REGISTER

The Enterprise Risk Register and Board Risk Appetite Statement

What this is	A pre-populated risk universe for human services, a scoring method that resists false precision, the four treatment responses, and the board risk appetite statement that tells management what it may decide without asking.
It assumes	A board that meets at least quarterly. You do not need a risk officer, a committee, or software.
Change before use	Which risks apply, every score, every owner, and the appetite thresholds — those are your board's to set and nobody else's.

The problem this fixes

Risk in most organizations is discussed twice: informally, by people who cannot act on it, and formally, after something has already happened. In between there is usually no register, no owner, and no agreed statement of what the board is willing to tolerate. The result is that every risk decision is made at the wrong altitude — either escalated to a board that lacks the detail, or absorbed by a manager who lacks the authority.

A register fixes the first half of that. The **risk appetite statement** fixes the second, and it is the half almost everyone omits. It is the document that lets a manager say "this is within what the board has already accepted" and be right — and lets them recognize the moment when it is not.

WHAT THIS IS NOT

This is not legal, insurance, or safeguarding advice, and it is not a compliance program. It is a structure for identifying, scoring, owning, and reporting risk.

It does not tell you what your risk appetite should be. That is a board judgment about your mission, your reserves, and the people who depend on you, and no external document can make it for you.

The risk universe below is a starting list for this sector, not a complete one. Every organization carries risks that are not on it.

The risk universe

Start here rather than from a blank page. Delete what does not apply, and add what is missing — the additions are usually the most valuable rows in the register.

Category	Risks that commonly sit here
Safety of people served	Harm during service delivery; failure to identify or escalate a concern; inadequate screening or supervision of those in contact with vulnerable people

Category	Risks that commonly sit here
Licensing and regulatory	License condition breached; adverse finding; inability to produce evidence on inspection; a change in regulation the organization does not notice in time
Funding and contracts	Concentration in a single payer; non-renewal or re-procurement; rate set below cost; disallowed costs on audit
Financial	Liquidity shortfall; reserve depletion; payroll interruption; going-concern exposure
Workforce	Key-person dependency; vacancy in a licensed role; sustained turnover; inability to recruit in a required discipline
Information and technology	Breach of confidential records; loss of the case system; unsupported software; vendor failure
Governance and conflict	Undisclosed conflict of interest; board unable to form a quorum; decisions taken without a recorded basis
Third parties	Failure of a critical vendor, subcontractor, or fiscal partner; unclear responsibility at a handover
Continuity	Loss of premises, systems, cash access, or key people — see the Continuity of Operations Plan
Reputational	Loss of confidence among referrers, funders, or the community, whether or not the underlying event was the organization's fault

Scoring, without pretending

Score likelihood and impact on a five-point scale, and **define every point in words before you use it**. A register where "3" means whatever each person thought it meant produces a heat map that looks rigorous and is not.

Score	Likelihood — define in frequency	Impact — define in consequence, not only dollars
1	Would be surprising within five years	Absorbed within normal operations
2	Possible within five years	Noticeable; managed without external involvement
3	Likely within three years	Material; requires board awareness and external notification
4	Likely within twelve months	Serious; harm to a person served, a license condition, or a major funding relationship
5	Expected, or has already happened this year	Severe; threatens the organization's ability to continue or causes serious harm

Adapt these definitions to your organization — but write them down, put them at the front of the register, and use the same ones every time. The definitions are the instrument; the numbers are just how it is recorded.

Inherent and residual

Score each risk twice. **Inherent** is the score with no controls at all. **Residual** is the score given the controls you actually have and can evidence — not the ones in a policy that nobody follows. The gap between the two is the value your controls deliver, and a risk where inherent and residual are identical is telling you something.

> **SCORE WHAT YOU CAN EVIDENCE**
>
> The single most common failure in a register is scoring the residual risk as though a control works because it exists on paper. If you cannot produce evidence that a control operated — a record, a log, a signed checklist — score it as though it did not. The register is not a place to be reassuring.

The four treatment responses

Every risk gets exactly one, chosen deliberately and recorded.

Response	What it means	The trap
Tolerate	Accept it at its current level; no further action	Tolerating by default, having never decided. A tolerated risk must be an explicit choice, minuted.
Treat	Add or strengthen a control to reduce likelihood or impact	A treatment with no owner and no date is a wish. Both are mandatory columns.
Transfer	Move the financial consequence elsewhere, usually by insurance or contract	Insurance transfers cost. It does not transfer the harm, the obligation, or the reputational consequence — and never the duty to the person affected.
Terminate	Stop the activity that creates the risk	Rarely available in a mission-driven organization, but it belongs on the list so that it is consciously ruled out rather than forgotten.

