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

WORKSHEET 1: THE ONE-ROW CONTRACT TEMPLATE & ARCHITECTURE

The One-Row Contract Law (Post 667): "*A register row is a small contract.*" The risk is stated as an event with a cause and a consequence — never a bare noun like "cyber." The owner is one named person senior enough to fund treatment. Controls are named concretely as running today. Residual risk is moved only with proof of last test. Treatment decisions are unambiguous (avoid, reduce, transfer, retain) with action, owner, and date.

WORKED EXEMPLAR CONTRACT ROW (POST 667 RANSOMWARE PEAK-SEASON)

Cause-Event-Consequence	Named Owner & Cat.	Inherent	Concrete Operating Controls	Residual	Treatment & Action	Review Dates
Cause: Edge VPN exploit / phishing **Event:** Ransomware encrypts file estate **Consequence:** Halts peak order processing	**Owner:** Sarah Lin (VP Tech Ops) **Cat:** Cyber / Core Operations	**L:** 4 **I:** 5 **Score:** 20	(1) Production micro-segmentation (2) Immutable offline backup regime (3) 24/7 Managed EDR & SOC triage	**L:** 2 **I:** 3 **Score:** 6	**Decision:** Reduce **Action:** Air-gap secondary rep **Owner:** D. Miller • **Due:** Dec 15	**Last:** 2026-10-15 **Next:** 2027-01-15 **Status:** Active

FILLABLE ONE-ROW CONTRACTS (ACTIVE WORKING REGISTER)

CONTRACT ROW 1 • RISK ID: RR-2026-_____

CAUSE-EVENT-CONSEQUENCE STATEMENT (NO BARE NOUNS)
Cause: _____ Event: _____
Consequence: _____

NAMED RISK OWNER (FUNDER SENIORITY)
Name: _____ Title: _____

CATEGORY / LINE
_____

INHERENT L × I
L: [ ] I: [ ] Sc: [ ]

CONCRETE CONTROLS OPERATING TODAY (SPECIFIC LAYERS)
1. _____ 2. _____ Last Test: _____

RESIDUAL L × I
L: [ ] I: [ ] Sc: [ ]

TREATMENT DECISION
[ ] Avoid [ ] Reduce [ ] Transfer [ ] Retain

ACTION ITEM • ACTION OWNER • TARGET DATE
Action: _____ Owner: _____ Target Date: _____

DATES & CADENCE STATUS
Last Review: _____ Next Review: _____ Status: [ ] Active [ ] Retired

CONTRACT ROW 2 • RISK ID: RR-2026-_____

CAUSE-EVENT-CONSEQUENCE STATEMENT (NO BARE NOUNS)
Cause: _____ Event: _____
Consequence: _____

NAMED RISK OWNER (FUNDER SENIORITY)
Name: _____ Title: _____

CATEGORY / LINE
_____

INHERENT L × I
L: [ ] I: [ ] Sc: [ ]

CONCRETE CONTROLS OPERATING TODAY (SPECIFIC LAYERS)
1. _____ 2. _____ Last Test: _____

RESIDUAL L × I
L: [ ] I: [ ] Sc: [ ]

TREATMENT DECISION
[ ] Avoid [ ] Reduce [ ] Transfer [ ] Retain

ACTION ITEM • ACTION OWNER • TARGET DATE
Action: _____ Owner: _____ Target Date: _____

DATES & CADENCE STATUS
Last Review: _____ Next Review: _____ Status: [ ] Active [ ] Retired

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

WORKSHEET 2: INHERENT VS. RESIDUAL HONESTY SHEET & EVIDENCE AUDIT

The Central Honesty Doctrine (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 on paper, tests assumed that never ran, vendors trusted whose evidence expired last year.
The Enforcement Mandate: "*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.*"

THE COSTUME-CONTROL TRAP LIST (AUDIT & DISQUALIFICATION GUIDE)

Costume Control Trap	Field Manifestation & How Registers Cheat	Required Documentary Proof	Reversion Rule
1. Policy on Paper	An information security or supplier governance policy exists on the intranet, but no compliance audit or enforcement log has ever run.	Dated audit report showing active operational enforcement (≤365 days).	Revert residual score to inherent. Disqualify control.
2. Untested Backup Regime	Daily backups run to cloud or tape, but full file estate recovery and bare-metal restoration has never been executed under load.	Dated restore test certificate with actual RTO/RPO achieved vs target.	Revert impact score to inherent catastrophic.
3. Expired Vendor Evidence	Critical cloud SaaS vendor is marked "secure" based on a SOC 2 Type II report or ISO certificate that expired 14 months ago.	Current SOC 2 / ISO cert (≤12 months old) plus bridge letter.	Revert supplier risk to unmitigated inherent.
4. Unmonitored Tooling	EDR or SIEM licenses purchased and software deployed, but alert notifications flow to an unmonitored mailbox with zero triage SLA.	Weekly SOC triage logs, alert response metrics, and escalation sign-offs.	Revert detection likelihood to raw inherent.
5. Phantom Segmentation	Network architecture diagrams show isolated production zones, but firewall audit reveals undocumented any-to-any bypass rules.	Automated firewall rule audit and penetration test proof (≤180 days).	Revert breach spread impact to inherent.

