Vendor Risk Management Framework

A practical framework for small and mid-sized businesses that rely on outside suppliers for systems, data and services.

Nov 10, 2026 · @Vijay Srinivas Kothapalli

Purpose

Most businesses now depend on outside suppliers for systems, data processing, payroll, logistics, IT support and back-office work. Each supplier can become a route into your business, or a point of failure. This framework gives management a repeatable way to decide which suppliers to use, how to protect the business in each contract, and how to keep watch once the work has started.

It is written for owners, directors and managers who make buying decisions without a dedicated procurement or risk team.

Scope

The framework applies to every supplier that does any of the following:

- Holds personal, customer, employee or financial data on your behalf.
- Has remote or administrator access to your systems or premises.
- Runs a process that you depend on, such as payroll, billing, dispatch or accounts.
- Provides software or cloud services that your business relies on.

A supplier that sells a one-off item with no data or system access can be handled with a simple purchase check only.

The vendor risk lifecycle

The framework has five stages. Each supplier passes through them in order, and the cycle repeats for as long as the relationship lasts.

1. **Identify and classify.** Record the supplier and rate its risk tier.
2. **Assess before contracting.** Check security, privacy and continuity before signing.
3. **Contract for protection.** Write the protections you need into the agreement.
4. **Monitor and review.** Check performance and risk at the frequency its tier requires.

5. **Exit.** Remove access and retrieve or delete data when the relationship ends.

Stage 1: Identify and classify

List every supplier in one register, then rate each one by the harm it could cause if it failed or misused its access. Use three tiers.

Tier	Typical examples	What it means
High	Cloud hosting, payroll, IT support with admin access, payment processors	Could stop the business or expose large amounts of data
Medium	Accounting firms, logistics partners, marketing platforms with customer lists	Could cause significant disruption or a contained data breach
Low	Office supplies, cleaning, software with no data or access	Limited harm if the supplier fails

Re-rate a supplier whenever its access, data or importance to operations changes. Record the owner for each supplier, the data it touches and the date of its last review.

Stage 2: Assess before contracting

Assess High-tier suppliers fully, Medium-tier suppliers in a shorter form, and Low-tier suppliers with a simple check. Ask for evidence, not only answers. Assess these areas:

1. **Security.** Multi-factor sign-in, encryption of data in transit and at rest, access controls, and how quickly they patch.
2. **Privacy.** Where personal data is stored and processed, whether they use other suppliers, and how they handle requests and deletion.
3. **Incidents.** How they detect, report and recover from incidents, and when they last had one.
4. **Continuity.** Their backup arrangements, recovery time, and what happens to your data if they close.
5. **Ownership and finances.** Whether they are financially stable and who controls them.
6. **Certifications and reports.** Any independent security report or certificate, checked for scope and date.

A supplier that refuses to answer or to provide evidence for High-tier work should not be used for that work.

Stage 3: Contract for protection

The contract is where your protections become enforceable. Include these terms for High and Medium tier suppliers:

- **Security standards:** a clear description of the controls the supplier must maintain.
- **Incident notice:** the supplier must tell you about a security incident affecting your data within a set time, such as 24 to 48 hours.
- **Data use and location:** what the supplier may do with your data, where it is kept, and that it cannot be sold or reused without consent.
- **Subcontractors:** they must tell you about and bind any subcontractor that handles your data to the same standards.
- **Audit and evidence:** you can request evidence of controls each year and, for High-tier suppliers, carry out or commission an audit.
- **Service levels and recovery:** agreed uptime and the time to restore service after an outage.
- **Liability and insurance:** responsibility for losses caused by the supplier's breach, and proof of cover.
- **Return and deletion:** your data is returned in a usable form and deleted on termination, with written confirmation.

Have a lawyer review High-tier contracts. For standard terms that a supplier will not change, record the gap and decide whether to accept it.

Stage 4: Monitor and review

Review each supplier at the frequency its tier requires, and whenever something changes.

Tier	Full review	Light check	Trigger for an early review
High	Yearly	Quarterly: service, incidents and access	New data type, new access, a reported incident, change of ownership

Tier	Full review	Light check	Trigger for an early review
Medium	Every two years	Yearly: certificates and incidents	Significant change in service or scope
Low	Only when the contract renews	None	Price or scope change

For each review, check:

- Did the service meet the agreed levels, and were there outages?
- Were there any security incidents or near misses, and were they reported on time?
- Are the people who have access still the right people, and is access still needed?
- Has the supplier changed its subcontractors, location or ownership?
- Are any findings from the last review closed?

