SECURITY RISK ASSESSMENT

A Beginner-Friendly Template for Small and Medium Businesses

Plain language. Worked examples. No jargon required.

Company Name	_____
Assessment Date	_____
Completed By	_____
Next Review Date	_____
Approved By	_____

How to Use This Document

If you have never done a risk assessment before, don't worry. This document walks you through it step by step. You don't need to be a cybersecurity expert, and you don't need any special tools beyond a word processor and maybe a spreadsheet.

What is a risk assessment?

A risk assessment is just a structured way of answering three questions:

1. What bad things could happen to my business?
2. How likely is each one, and how bad would it be?
3. What am I going to do about it?

That's it. Everything else is just detail.

How long will this take?

For a small business (under 50 employees), expect 4–8 hours spread across a week or two. Don't try to do it all in one sitting. Work through one section at a time, talk to people in your company who know the systems, and come back to tough questions later.

Who should be involved?

- At least one person who knows how the business runs day to day (owner, operations manager)
- Someone who knows the IT setup (internal IT, managed service provider, or whoever fixes computers)
- Someone who handles money and sensitive data (finance, HR)
- If you have legal or compliance obligations, the person responsible for them

You don't need all of them in the same room. A 20-minute conversation with each is often enough.

The sections in this document

- Section 1 — What You're Protecting: List your important stuff (data, systems, people, physical assets).
- Section 2 — What Could Go Wrong: Identify the threats that apply to you.
- Section 3 — How to Score Risks: A simple 1–5 scale for likelihood and impact.
- Section 4 — The Risk Register: The main worksheet where you write it all down.
- Section 5 — Treatment Plan: Deciding what to actually do about each risk.
- Section 6 — Control Checklist: Quick yes/no check of basic security controls.
- Section 7 — Keeping It Alive: How to make sure this doesn't become a dusty document.

Tip: Skim the whole document first before filling anything out. You'll make better decisions once you see how the pieces fit together.

Section 1 — What You're Protecting (Asset Inventory)

Before you can protect things, you need to know what things you have. This is called an asset inventory. An "asset" is just anything valuable to your business — if you lost it, stole it, broke it, or leaked it, you'd have a problem.

The five categories of assets

Most small businesses have assets in these five buckets. Don't overthink it — list the obvious stuff first.

Category	What it means	Examples for a typical business
Data	Information your business creates, stores, or processes.	Customer records, employee files, financial records, contracts, passwords, intellectual property.
Systems & Software	The tools used to run the business.	Email, accounting software, CRM, point-of-sale, website, internal network, cloud storage.
Hardware	The physical equipment that holds or runs the systems.	Laptops, phones, servers, routers, printers, payment terminals, security cameras.
People	Anyone with access to systems, data, or facilities.	Employees, contractors, vendors, cleaning staff, delivery drivers.
Physical & Facilities	Locations and the things in them.	Office, warehouse, server room, filing cabinets, keys and access cards.

Worksheet: Your asset inventory

Fill in your top assets. You don't need to list every pen and paperclip — focus on things where loss, damage, or exposure would genuinely hurt the business. Aim for 15–30 entries total.

#	Category	Asset	Why it matters (what happens if lost?)	Owner
1	Data	Customer database (names, emails, purchase history)	Lost trust, regulatory fines, can't contact customers	Sales Manager
2	Systems	Accounting software (QuickBooks Online)	Can't invoice, can't pay bills, tax problems	Finance Lead
3				

#	Category	Asset	Why it matters (what happens if lost?)	Owner
4				
5				
6				
7				
8				
9				
10				
11				
12				

The yellow rows are examples. Replace them or add more rows as needed.

Section 2 — What Could Go Wrong (Threat Catalog)

A threat is anything that could cause harm to one of your assets. You don't have to invent these from scratch — most businesses face the same set of common threats. Read through the list below and mark which ones apply to you.

Common threats for most businesses

Cyber threats

- Phishing emails — someone tricks an employee into clicking a link or handing over credentials.
- Ransomware — malicious software locks your files and demands payment.
- Business email compromise — an attacker poses as a colleague or vendor to redirect a payment.
- Stolen or weak passwords — attacker reuses a breached password or guesses an obvious one.
- Unpatched software — a known vulnerability in software you never updated gets exploited.
- Malicious website or download — an employee visits a compromised site and infects their device.

