the business can still stand behind a year later: measured, factual, and spoken in one voice through channels chosen in calm.

1. Decide in advance who approves anything said publicly, and which channels you would use, such as your website, email to customers, or your social accounts.

2. Draft template wording now that you can adapt quickly under pressure: acknowledge the situation, say what you are doing and what customers should do.

3. Keep the message factual and measured, avoid speculating on cause or scope before it is confirmed, and route every public update through the named approver so one voice speaks for the business.

From your answers: With nothing prepared, a public update gets composed under pressure, which is when tone and accuracy slip. Draft a short, factual template you can adapt quickly: acknowledge the situation, and say what you are doing and what customers should do. Avoid guessing at cause or scope before it is confirmed. Ready wording, routed through one approver, keeps public messaging calm and consistent.

Your note: We assume the CEO would speak for us, but nothing is approved or drafted.

Now 4 **Risk decisions** **Risk judgments written down** Covers two areas

Your leadership already decides which risks to accept and which to fix, but those decisions live in people's heads. A written record of what the business will accept, fix or insure against makes the next decision faster and defensible. Each control below puts one part of how the business spots, weighs and decides on risk in writing.

Control	Rating	Next step	Your note
Now 4.1 GV.RM-07 **Govern**	Informal	List the business opportunities good security could support, such as winning larger customers, and name one person to assess which to pursue.	
Now 4.2 GV.RM-02 **Govern**	Developing	Write a short statement of which risks you will fix promptly, which you will insure against, and which you will accept for now.	Leadership knows what it would never risk, such as checkout going down in November, but nothing written says how much risk we accept.

Now 5 **Suppliers and third parties** **Suppliers checked, watched, and offboarded** Covers four areas

Outside firms and apps reach your systems and data, and the checks on them are uneven or, for some, missing. The controls below ask for a check before signing, a watch during the contract and a clean exit at the end. Start with the suppliers that hold customer data or admin access.

Control	Rating	Next step	Your note
Now 5.1 GV.SC-10 **Govern**	Informal	Create an exit checklist for important suppliers: get your data back or confirm it is deleted, and remove their access.	We found our former marketing agency's login still active in the storefront admin nine months after the contract ended.
Now 5.2 GV.SC-06 **Govern**	Developing	Before signing, ask each new supplier with access to your data or systems how it protects them, and keep the answers on file.	Big suppliers get our security questionnaire. Marketing installs storefront apps and marketing tools without one.
Now 5.3 ID.RA-10 **Identify**	Developing	Ask each critical supplier a short list of security questions before you sign, and keep their answers on file.	We checked the payment and monitoring providers before signing. The storefront apps that can read customer orders were chosen on features and price.
Now 5.4 DE.CM-06 **Detect**	Developing	List the providers that can reach your systems, subscribe to their security notices, and check each notice against that access.	Our monitoring provider covers Microsoft 365 and the laptops. Nobody watches what apps, the agency or platform support do in the storefront admin.

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 **Respond** **RS.AN-07** **2 to 3** **Quick**

Incident data and metadata are collected, and their integrity and provenance are preserved

Preserve the emails, logs, and machines an incident touched before anything is cleaned up.

The instinct in an incident is to clean up fast, but wiping a machine or deleting a suspicious email destroys the evidence you need to understand what happened and to support an insurance claim. Cleaning up is also the one action that feels like progress, which is why it happens first.

Aim for: The instinct to preserve before cleaning up: when something happens, the emails, logs, and affected machines are treated as evidence first and clutter second.

1. Preserve the evidence before anything gets wiped or reused: copies of suspicious emails with their full headers, the relevant log files, and where practical the affected device left powered but isolated rather than reimaged.

2. Note against each item where it came from, who collected it, and the date, which is the chain-of-custody note an insurer or an advisor will ask for.

3. Store the copies somewhere they cannot be altered, so what you kept still counts when it is questioned later.

Next 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.

Next 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.

Next 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.

Next 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.

