Cybersecurity Risk Register Worksheet

A concern becomes useful when it leads to a named decision, a practical action and evidence of follow-through.

Start with one business scenario

Write: If [event] affects [service or dependency], the business could experience [consequence]. Explain existing safeguards and what remains unverified.

How to use these four pages

1. Read the prompts below. **2.** Review the fictional example. **3.** Complete one risk record. **4.** Assign the action and review its outcome. Copy blank pages for additional scenarios.

Describe priority; do not manufacture precision

Discussion point	Record the reason
Potential harm	What work, people, information, money or obligations could be affected? Explain your low, medium or high description.
Plausibility / uncertainty	Over what period could this happen? What evidence supports your judgement? Use “not yet verified” for material unknowns.
Attention needed	Why does this scenario need action now or later? Include dependencies, deadlines and consequences of delay.

The labels are discussion aids, not calibrated probabilities. Do not multiply ordinal ratings and present the result as a precise measurement.

Keep the record proportionate and protected

The risk owner decides the response and remaining exposure; the action owner performs the work. They can be the same person. Keep completed records confidential: they may describe vulnerabilities, accounts or recovery arrangements. Do not write passwords or secret recovery codes here.

Source guidance

NIST SP 1300, Small Business Quick-Start Guide (26 February 2024)
https://csrc.nist.gov/pubs/sp/1300/final

NIST SP 1303, Enterprise Risk Management Quick-Start Guide (October 2024)
https://csrc.nist.gov/pubs/sp/1303/final

Original GRCPreneur design and examples. Sources inform the approach; no endorsement is implied.

A completed example

Fictional example: an online consultancy depends on a contractor-controlled booking account. This is a management discussion, not a universal account configuration.

Record	Illustrative entry
Risk / service	R-01 | Customer bookings
Scenario	If the only administrator loses access, the business may be unable to update appointments or receive new bookings.
Evidence and unknowns	Only one administrator is listed. Recovery steps have not been demonstrated. No incident is asserted.
Priority	Potential business harm: high. Plausibility: uncertain pending review. Prioritise because an important service depends on one person.
Current safeguards	Provider support is available. Its account-recovery scope and availability still need confirmation.
Risk owner / decision	Business owner. Establish business-controlled recovery access with the provider and record the agreed responsibilities.
Action owner / due date	Provider performs the agreed change; business owner verifies the recovery route. Set an achievable date before work starts.
Completion evidence	An authorised, safe demonstration of the recovery process and an accessible responsibility record.
Remaining exposure / review	Provider outages can still interrupt bookings. Revisit when provider, account ownership or recovery settings change.

What makes the record useful?

It distinguishes observed facts from assumptions, assigns an owner and states what completion evidence is needed. A green status without evidence would not resolve the original concern.

The available response may reduce, avoid, share or accept exposure. Outsourcing or insurance does not automatically transfer every responsibility. Decisions must fit the actual arrangement.

Your risk record

Record ID: _____ Date: _____ Next review: _____

Business activity, system or supplier affected

Scenario: event -> affected dependency -> business consequence

Existing safeguards; evidence checked and its date; important unknowns

Potential harm, plausibility and reason for priority (include uncertainty)

Risk owner; decision; options considered and reason for the chosen response

Remaining exposure and who is authorised to accept it

Do not record passwords, authentication codes or confidential customer examples. Use references to protected evidence instead.

Action and review

Related risk record: _____ Review date: _____

Agreed action	Action owner / due date	Evidence of completion

What evidence changed our understanding? What is still unverified?

Remaining exposure, owner decision and next review trigger

Close the loop

Check that the action addresses the scenario, not only that a document exists. If work is delayed, record the reason and any interim decision. Review sooner if the service, supplier, access arrangements or obligations change.

General management guidance. This worksheet is not a technical assessment, a compliance certification or a substitute for appropriate specialist advice.