People threats

- Accidental mistakes — someone emails the wrong attachment, deletes a critical file, or misconfigures a setting.
- Insider misuse — an employee takes data with them when they leave, or abuses their access.
- Social engineering — someone talks their way into information or a building by pretending to belong.
- Lost or stolen device — a laptop or phone goes missing with company data on it.

Physical threats

- Break-in or theft — someone breaks in and takes equipment or documents.
- Fire, flood, or power loss — building or equipment is damaged.
- Unauthorized access — a visitor, ex-employee, or stranger enters a restricted area.

Third-party and supply chain threats

- Vendor breach — a supplier you share data with gets hacked.
- Service outage — a cloud provider goes down and you can't operate.
- Contractor access abuse — a contractor misuses access you gave them.

Compliance and legal threats

- Regulatory non-compliance — you fail a requirement (privacy law, PCI, HIPAA, etc.) and get fined.
- Contract breach — you lose a customer because of missed security obligations.

Don't try to think of everything

A common mistake is trying to brainstorm every possible bad thing. Don't. Start with this list, add the two or three industry-specific threats you know about, and move on. You can always add more later.

Example: A dental office might add "patient record disclosure violating HIPAA" to the list. A retailer might add "payment card skimmer installed on point-of-sale terminal." A construction company might add "equipment theft from job site." Use what you know about your own business.

Section 3 — How to Score Risks

To compare risks to each other, you need a consistent scoring method. We'll use a simple 1–5 scale for two things:

4. Likelihood — how likely is this to happen in the next year?
5. Impact — if it did happen, how bad would it be?

Multiply them together and you get a risk score from 1 to 25. Higher = more urgent.

Likelihood scale

Score	Label	Plain-language meaning	Rough rule of thumb
1	**Rare**	Would be surprising if it happened.	Less than once every 5 years.
2	**Unlikely**	Could happen, but probably won't.	Roughly once every 2–5 years.
3	**Possible**	Might happen from time to time.	Roughly once a year.
4	**Likely**	Expect it to happen at some point this year.	Several times a year.
5	**Almost certain**	Already happens or will happen soon.	Monthly or more often.

Impact scale

Score	Label	What this looks like for the business	Rough financial yardstick
1	**Minimal**	Minor nuisance, handled within a day.	Less than a day's revenue.
2	**Minor**	Noticeable disruption, limited customer impact.	A few days of revenue or under 1% of annual.
3	**Moderate**	Significant disruption, some customers affected, reputation dings.	Roughly 1–5% of annual revenue.
4	**Major**	Business stops for days, major customer or legal problems.	5–20% of annual revenue.

Score	Label	What this looks like for the business	Rough financial yardstick
5	**Severe**	Existential — business may not recover.	More than 20% of annual revenue, or regulatory shutdown.

The risk matrix

Multiply Likelihood × Impact to get a score from 1 to 25. Use the color to figure out how urgent it is.

	Impact 1	Impact 2	Impact 3	Impact 4	Impact 5
Likelihood 5	**5**	**10**	**15**	**20**	**25**
Likelihood 4	**4**	**8**	**12**	**16**	**20**
Likelihood 3	**3**	**6**	**9**	**12**	**15**
Likelihood 2	**2**	**4**	**6**	**8**	**10**
Likelihood 1	**1**	**2**	**3**	**4**	**5**

What the colors mean

Color	Score	What to do
Low	1–4	Acceptable. Note it, but no action required beyond normal hygiene.
Medium	5–9	Worth addressing when convenient. Plan improvements within 6 months.
High	10–15	Needs action. Assign an owner and a deadline within 1–3 months.
Critical	16–25	Stop and fix. Escalate to leadership. Work on it this week.

A worked example

Risk: An employee falls for a phishing email and their password is stolen.

Likelihood = 4 (Likely). Phishing emails arrive weekly, and not everyone on staff is trained. At some point, somebody will click.

Impact = 3 (Moderate). The employee has access to the shared drive and customer email list, but not to financial systems. We'd lose a day dealing with it and might have to notify customers.