Next 6 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 7 **Respond** **RS.MA-02** **3 to 4** **Quick**

Incident reports are triaged and validated

Appoint one person to receive reports of a possible security problem, decide whether each is real, and record the outcome.

Without triage, every report is treated the same: real incidents get lost among false alarms, and the business either panics over nothing or misses something serious. The cost of that lands on the person who reported it, who learns that raising something is not worth the trouble.

Aim for: Triage of reported concerns is practiced in walk-throughs, and past reports are reviewed on a schedule to see whether real incidents were caught quickly.

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 log of incoming problem reports, each marked genuine or false alarm and given a severity.

Next 8 **Review and evidence** **Practices in place, put on a review calendar** Covers 32 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 8.1 GV.OC-02 **Govern** List the customers, partners, insurers, and regulators who expect something of your security, with one line on what each expects.	The list of stakeholders and their security expectations is reviewed on a schedule and checked against real feedback from those stakeholders.
Next 8.2 RS.MI-02 **Respond** Remove the cause of an incident and close the way in before restoring anything.	Removing an incident's cause is practiced in walk-throughs, and each real incident keeps evidence that the cause was verified gone.
Next 8.3 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 8.4 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 8.5 GV.PO-02 **Govern** Give the security rules a named owner and a yearly review date, and re-share each new version with staff.	Policy reviews happen on a schedule, changes are logged, and staff acknowledgment of each update is recorded.

Control	What to add
Next 8.6 GV.RM-05 **Govern** Give staff one known, blame-free route to raise anything that looks wrong.	The staff reporting route is reviewed or tested on a schedule, and reports are logged and followed up with evidence.
Next 8.7 GV.RR-03 **Govern** Set a yearly security budget, set aside work hours for the people who own security tasks, and reserve money for outside help.	The security budget and protected time are reviewed on a schedule against the plan, and adjustments are recorded with reasons.
Next 8.8 GV.SC-04 **Govern** List every supplier, including cloud subscriptions, and mark the few the business could not operate without.	The supplier list is reviewed on a schedule, and which suppliers are marked critical is re-checked.
Next 8.9 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 8.10 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 8.11 ID.RA-04 **Identify** Rate each risk by how likely it is and how much harm it would cause, using a simple scale of high, medium, or low.	Risk ratings are reviewed on a schedule and adjusted using real incidents and near misses.
Next 8.12 PR.IR-02 **Protect** Protect servers and key equipment from power surges, outages, water, and overheating, using surge protectors and a battery backup.	Protections for key equipment against power, water, and heat are inspected on a schedule and tested, for example confirming the battery backup works.
Next 8.13 PR.PS-03 **Protect** Replace aging equipment before it fails, and wipe every device before it leaves.	Hardware age and support status are reviewed on a schedule, and disposals are recorded as wiped.
Next 8.14 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 8.15 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.

Control	What to add
Next 8.16 RC.RP-06 **Recover** Write the criteria for ending recovery, and have the recovery lead close each incident with a note of follow-up actions and owners.	Declaring recovery complete and writing the closure note are practiced in recovery runs, and closure notes exist for every real incident.
Next 8.17 GV.SC-01 **Govern** Write a few sentences on which suppliers you check for security, what you expect of them, and who owns that work.	The written approach to supplier risk is reviewed on a schedule, with evidence checked that each step happens in practice.
Next 8.18 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 8.19 GV.SC-05 **Govern** Add security clauses, such as breach notification and data deletion, to agreements with suppliers that hold your data or connect to your systems.	You review the contract security terms on a schedule and check existing agreements for gaps.
Next 8.20 GV.SC-08 **Govern** Add your key suppliers and their emergency contacts to your incident plan, and keep those contacts reachable when your systems are down.	Supplier roles in the incident plan are tested, such as a walkthrough with your IT provider, and contacts are verified on a schedule.
Next 8.21 GV.SC-09 **Govern** Cover supplier security in the risk reviews you already run, from choosing a supplier to ending the relationship.	Supplier security monitoring runs on a schedule with recorded results, covering the full life cycle including exit and disposal.
Next 8.22 ID.IM-02 **Identify** Fix each weakness a security test or practice exercise finds, and check afterward that the fix worked.	Security tests and exercises run on a schedule, include key suppliers where relevant, and fixes are verified afterward.
Next 8.23 ID.IM-03 **Identify** Give staff a way to report security problems and near misses, and name one person to fix the cause of each.	Security process problems logged by staff are reviewed on a schedule, and completed fixes are checked for effect.
Next 8.24 ID.RA-02 **Identify** Subscribe to security alerts from your main software vendors or a national cybersecurity agency, and have one person read them weekly.	Threat warnings are reviewed on a schedule, and the actions taken in response are recorded.
Next 8.25 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.

