Current version — Nov 1, 2026
Update history: continuityhub.org/risk-register-template-fields-owners-review-cadence/

RISK REGISTER QUICK CARD: THE ONE-ROW CONTRACT & LIVING CADENCE

The Core Operating Law (Post 667): "*The risk register is where risk management stops being a workshop and becomes a workload.*" It is the living list of what the organization has decided to worry about — each risk named, owned, scored, treated, and scheduled for another look. Without active upkeep, it deteriorates into an outdated spreadsheet that teams stop using.

1. THE ONE-ROW CONTRACT: THE FIELDS THAT EARN THEIR PLACE

A register row is a small contract. Every field must earn its place by enforcing operational accountability, verifiable control evidence, or a scheduled governance event:

Contract Field	Standard Definition & Precision Rule (Post 667)	Enforcement Gate / Anti-Pattern
1. Risk Event Statement	Stated as an event with a specific **cause** and **consequence** (e.g., *"ransomware encrypts the file estate during peak season, halting order processing"*).	**Refuse bare nouns** like "cyber," "supply chain," or "weather." Nouns are untestable, unownable, and unscoreable.
2. Named Owner	**One named individual** whose job includes this risk, positioned at a seniority level sufficient to fund and authorize its treatment.	**No departments, committees, or roles.** Assigning to a committee is assigning to no one. Single point of funding accountability.
3. Category	Hazard family or business line classification so the register can be filtered, aggregated, and read by strategic operational theme.	Must map directly to core operating functions or threat landscapes to enable thematic board-level reporting.
4. Inherent L × I	Exposure before controls — the raw flood plain, unpatched estate, or single critical supplier. Scored on risk matrix scales.	Evaluates absolute exposure without mitigation. Reflects intrinsic vulnerability of the unshielded operation.
5. Concrete Controls Today	Named concretely as operating today — not vague categories like "IT security", but specific segmentation, backup regimes, and monitoring.	Must exist in active operation today. Paper policies, unconfigured tools, and aspirational architectures are barred.
6. Residual L × I	Exposure remaining after accounting for concrete operational controls that are actively running and verifiable.	**The Evidence Gate:** Residual score moves only if you can point to the last verified control test date.
7. Treatment Decision	Explicit executive decision choosing one of four formal treatments: **Avoid**, **Reduce**, **Transfer**, or **Retain**.	Ambiguity prohibited. Retaining risk requires documented sign-off; avoiding requires decommissioning the exposure.
8. Action, Owner & Date	Where treatment requires active intervention: the specific action task, the single named action owner, and hard calendar target date.	Every "Reduce" or "Avoid" treatment must have a live action row. High-risk rows without actions/budgets are orphans.
9. Dates & Status	**Last reviewed date**, **next review date**, and register status (Active, Monitored, or Retired with documented rationale).	Rows without calendar dates are static archives. Retired rows must document why the hazard ceased to exist.

2. FULL WORKED CONTRACT ROW: THE RANSOMWARE PEAK-SEASON EXEMPLAR

Field	Exemplar Row Values (Post 667 Grounded)	Operational Audit Notes
Cause-Event-Consequence	Phishing / unpatched edge vulnerability allows ransomware to encrypt file estate during peak seasonal demand, halting order fulfillment.	Passes event test: explicit trigger (unpatched edge), concrete failure (encryption), quantified operational consequence (halted orders).
Named Risk Owner	Sarah Lin, VP of Enterprise Technology & Infrastructure	Single named officer with autonomous budget authority to procure software, retain forensic incident response, and enforce patching.
Category	Cyber Hazard / Core Commercial Operations	Cross-functional theme: bridges technology infrastructure and frontline supply chain fulfillment.
Inherent L × I	Likelihood: 4 (Likely) • Impact: 5 (Catastrophic) • Score: 20/25	Uncontrolled exposure reflects unsegmented file estate and unverified backup restores during peak revenue window.
Concrete Controls Operating Today	(1) Micro-segmentation between corporate and order processing systems; (2) Immutable offline backup regime; (3) 24/7 Managed EDR monitoring.	All controls named concretely. Not "IT security" or "cyber policy," but specific technical layers actively running.
Residual L × I	Likelihood: 2 (Unlikely) • Impact: 3 (Moderate) • Score: 6/25	Score reduction justified strictly by verified control tests: offline restore test (2026-09-14) and quarterly penetration test (2026-10-02).
Treatment Decision	**Reduce** (Mitigate operational outage window via immutability)	Formally approved treatment. Target residual threshold established in enterprise risk governance policy.
Action, Owner & Date	Deploy automated immutable air-gap replication for secondary storage • Owner: Dave Miller (Sr NetSec) • Due: Dec 15, 2026	Specific action item with assigned delivery engineer and hard pre-peak completion milestone.
Review Dates & Status	Last Reviewed: Oct 15, 2026 • Next Review: Jan 15, 2027 • Status: **Active (Top Tier)**	Assigned to Quarterly Top-Residual Owner Review schedule due to high inherent impact.