Risk score = 4 × 3 = 12 (High). Needs action — plan phishing training and multi-factor authentication within 1–3 months.

Section 4 — The Risk Register

This is the heart of the assessment. For each risk you care about, fill in one row. Start with maybe 10–15 of the most important ones — you don't need hundreds.

How to fill in each column

- ID — Just a number (R-01, R-02, etc.). Makes it easy to refer to later.
- Risk description — One sentence: "What could happen to which asset, caused by what." Example: "Customer database exposed due to a ransomware attack."
- Asset affected — From your Section 1 inventory.
- Threat source — From your Section 2 list.
- Likelihood (1–5) — Using the scale in Section 3.
- Impact (1–5) — Using the scale in Section 3.
- Score — Likelihood × Impact.
- Existing controls — What you're already doing about it (firewall, backups, training, etc.).
- Treatment — See Section 5. Usually "Reduce," but can also be Accept, Transfer, or Avoid.
- Owner — Who is responsible for doing something about it.
- Target date — When will the action be complete?

Tip: Don't get stuck trying to perfect each score. Risk scoring is deliberately approximate. If you can't decide between a 3 and a 4, pick one and move on — you can refine it later.

Risk register worksheet

Two example rows are filled in (yellow). Replace them with your own, and add more rows as needed.

ID	Risk description	Asset	Threat	L	I	Score	Existing controls	Owner	Due
R-01	Employee tricked by phishing email, credentials stolen	Email account	Phishing	**4**	**3**	**12**	Spam filter, basic annual training	IT Manager	Q2
R-02	Laptop stolen from car with unencrypted customer data	Laptops, customer data	Theft	**2**	**4**	**8**	Password on laptop, locked office	IT Manager	Q2
R-03									
R-04									
R-05									

ID	Risk description	Asset	Threat	L	I	Score	Existing controls	Owner	Due
R-06									
R-07									
R-08									
R-09									
R-10									
R-11									
R-12									
R-13									
R-14									

L = Likelihood, I = Impact, Score = L × I. For a roomier version, rebuild this as a spreadsheet — it's easier to sort and filter.

Section 5 — Treatment Plan (What to Do About Each Risk)

For every risk, you have four choices. There's no "right" answer — the right choice depends on the cost, the severity, and what else is going on in the business.

Option	What it means	When to use it	Example
Reduce	Put controls in place to make it less likely, less impactful, or both.	Most of the time. This is your default answer.	Add multi-factor authentication to reduce the risk of stolen passwords.
Transfer	Shift the risk to someone else — usually through insurance or by outsourcing.	When the impact is big but it's not cost-effective to reduce further on your own.	Buy cyber insurance to cover ransomware recovery costs.
Avoid	Stop doing the activity that creates the risk.	When the activity isn't essential and the risk is high.	Stop storing credit card numbers yourself and use a payment processor instead.
Accept	Acknowledge the risk and decide to live with it.	When the risk is low, or when the cost of fixing exceeds the cost of the problem.	Accept that a minor website outage could cost a few hours of traffic each year.

Accepting a risk is a real decision

Accepting a risk doesn't mean ignoring it. It means you've looked at it, made an informed decision that the cost of treatment isn't worth it right now, and documented that decision. If the situation changes (the risk grows, a cheap fix becomes available), you revisit it.

Whenever you accept a risk that's Medium or higher, write down who made the decision and why. This matters a lot if something goes wrong later — you'll want evidence that it was a conscious, reasoned choice.

Action plan worksheet

For every High and Critical risk, fill in one row here with the specific actions you're going to take.

Risk ID	Action to take	Expected outcome	Owner	Due date
R-01	Enable MFA on email; run phishing simulation every quarter.	Reduce likelihood from 4 to 2.	IT Manager	End of Q2

Risk ID	Action to take	Expected outcome	Owner	Due date

Section 6 — Basic Security Control Checklist

Here's a quick gut-check of the controls most businesses should have in place. If you can't check a box, that's a clue that you probably have an elevated risk somewhere in your register.