Control	What to add
Next 8.26 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.
Next 8.27 ID.RA-09 **Identify** Buy hardware and software only from the official vendor or a reputable reseller, and download software only from the vendor's own site.	Hardware and software purchases are checked on a schedule against the rule to buy from verified vendors, with records of the checks kept.
Next 8.28 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 8.29 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.
Next 8.30 DE.CM-02 **Detect** Lock the doors to offices, network cabinets, and rooms holding sensitive paperwork, and have staff question any unfamiliar visitor.	Alarm tests, camera checks, and visitor-record reviews run on a schedule, with evidence kept that each one happened.
Next 8.31 RS.AN-06 **Respond** Have a named person log each incident action, decision, and time, then store the log where no one can edit it.	Keeping the incident log is practiced in walk-throughs, and past logs are checked on a schedule for completeness and safe storage.
Next 8.32 RC.RP-04 **Recover** After an incident, list the temporary workarounds to remove and the precautions to keep, and give each an owner and date.	Post-incident decisions on what returns to normal are reviewed later to confirm workarounds ended and agreed changes happened, with the reviews kept.

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 data map, listing each sensitive data type, where it lives, and who can reach it.		
Now 2	The training record for each sensitive role, showing what the person in it took and when.		
Now 3	The pre-drafted public statement template, with the name of who approves anything published.		
Now 4.2	The short written note of which risks the business will fix, insure against, or live with, kept where decision-makers can find it.		

Roadmap item	Record	Where it is kept	Date last checked
Now 5.1	Your supplier exit checklist, with the worked copy from the last relationship that ended.		
Now 5.2	The kept answers from each new critical supplier's security questions.		
Now 5.3	The kept assessment results for each critical supplier, dated before the contract was signed.		
Now 5.4	Your provider list showing what access each holds, with the date it was last reviewed.		
Next 1	Your evidence-preservation checklist, with the labeled items saved from its last use.		
Next 2	The record of your last access review, with the permissions and admin rights it removed.		
Next 3	Your software and subscription list, with the date it was last checked against statements and sign-ins.		
Next 4	Your account inventory, with the date it was last reconciled against your staff roster.		
Next 5	Your written response plan, with dated notes from its most recent walk-through.		
Next 6	A retrieved sample, such as last week's sign-in records pulled from one key system, with the retention setting noted.		
Next 7	Your log of incoming problem reports, each marked genuine or false alarm and given a severity.		

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
GV.PO-02	Established	The 2026 policy review is two months overdue.
GV.RM-02	Developing	An informal sense sits in one person's memory and moves with their mood, so the same risk receives a different answer depending on the week and who is asked. Put a rough number on the loss the business could take without borrowing or cutting staff, and write it where the staff making security and spending decisions will see it. An approximate figure all staff share is worth more than a precise one nobody has been told.
GV.SC-04	Established	Finance keeps the supplier list. The storefront apps are billed through the platform, so they are not on it. Owning the registrations means the business can change provider, recover an account, or respond to a takeover without needing another party's cooperation. Keep the registrant details, the billing owner, and the recovery address pointed at a business mailbox that more than one person can open, rather than at a personal account. Check them yearly, since a recovery address belonging to a departed employee undoes that ownership quietly.
GV.SC-10	Informal	Assuming you could get your data back is where most exits go wrong, because export options are often limited, chargeable, or produce a format nothing else opens. Pick your most important supplier and run the export now, while there is time to discover the limits. What the export produces tells you how tied the business is, and that is useful long before you plan to leave.
ID.AM-02	Established	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.