FILLABLE CONTROL TESTING EVIDENCE LOG (RESIDUAL VALIDITY CHECK)

Risk ID	Named Concrete Control	Last Test Date	Test Evidence / Log Ref	Tested By (Named)	Residual Status
RR-01	Offline Immutable Backups	2026-09-14 (Pass)	Restore-Report-Q3-Pass.pdf	Mark Vance (Lead Arch)	[✓] VALID CLAIM
_____	_____	_____	_____	_____	[ ] VALID [ ] REVERT
_____	_____	_____	_____	_____	[ ] VALID [ ] REVERT
_____	_____	_____	_____	_____	[ ] VALID [ ] REVERT
_____	_____	_____	_____	_____	[ ] VALID [ ] REVERT
_____	_____	_____	_____	_____	[ ] VALID [ ] REVERT

Auditor Reversion Protocol: If the *Last Test Date* is blank, older than the scheduled test cadence, or resulted in an uncorrected failure, cross out the residual score immediately. Enter the inherent score into the residual column in red ink and notify the named risk owner in writing within 24 hours.

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

WORKSHEET 3: REVIEW CADENCE PLANNER & EVENT-DRIVEN TRIGGER LOG

The Cadence Imperative (Post 667): "*Registers die of neglect between annual reviews.*" The rhythm that works: (1) Full register reviewed on the same cycle as the risk assessment refresh — annually at minimum; (2) The top tier — highest residual risks — reviewed quarterly by the people who own them; (3) Event-driven updates whenever the world moves.

THE 5 EVENT-DRIVEN REVIEW TRIGGERS (IMMEDIATE ACTION)

Event Trigger	Operational Trigger Definition (Post 667)	Mandatory Register Update Action	SLA Window
1. Incident Occurred	Any security breach, system outage, supply disruption, or physical incident impacting operations.	Audit inherent score validity; review failed controls; update event statement and residual score.	Within 5 business days of debrief
2. Near-Miss Reported	An event that came within defined tolerance limits of causing an operational failure or data loss.	Re-evaluate likelihood score upward; verify whether existing controls functioned by design or luck.	Within 10 business days of report
3. New Critical Vendor	Contracting or onboarding a vendor supporting core business functions or holding confidential data.	Create dedicated single-supplier contract row; verify evidence; assign named procurement owner.	Prior to production data access
4. Facility / Site Change	Relocation, expansion, closure, or physical restructuring of any operational facility or datacenter.	Re-score geographic hazards (flood, power, utility); inspect physical controls and site access.	30 days prior to site transition
5. Failed Control Test	Disaster recovery test fail, backup restore timeout, pen-test finding, or expired vendor attestation.	**Immediate reversion of residual score to inherent.** Issue urgent remediation action row.	Within 24 hours of test failure

CADENCE SCHEDULE & EVENT INTAKE LOG (FILLABLE TRACKER)

Cadence / Trigger	Date Triggered	Trigger Details / Target Risks	Named Lead	Action Completed	Sign-off
Annual Full Review	Target: 2026-11-15	All active rows • Risk assessment refresh	Risk Governance Lead	[ ] Scheduled	_____
Quarterly Top-Tier	Target: 2027-01-15	Top 8 residual risks • Control tests check	Named Risk Owners	[ ] Scheduled	_____
Event: Incident	_____	_____	_____	[ ] Done [ ] Open	_____
Event: Near-Miss	_____	_____	_____	[ ] Done [ ] Open	_____
Event: New Vendor	_____	_____	_____	[ ] Done [ ] Open	_____
Event: Failed Test	_____	_____	_____	[ ] Done [ ] Open	_____

Cadence Governance Rule: An annual review that does not produce a published diff against the prior year's register is presumed to be an unperformed administrative pass. All modifications, score shifts, and control test verifications must be documented in the Version Diff Tracker (Worksheet 4).