This is not an exhaustive list — it's a starting point based on common advice from sources like CIS Controls, NIST, and the UK's Cyber Essentials. If you're subject to specific regulations (HIPAA, PCI DSS, GDPR, etc.), your list will be longer.

Identity and access

- ☐ Every person has their own account — nobody shares logins.
- ☐ Multi-factor authentication (MFA) is turned on for email, admin accounts, and anything touching the internet.
- ☐ Passwords are at least 12 characters OR managed with a password manager.
- ☐ When someone leaves the company, their access is revoked the same day.
- ☐ Administrator accounts are only used for admin work — not everyday browsing or email.

Devices and software

- ☐ Operating systems and applications are set to auto-update.
- ☐ Antivirus or endpoint protection is installed on every computer.
- ☐ Laptops and phones have full-disk encryption turned on.
- ☐ A device can be remotely wiped if it's lost or stolen.
- ☐ An up-to-date list of every device that accesses company data exists.

Data and backups

- ☐ Critical data is backed up daily.
- ☐ Backups are tested at least quarterly to make sure they actually restore.
- ☐ At least one backup copy is offline or immutable (so ransomware can't encrypt it).
- ☐ Sensitive data (customer records, financials) is only accessible to people who need it.
- ☐ Old data is deleted on a schedule — don't keep what you don't need.

Network and email

- ☐ The office network has a firewall and the default admin password has been changed.
- ☐ Wi-Fi uses WPA2 or WPA3, and guests use a separate network.
- ☐ Email has SPF, DKIM, and DMARC set up to prevent spoofing.
- ☐ Remote access uses a VPN or equivalent secure method, not direct exposure to the internet.

People and process

- ☐ All staff get security awareness training at least once a year.
- ☐ Phishing simulations are run at least twice a year.
- ☐ A written incident response plan exists and at least one person knows where it is.
- ☐ Key vendors have been asked about their security posture.
- ☐ Someone knows how to reach regulators, insurers, and law enforcement if something goes wrong.

Physical

- ☐ The office is locked when unattended, and keys/access cards are tracked.
- ☐ Visitors are signed in and escorted.
- ☐ Server rooms or equipment closets are locked.
- ☐ Paper records with sensitive data are stored in locked cabinets.
- ☐ A shredder is used for sensitive printed documents.

Section 7 — Keeping This Assessment Alive

The biggest mistake with risk assessments is treating them as a one-time project. The value comes from updating them regularly and using them to make real decisions.

A simple maintenance rhythm

How often	What to do	Why
Monthly	Check progress on action items.	Keeps treatments moving forward instead of sitting on a shelf.
Quarterly	Review the register for new or changed risks.	New tools, new staff, new vendors, and new threats all appear between annual reviews.
Annually	Full refresh of the whole document.	Re-score everything, re-check controls, get leadership sign-off again.
After any incident	Update the relevant risk.	If something happened, your likelihood estimate was probably wrong. Use the evidence.
After any big change	Reassess affected areas.	New system, new location, new product, acquisition — all change your risk picture.

Signs you're doing it right

- Leadership can name the top three risks without looking them up.
- When someone proposes a new project, somebody asks "what does this do to our risk register?"
- The register shrinks and grows over time as risks are resolved and new ones appear — it's not static.
- The same risks don't keep showing up year after year with no progress.

Signs something's off

- The document looks exactly the same as last year.
- Every risk is scored Medium (it means you're not really thinking about them).
- The people responsible for the actions didn't know they were assigned.
- Nobody outside of IT or security has read it.

Where to go next

Once you're comfortable with this assessment, you may want to go deeper. Good places to start:

- CIS Critical Security Controls — a prioritized list of things to implement. Practical and free.

- NIST Cybersecurity Framework (CSF) — a widely used framework for organizing security work. More formal.
- ISO 27001 — a certifiable standard, useful if customers or partners demand it.
- Cyber Essentials (UK) or Essential Eight (Australia) — national-level baselines with clear checklists.

You don't need to adopt all of them. Pick the one whose style matches your business, and use this risk assessment alongside it.

Sign-off

This assessment has been reviewed and approved. Action items have been assigned and will be tracked to completion.

_____ Name	_____ Signature	_____ Date
_____ Name	_____ Signature	_____ Date