The Critical Distinction — Risk Register vs. Risk Matrix (Post 667 FAQ):

- **The Risk Register** is the record — every risk with its named owner, verified controls, treatment decisions, and review dates. *It is where the operational work lives.*
- **The Risk Matrix** is the likelihood-against-impact scoring grid used to triage attention in a room. *It is how the work gets discussed.* Never confuse the visual discussion tool with the operational record of accountability.

Current version — Nov 1, 2026
Update history: continuityhub.org/risk-register-template-fields-owners-review-cadence/

LIVING CADENCE & INHERENT VS. RESIDUAL HONESTY

Inherent vs. Residual: The Register's Central Honesty (Post 667):
"*The gap between the two scores is a claim, and claims need evidence.*" Inherent risk is exposure before controls (the flood plain, unpatched estate, single supplier). Residual risk is what remains once controls you actually run are accounted for. Registers go dishonest in the residual column: controls that exist only on paper, tests assumed that never ran, vendors trusted whose evidence expired last year.
The Working Rule: *A control may move a residual score only if you can point to its last test.* Everything else is inherent risk wearing a costume — and the register's job is precisely to refuse the costume, politely, in writing, forever.

3. THE REVIEW CADENCE THAT KEEPS IT ALIVE

Registers die of neglect between annual reviews. The 3-tier living cadence maintains operational freshness and prevents static archiving:

Cadence Tier	Interval & Trigger	Operational Focus & Scope	Accountability & Deliverables
Tier 1: Full Register Review	**Annual (minimum)** • Aligned with Risk Assessment refresh	Exhaustive audit of every active row across all business lines. Re-score inherent vulnerabilities, verify control validity, and align with annual corporate strategy.	Risk Lead & Executive Risk Committee. Deliverable: Updated master register with published year-over-year diff.
Tier 2: Top-Tier Owner Review	**Quarterly** • Scheduled 90-day cycle	Intensive sprint dedicated to top-residual risks (highest scoring tier). Evaluates control drift, confirms ongoing test evidence, and reviews treatment progress.	Named Risk Owners individually. Deliverable: Quarterly control test verification sign-off and action date adjustments.
Tier 3: Event-Driven Updates	**Immediate (ad-hoc)** • Triggered whenever the world moves	Triggered immediately upon: (1) An incident; (2) A near-miss; (3) A new critical vendor onboarded; (4) A facility or site change; (5) A control failing its test.	Affected Risk Owner & Risk Manager. Deliverable: Immediate register row amendment, control re-scoring, or treatment plan revision.
Retire With Reason	**Continuous** • Part of all review tiers	Retire risks that no longer exist and state the rationale in writing. A register that only grows teaches its readers that it is a museum.	Named Risk Owner & Risk Lead. Deliverable: Documented retirement log with verifiable reason (process/asset decommissioned).
Version & Diff Tracking	**At each publication** • Formal change log	Version it, date it, and make changes visible — the diff between this year's register and last year's shows how the organization actually evolved.	Risk Governance Office. Deliverable: Published changelog detailing added risks, modified controls, score shifts, and retirements.

4. THE 5 COMMON FAILURE MODES PRUNING DIAGNOSTIC

Failure Mode	Symptom & Root Cause (Post 667)	Operational Consequence	The Field Remedy
1. The Noun Register	Rows naming abstract topics ("supply chain," "cyber," "weather") instead of specific failure events.	Untestable, unownable, and unscoreable. Nobody knows what controls apply or what success means.	Rewrite as cause-event-consequence triad. Ground in a specific trigger, asset, and business outcome.
2. The Ownerless Register	Risks assigned to broad departments, steering committees, or job roles ("IT Department," "Safety Team").	Diffusion of responsibility: assigned to a committee means assigned to no one. No funding authority.	Enforce single named individual owner senior enough to allocate funding and authorize remediation.
3. The Static Register	Built for an annual audit, frozen until the next one. Reflects compliance theater, not operational reality.	Describes an organization that no longer exists; misses new vendor risks, system changes, and near-misses.	Institute quarterly top-tier reviews and mandatory event-driven triggers after incidents or changes.
4. The Padded Register	200 low-value rows no one reads, burying the 8 critical threats that genuinely threaten survival.	Destroys signal-to-noise ratio. Leadership tunes out the entire document as administrative bureaucracy.	Prune aggressively. Signal-to-noise sets register credibility. Pruning is an active risk decision.
5. The Orphan Register	Disconnected from operational plans, budgets, and the Business Impact Analysis (BIA) it should argue with.	Risks scored high that no plan treats and no budget funds are not being managed; they are merely documented.	Tie every high-residual risk to a BIA RTO/RPO target, a funded mitigation action, or an active plan.

Field Pruning Standard: When reviewing your register, run the **Signal-to-Noise Test**: If a risk does not have a testable cause-event-consequence statement, a named funder owner, verifiable control test dates, and an active review cadence, it is noise. Prune it, rewrite it, or retire it with reason.