CONTINUITY HUB • QUICK CARD

5x5 Risk Scoring Methodology: Likelihood Bands, Matrix & Worst-Case Vector Rule

Current version — Oct 31, 2026
Update history: continuityhub.org/risk-assessment-threat-analysis...

THE GOVERNING PRINCIPLES: BIA-FIRST LINKAGE & THE WORST-CASE VECTOR RULE

1. BIA First, Threats Second (ISO 22301:2019 Clause 8.2): Never score threats in a vacuum. The Business Impact Analysis (BIA) defines what matters, Maximum Tolerable Periods of Disruption (MTPD), and Recovery Time Objectives (RTO). The risk assessment identifies threat likelihood and exposure against those prioritized activities.

2. The Worst-Case Vector Rule (ISO/IEC 31010): Impact across the 5 domains (Financial, Operational, Regulatory, Safety, Reputational) must *never* be averaged. A facility fire causing $2.5M loss and 2-week outage is not "diluted" because zero regulatory fines occurred. **The composite impact rating equals the single highest score among all evaluated domains.**

1. Likelihood Calibration (1–5 Scale)

PROBABILITY BANDS

Rating	Descriptor	Empirical Recurrence Interval	Annual Probability
1	**Rare**	Exceptional; > 20-year recurrence	< 5% per year
2	**Unlikely**	Occurs once every 10 to 20 years	5% – 10% per year
3	**Possible**	Occurs once every 3 to 10 years	10% – 30% per year
4	**Likely**	Occurs once every 1 to 3 years	30% – 70% per year
5	**Almost Certain**	Multiple times per operational year	> 70% per year

* Calibrated against historical records, regional hazard maps, insurance tables, and vendor loss reports.

2. The 5x5 Heat Matrix Grid

SCORE: L × I (1–25)

Likelihood (1 to 5)	Consequence / Impact (Worst-Case Domain 1 to 5)				
	1 Neg	2 Min	3 Mod	4 Maj	5 Cat
5 Almost Certain	5 Mod	10 High	15 Crit	20 Crit	25 Crit
4 Likely	4 Low	8 Mod	12 High	16 Crit	20 Crit
3 Possible	3 Low	6 Mod	9 Mod	12 High	15 Crit
2 Unlikely	2 Low	4 Low	6 Mod	8 Mod	10 High
1 Rare	1 Low	2 Low	3 Low	4 Low	5 Mod

1–4: Low (Accept)	5–9: Moderate (Monitor)	10–14: High (Mitigate)	15–25: Critical (Board Action)

3. Inherent vs. Residual Risk & Quantitative Modeling (ALE)

ISO 31000:2018

Inherent Risk (Gross): Likelihood × Impact (1–25) with zero safeguards in place.
Control Effectiveness (CE%): 0% to 100% verified efficacy of active preventative & detective controls.
Residual Risk (Net): Remaining operational risk after existing controls. The delta quantifies the protective value of continuity investments.

Quantitative ROI Formula: `ALE = SLE × ARO`

- **SLE (Single Loss Expectancy):** Asset Value (AV) × Exposure Factor (EF).
- **ARO (Annualized Rate of Occurrence):** Estimated event frequency per operational year.
- **Safeguard Net ROI:** `(ALE_inherent - ALE_residual) - Annual Safeguard Cost`.

4. Five-Domain Consequence Scoring Matrix (Page Calibration Baseline)

WORST-CASE VECTOR APPLIED

Rating Level	Financial Loss	Operational Outage vs. MTPD/RTO	Regulatory & Legal Exposure	Life Safety & Workforce	Reputational Impact
1 Negligible	< $25,000	< 2 hours; no impact on critical business activities or client deliverables.	No regulatory notification required; minor internal policy variance.	No injuries; minor ergonomics or temporary workstation discomfort.	Zero public awareness; isolated internal departmental grievance.
2 Minor	$25,000 – $100,000	2 to 8 hours; non-critical batch processing delayed; RTO targets maintained.	Informal supervisory inquiries; standard periodic compliance reporting notes.	Minor first-aid treatment on site; zero lost workday cases.	Localized client complaints resolved through routine customer service channels.
3 Moderate	$100,000 – $500,000	8 to 24 hours; critical business activities degraded; RTO challenged but within MTPD.	Formal regulatory notice required (e.g., state privacy breach notification, standard OSHA report).	Medical treatment beyond first aid; 1 to 5 lost workdays.	Regional media coverage; customer churn rate increases by 2% to 5%.
4 Major	$500,000 – $2,500,000	24 to 72 hours; critical activity failure exceeds RTO; approaches MTPD limit.	Applicable accelerated regulatory reporting obligations; material penalty exposure.	Severe physical injuries; hospitalizations; extensive facility evacuation.	National trade/business media; executive public testimony; brand sentiment drops.
5 Catastrophic	> $2,500,000	> 72 hours; full critical business outage exceeding MTPD; irreversible insolvency risk.	Formal consent decrees, criminal liability investigations, operating charter suspension.	Fatalities or permanent life-altering disabilities; massive public safety contamination.	International front-page coverage; systemic client abandonment; executive removal.

5. The Five Continuity Threat Categories & Key Architectural Checks

COMPREHENSIVE SCOPE

Category	Core Hazard Scenarios & Disruption Modes	Mandatory Continuity Controls & Verified Precedents
1. Natural Hazards	Seismic, tropical cyclones, tornadoes, riverine/flash floods, wildfires, heat domes, winter ice storms. Wide-area infrastructure loss.	**NOAA 28 Billion-Dollar Disasters (2023):** ISO 22301:2019/Amd 1:2024 climate action mandate; facility elevation, utility dual-feeds, regional dispersal.
2. Cyber Threats	Ransomware, extortion exfiltration, DDoS, identity infrastructure hijacking, software supply chain, insider data sabotage.	**Targeted Backups:** Enforce immutable write-once-read-many (WORM) storage, air-gapped forensic staging networks, and malware eradication gates before restore.
3. Technology Failures	Cloud AZ outages, telecom backbone cuts, DNS blackouts, substation failures, automated deployment kernel crashes.	**CrowdStrike Precedent (8.5M Systems Disabled):** Eliminate architectural Single Points of Failure (SPOFs), cross-system API dependencies, SaaS concentration.
4. Human & Org	Key-person dependency, executive incapacitation, labor walkouts, pandemic illness surges, civil unrest, change-management failures.	**Institutional Knowledge Silos:** Cross-trained deputies, documented step-by-step standard operating runbooks, succession authorizations.
5. Supply Chain	Critical supplier insolvency, single-source factory halts, maritime logistics bottlenecks, geopolitical embargoes.	**65%+ Disruption Prevalence ($184B Global Cost):** Audit critical suppliers' BCPs, multi-tier fabricator mapping, secondary certified sourcing contracts.

RAPID RISK SCORING PROTOCOL: 4-STEP PROCEDURE

Step 1: Identify threat event & cross-reference affected business activity to BIA MTPD.
Step 2: Score gross Likelihood (1–5) and evaluate all 5 Impact domains assuming 0 controls. *Set Consequence = max domain score.* Multiply to get Inherent Risk (1–25).
Step 3: Audit active controls. Score Control Effectiveness (0–100%) and determine net Residual Likelihood & Impact. *Multiply for Residual Score (1–25).*
Step 4: Compare Residual Score against Enterprise Risk Appetite: ≥10 requires formal Treatment Plan (Mitigate, Transfer, Avoid).