Record the outcome, the decision (continue, improve or exit) and the next review date.

Stage 5: Exit and offboarding

Many problems appear at the end of a relationship. Plan the exit when you sign the contract.

1. **Remove access.** Withdraw system accounts, remote access, keys and shared credentials on the day the service ends.
2. **Retrieve data.** Obtain a complete copy of your data in a usable format before termination.
3. **Confirm deletion.** Ask for written confirmation that the supplier has deleted your data, including backups, within the contractual period.
4. **Check for continuing duties.** Confidentiality and data protection obligations often survive the contract. Diarise them.
5. **Update the register.** Mark the supplier as closed and record the date and the evidence of deletion.

Roles and responsibilities

Role	Responsibility
Board or owner	Approves the framework, the high-tier supplier list and the risk appetite for outsourcing
Senior manager	Owns the framework, approves contracts for High-tier suppliers and reviews the register each quarter
Supplier owner (a manager in each business area)	Manages the relationship, assesses performance and raises issues early
Finance or procurement lead	Keeps the register, checks payment terms and confirms supplier onboarding is complete before the first payment
IT or operations lead	Assesses technical controls, manages supplier access and removes access at exit
Legal adviser	Reviews High-tier contracts and advises on notification duties

Where one person holds several roles, make sure the review is still independent: the person who selects a supplier should not be the only one who checks it.

Handling a vendor security incident

When a supplier reports an incident, or you suspect one:

1. **Log it.** Record the time you were told, by whom, and what they said.
2. **Confirm scope.** Ask which of your data or systems are affected, and whether the incident is contained.
3. **Assess your duties.** Decide whether customers, employees, the bank, insurers or a regulator must be told, and by when. Take advice on the legal position.
4. **Protect access.** If in doubt, suspend the supplier's access while the facts are established.
5. **Ask for the report.** Request a written root-cause report and the steps taken to prevent a repeat.

6. **Decide.** Continue, continue with conditions, or exit. Record the reasons and update the risk tier.

The contract should give you the right to these steps. If it does not, record that as a gap for the next renewal.

Implementing the framework in 60 days

Days	Action	Owner
1 to 15	Build the supplier register with every supplier, its owner and the data it touches.	Finance or procurement lead
1 to 15	Agree the three risk tiers and assign each supplier a tier.	Senior manager
16 to 30	Run full assessments for High-tier suppliers and record the gaps.	Senior manager with IT lead
16 to 30	Review the contract terms for High-tier suppliers against the list in Stage 3.	Legal adviser
31 to 45	Agree remediation for each gap, or decide to exit.	Supplier owners
31 to 45	Set the review calendar for each tier.	Finance or procurement lead
46 to 60	Report the first register and gap summary to the board.	Senior manager

After 60 days, the framework moves into routine operation, with the register reviewed each quarter.

Vendor register: fields and tiering criteria

Keep the register in a spreadsheet or a simple database. Each supplier should have these fields:

Field	Purpose
Supplier name and registered address	Identification

Field	Purpose
Service provided	What the business uses them for
Business owner	Who manages the relationship
Data types and volume	Personal, customer, financial or none
System or premises access	Remote, administrator, on-site or none
Tier (High, Medium, Low)	Drives assessment and review frequency
Contract end or renewal date	Trigger for review
Last assessment date and outcome	Evidence of control
Open findings and due dates	Remediation tracking
Incident history	Patterns of concern

To assign a tier, answer yes or no to each question. Any yes to the first two makes the supplier High tier.

- Does it hold personal or financial data, or could a failure stop a key process?
- Does it have administrator access to your systems?
- Would a breach affect more than a small group of customers or staff?
- Could you replace it within a month?

About CRCO LLP

CRCO LLP is a Hyderabad-based advisory firm working with businesses on cybersecurity, data privacy and protection, outsourcing, process improvement and automation. We help management set up supplier registers, assess vendors, negotiate protective contract terms and run the review cycle.

Book a consultation: visit the Contact page on our website, or write to us through the enquiry form.

This framework provides general guidance only. It is not legal advice. Contract and notification duties depend on your sector and circumstances, and should be confirmed with a qualified adviser.