Control	Rating	Note
ID.AM-07	Developing	Data kept out of habit rather than need quietly grows your exposure, because every extra record is one more record that can be leaked and one more privacy obligation. Decide roughly how long you need each type of personal data, and start clearing out what is past that point, including copies in email, old spreadsheets, and archived systems. Holding less sensitive data is one of the simplest ways to reduce both your risk and the scope of a breach. Knowing and limiting who can reach your sensitive data is the control that contains a breach, so keep access matched to what each person genuinely needs. Review it when staff change roles or leave, because access tends to accumulate, and remove anything no longer justified. Tight, well-understood access both lowers the chance of misuse and shrinks how much a single compromised account can expose. A log that records every export is only a control while a member of staff reads it. An unread activity log tells you what left only after you already know to ask. Narrow export or download rights in your main system to the roles that genuinely need them, then set a date each month to read what the log shows. Cutting the number of staff who can copy records out is what makes the log short enough to be read at all.
ID.IM-02	Established	Our monitoring provider runs a ransomware exercise with leadership each spring. The platform and payment provider have never taken part.
ID.RA-04	Established	Risks described only vaguely are quick for decision-makers to discount, so cyber risk ranks below business risks that carry a number. For your main risks, put a rough figure on the harm, lost revenue, days of downtime, cost of recovery, customers lost. Stated that way, they can sit alongside financial and operational risks on the same basis. Even rough numbers make the case for action far stronger than technical language leaders cannot easily weigh.
ID.RA-10	Developing	Asking informally means the question gets skipped exactly when the deal is moving fast, which is usually the supplier that ends up holding the most. Write down five questions and ask them every time. The questions are: who can reach your data, is your data encrypted, do their staff use multi-factor authentication, how quickly would they report a breach, and where is it stored. Five questions on one page is enough at your size.

Control	Rating	Note
PR.AA-01	Established	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.
PR.AA-03	Advanced	Conditional Access enforces MFA for all staff; admins and finance use hardware keys.
PR.AT-02	Developing	Payment staff who can recognize invoice fraud and payment-change scams, and who verify requests through a second channel, are your main defense against a costly and common attack. Keep reinforcing the habit of confirming any new or changed payment details by calling a known number, never a number from the request itself. Refresh the examples as the scams evolve, since attackers adapt their wording and timing to reach staff at their busiest.
PR.DS-11	Advanced	Restores are tested every quarter, and the backup copies cannot be altered.
PR.PS-03	Established	The warehouse handheld scanners are past the vendor's support date.
DE.AE-03	Established	The monitoring provider correlates laptops, Microsoft 365 and the firewalls. The storefront and ERP are not connected to it.
DE.CM-06	Developing	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.
RS.AN-07	Developing	Storefront and ERP logs expire within days, and we have no evidence checklist of our own. Preserving before cleaning up is what keeps the answers available, since reimaging a machine destroys the record of how the incident started. Keep the habit specific: disconnect the device from the network but leave it powered, and save the suspicious email in full rather than as a screenshot. Label each item with where it came from and the date. Labeling is the part people skip and the part that matters later.

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-01	Established	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.
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.
RS.MI-02	Established	Our plan covers removing the cause for laptop and email incidents. It has no steps for a compromised storefront app or an injected script. Resetting beyond the single account is right, because a compromised mailbox usually exposes passwords saved in that browser, shared logins, and any service that resets through that address. Keep a short list of what to reset in that case: the account itself, anything sharing its password, saved browser passwords, and every service whose reset link arrives in that mailbox. The list is what makes the sweep repeatable rather than remembered. Watching for a period afterwards is what catches the attacker who kept a second way in, since a return is normally quiet and comes weeks rather than days later. Make the arrangement explicit: name who watches, for how long, and what they look at, such as sign-in alerts, mail rules that were not there before, and unfamiliar administrator changes. Close the incident only when that period passes clean.
RC.RP-06	Established	Confirming that the emergency measures were removed is what stops an incident leaving the business weaker than it found it. Keep the list explicit at closure: the sharing that was opened, the rights that were raised, the account created to get work moving again. Naming them as they are made, rather than recalling them at the end, is what keeps the removal check short.