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

WORKSHEET 4: RETIRE-WITH-REASON LOG & YEAR-OVER-YEAR DIFF TRACKER

The Anti-Museum Doctrine (Post 667): *"Retire risks that no longer exist and say why; a register that only grows teaches its readers that it is a museum. Version it, date it, and make the changes visible — the diff between this year's register and last year's shows how the register changed."*

RETIRE-WITH-REASON LOG (MANDATORY DECOMMISSIONING JUSTIFICATION)

Risk ID	Original Event Statement	Date Retired	Documented Retirement Rationale (Why Risk Ceased to Exist)	Authorizing Owner
RR-042	On-premise Exchange server unpatched vulnerability exploited by external actor.	2026-06-30	**Asset Decommissioned:** Mail infrastructure migrated 100% to managed cloud with SSO & MFA. On-prem server wiped and retired from network.	Sarah Lin (VP Tech Ops) Sign: *S. Lin*
_____	_____	_____	_____	_____ Sign: _____
_____	_____	_____	_____	_____ Sign: _____
_____	_____	_____	_____	_____ Sign: _____
_____	_____	_____	_____	_____ Sign: _____

YEAR-OVER-YEAR DIFF LOG (VISIBLE CHANGE RECORD)

Change Type	Risk ID	Nature of Modification / Evidence Update	Previous → New Score	Approved By
[+] ADDED	RR-2026-14	New critical payment processor vendor onboarded; added API outage risk row.	Inherent: 4×4 (16) → Res: 2×3 (6)	C. Vance (CFO)
[-] RETIRED	RR-2026-08	Secondary warehouse lease terminated; consolidated inventory to primary facility.	Residual: 3×3 (9) → RETIRED	M. Stone (COO)
[Δ] RE-SCORED	RR-2026-03	Annual DR restore test failed (RTO exceeded 8h target); reverted control credit.	Residual: 2×2 (4) → Res: 4×4 (16)	S. Lin (VP Tech)
[ ] _____	_____	_____	_____	_____
[ ] _____	_____	_____	_____	_____

Audit Integrity Notice: Deleting a row without entering it into the Retire-With-Reason Log is an operational failure. An auditor, executive, or regulator must be able to trace every risk from inception to active mitigation or documented formal retirement.

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

WORKSHEET 5: 5 FAILURE MODES PRUNING CHECKLIST & SIGNAL-TO-NOISE SCORECARD

Signal-to-Noise Law (Post 667): "*Two hundred rows no one reads, burying the eight that matter; a register's credibility is set by its signal-to-noise, and pruning is a risk decision too.*" A bloated register is an unmanaged register. Use this worksheet to interrogate, prune, and re-anchor your operational register.

THE 5 FAILURE MODES PRUNING AUDIT CHECKLIST

Failure Mode	Diagnostic Audit Questions (Inspect Every Active Row)	Pruning Action Required	Pass / Fail
1. The Noun Register	Does any row name a bare topic like "cyber," "weather," "supply chain," or "regulatory"? Is the event missing an explicit cause or quantifiable consequence?	Rewrite as testable cause-event-consequence row or strike from register.	[ ] PASS [ ] FAIL (Rewritten)
2. The Ownerless Register	Is any risk assigned to a committee ("Safety Committee"), department ("IT"), or generic title? Does the named person lack budget authority to fund treatment?	Reassign to a single named funder-level executive with signing authority.	[ ] PASS [ ] FAIL (Reassigned)
3. The Static Register	Has any row gone unreviewed for >365 days? Have recent incidents, near-misses, vendor changes, or facility changes failed to produce register updates?	Trigger immediate event-driven update session or archive to historical log.	[ ] PASS [ ] FAIL (Updated)
4. The Padded Register	Does the register contain dozens of minor nuisance risks that dilute focus? Are the 8 enterprise-critical threats clearly visible to the executive committee?	Prune low-severity noise. Consolidate trivial operational items into SOPs.	[ ] PASS [ ] FAIL (Pruned)
5. The Orphan Register	Are high-residual risks disconnected from operational continuity plans, capital budgets, or the Business Impact Analysis (BIA) RTO/RPO targets?	Establish direct linkage to funded continuity plans or downgrade score.	[ ] PASS [ ] FAIL (Linked)

SIGNAL-TO-NOISE SCORECARD & EXECUTIVE PRUNING CHARTER

Register Health Metric	Target Healthy Standard	Your Register Actual	Operational Verdict
Total Active Risk Rows	**8 – 25 vital risks**	[ ] rows	[ ] Healthy [ ] Padded Bloat
Rows with Testable Events (No Nouns)	**100% compliant**	[ ] %	[ ] Testable [ ] Vague Topics
Single Named Funder-Level Owners	**100% individual officers**	[ ] %	[ ] Owned [ ] Committee Void
Controls Backed by Verified Last Test	**100% proven (≤365 days)**	[ ] %	[ ] Honest [ ] Costume Claims
Alignment with BIA Plans & Budgets	**100% of top-tier risks**	[ ] %	[ ] Managed [ ] Merely Documented

EXECUTIVE PRUNING CHARTER & SIGN-OFF

"We hereby certify that the active risk register has been audited against the 5 Failure Modes. All vague nouns have been eliminated, all controls without verified test dates have had their residual claims reverted to inherent exposure, and redundant padding has been pruned to preserve executive focus on critical enterprise risks."

Risk Governance Lead: _____ • **Signature:** _____ • **Date:** _____

Executive Sponsor: _____ • **Signature:** _____ • **Date:** _____