

Cybersecurity Risk Assessment Worksheet

Identify your key business assets, the threats they face and what to fix first, using a simple likelihood and impact scoring method.

An initial prioritisation aid, not a formal compliance assessment

This worksheet helps you decide what to focus on first. It is not a formal risk assessment, audit or compliance assessment, and the ratings are a guide for discussion rather than a definitive measure of risk.

Business name

Completed by

Date

Next review date

How to score each risk

For each business asset or process, think about a realistic threat. Score how **likely** it is to happen and how much **impact** it would have, each from 1 to 5, taking your existing controls into account. Multiply the two scores to get the **risk score**, then use the rating bands to prioritise.

Score	Likelihood: how likely is it?	Impact: how bad would it be?
1	Rare. Hard to imagine happening in the next few years.	Minimal. Barely noticeable, fixed within hours at little cost.
2	Unlikely. Could happen but not expected.	Minor. Some inconvenience, fixed within a day.
3	Possible. Might happen in the next year or two.	Moderate. Disruption for several days, noticeable cost or customer impact.
4	Likely. Expected to happen in the next year.	Major. Serious disruption, data loss, financial loss or reputational harm.
5	Almost certain. Already happening or expected soon.	Severe. Threatens the survival of the business or causes serious harm to people.

Risk score (likelihood × impact)	Rating	Suggested response
1 to 4	Low	Accept and monitor, or improve when convenient.
5 to 9	Medium	Plan improvements within the next few months.
10 to 16	High	Prioritise. Act within weeks and assign an owner.
20 to 25	Critical	Act now. Seek professional help if needed.

Treatment options

Reduce the risk by adding or improving controls. **Transfer** part of it, for example through insurance or a supplier. **Avoid** it by stopping the activity. **Accept** it, if it is within what the business is comfortable with. Record the risk that remains after treatment as the **residual risk**.

Risk worksheet

Business asset or process	Threat	Existing controls	Potential business impact	Likelihood (1–5)	Impact (1–5)	Risk rating	Recommended treatment	Responsible person	Target date	Residual risk	Review date
Example: customer email	Account takeover by phishing										

The first row shows the kind of entry to make. Use additional copies of this page as needed.

Need a hand?

Omnicon I.T. Services can help you put this into practice. Visit **omnicron.com.au/contact-us**, call **(03) 9022 1376** or email **admin@omnicron.com.au**.

This resource provides general guidance only. It is not legal advice, a formal audit, a compliance certification or an official government assessment. Your obligations depend on your industry, contracts and circumstances.