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-01	Advanced	**GV.OC-02**	Established	**GV.OC-03**	Advanced
GV.OC-04	Advanced	**GV.OC-05**	Advanced	**GV.OV-01**	Advanced
GV.OV-02	Advanced	**GV.OV-03**	Advanced	**GV.PO-01**	Advanced
GV.PO-02	Established	**GV.RM-01**	Advanced	**GV.RM-02**	Developing
GV.RM-03	Advanced	**GV.RM-04**	Advanced	**GV.RM-05**	Established
GV.RM-06	Advanced	**GV.RM-07**	Informal	**GV.RR-01**	Advanced
GV.RR-02	Advanced	**GV.RR-03**	Established	**GV.RR-04**	Advanced
GV.SC-01	Established	**GV.SC-02**	Advanced	**GV.SC-03**	Established
GV.SC-04	Established	**GV.SC-05**	Established	**GV.SC-06**	Developing
GV.SC-07	Advanced	**GV.SC-08**	Established	**GV.SC-09**	Established
GV.SC-10	Informal				
ID: Identify					
ID.AM-01	Advanced	**ID.AM-02**	Established	**ID.AM-03**	Established
ID.AM-04	Established	**ID.AM-05**	Advanced	**ID.AM-07**	Developing
ID.AM-08	Advanced	**ID.IM-01**	Advanced	**ID.IM-02**	Established
ID.IM-03	Established	**ID.IM-04**	Advanced	**ID.RA-01**	Advanced
ID.RA-02	Established	**ID.RA-03**	Advanced	**ID.RA-04**	Established
ID.RA-05	Advanced	**ID.RA-06**	Advanced	**ID.RA-07**	Established
ID.RA-08	Established	**ID.RA-09**	Established	**ID.RA-10**	Developing
PR: Protect					
PR.AA-01	Established	**PR.AA-02**	Advanced	**PR.AA-03**	Advanced

Control	Rating	Control	Rating	Control	Rating
PR.AA-04	Advanced	**PR.AA-05**	Established	**PR.AA-06**	Advanced
PR.AT-01	Advanced	**PR.AT-02**	Developing	**PR.DS-01**	Advanced
PR.DS-02	Advanced	**PR.DS-10**	Established	**PR.DS-11**	Advanced
PR.IR-01	Advanced	**PR.IR-02**	Established	**PR.IR-03**	Established
PR.IR-04	Advanced	**PR.PS-01**	Advanced	**PR.PS-02**	Advanced
PR.PS-03	Established	**PR.PS-04**	Established	**PR.PS-05**	Advanced
PR.PS-06	Established				
DE: Detect					
DE.AE-02	Advanced	**DE.AE-03**	Established	**DE.AE-04**	Advanced
DE.AE-06	Advanced	**DE.AE-07**	Advanced	**DE.AE-08**	Advanced
DE.CM-01	Advanced	**DE.CM-02**	Established	**DE.CM-03**	Advanced
DE.CM-06	Developing	**DE.CM-09**	Advanced		
RS: Respond					
RS.AN-03	Advanced	**RS.AN-06**	Established	**RS.AN-07**	Developing
RS.AN-08	Advanced	**RS.CO-02**	Advanced	**RS.CO-03**	Established
RS.MA-01	Established	**RS.MA-02**	Established	**RS.MA-03**	Advanced
RS.MA-04	Established	**RS.MA-05**	Advanced	**RS.MI-01**	Advanced
RS.MI-02	Established				
RC: Recover					
RC.CO-03	Advanced	**RC.CO-04**	Developing	**RC.RP-01**	Advanced
RC.RP-02	Advanced	**RC.RP-03**	Advanced	**RC.RP-04**	Established
RC.RP-05	Advanced	**RC.RP-06**	Established		

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.