Owners

One named person per risk. Not a department, not a committee, not "management". The owner is accountable for the treatment happening, not necessarily for doing it. **A risk with no named owner is not being managed, and the register should show that plainly rather than hide it behind a job title.**

The heat map, and its dangers

A heat map is a communication device, not an analysis. It earns its place because a board absorbs it in seconds. It misleads in three ways worth guarding against.

1. **False precision.** A 4×3 and a 3×4 both score twelve and are not remotely the same risk. Never rank by the product alone; the two dimensions mean different things.
2. **Color alone.** Roughly one in twelve men has a color vision deficiency, and red-green is the common one. Label every plotted risk with its number and name — never rely on the color to carry the meaning.

3. **The comfortable middle.** Registers drift toward threes because a three requires no argument. If most of your risks score three on both axes, the scoring conversation has not actually happened.

The board risk appetite statement

This is the part that changes how the organization operates, and it takes one board meeting to write. It states, for each category, what the board is willing to accept — so that management knows the boundary of its own authority without asking.

Appetite is not uniform. A serious organization has almost none in some categories and a good deal in others, and saying so out loud is the point.

Category	Appetite	What that means in practice — illustrative wording
Safety of people served	None	We accept no avoidable risk to the safety of people in our care. Cost is not a reason to reduce a safeguarding control. Any such proposal comes to the board.
Licensing and regulatory	None to low	We do not accept known breaches. We accept the risk inherent in operating in a regulated field, and we invest ahead of requirements rather than after findings.
Financial	Low	We accept planned deficits where funded by reserves and approved in advance. We do not accept unplanned deficits or reserves falling below the adopted target for more than two quarters.
Funding concentration	Moderate, reducing	We accept present concentration because it reflects our mission, and we commit to reducing it. No single source above the adopted ceiling without a board-approved plan.
Program innovation	Moderate to high	We accept that new programs may fail. We require they be time-limited, evaluated, and funded so failure does not threaten existing services.
Information security	Low	We accept no avoidable risk to confidential records. Convenience is not a justification for weakening a control.
Reputational	Low	We accept the reputational risk of saying true things publicly, including about our own shortfalls. We do not accept risk arising from concealment.

Every word above is illustrative. Your board writes its own, argues about it properly, adopts it by resolution, and reviews it annually. The final row is the one boards find hardest and value most.

How to use it

- **As a decision rule.** A manager facing a choice checks the statement first. Within appetite, decide and record. Outside it, escalate. This removes an enormous amount of unnecessary escalation and, more importantly, catches the escalations that matter.
- **As a test of the register.** Any residual risk scoring above appetite for its category must have a live treatment with an owner and a date — no exceptions, and the register should make the exceptions visible.
- **As a governance record.** When a decision is later questioned, "this was within the appetite the board adopted in writing" is a materially stronger position than a recollection.

What the board sees, and when

Cadence	What is presented
Every meeting	Risks scoring above appetite, by exception only. Any new risk added since the last meeting. Any risk whose score moved, and why.
Quarterly	The full register, with the heat map and treatment progress against dates.
Annually	Re-score everything from scratch. Re-adopt or amend the appetite statement. Review the categories themselves — the universe changes.
On event	Any risk that materializes, with the register entry that anticipated it, or an honest note that none did. The second case is the more useful lesson.

Common failures

- **The register is written once and never re-scored.** It becomes a historical document that describes an organization that no longer exists.
- **Everything is amber.** Nobody wants to say "high" in writing. A register with no red is not a low-risk organization; it is an unfinished register.
- **Treatments have no dates.** The single strongest predictor of whether a register does anything.
- **The appetite statement is written by the executive.** It must be the board's, in the board's words, adopted by resolution — otherwise it is management marking its own boundary.
- **Risks the board would find uncomfortable are quietly omitted.** These are precisely the entries that justify the register existing.

Limits

- **A register does not reduce risk.** Treatments do, and only when someone does them by a date.
- **Scores are judgments, not measurements,** and should be presented as such. Any process that turns them into a single ranked number has thrown away the information.
- **This does not satisfy a specific regulatory risk requirement** unless you have checked that it does. Where a funder or license prescribes a format, use theirs.
- **It is not a substitute for insurance advice.** Your broker needs the register; the register does not replace the broker.

Published by The CARES Collaborative, a program of Knotts Family Services, Inc., for adaptation and use by charitable and community-serving organizations. No registration, no fee, no attribution required. This document is a working template, not legal, tax, or accounting advice — the requirements that apply to your organization are confirmed by your own counsel, auditor, and licensing authority. Version 1.0 · August 2026 · carescollaborative.org/open-shelf