TEMPLATE

Risk Register Template & Best Practices

Complete risk register template with 20 example risks, 5×5 matrix, scoring methodology, risk appetite guidance, and treatment options.

Published by
Compliance Enablers LLP

Last Updated
March 2026

Pages
~13 pages

Introduction

A risk register is the cornerstone of any risk management program. It serves as a centralized repository for identifying, assessing, tracking, and treating risks across your organization. Whether you are implementing ISO 27001, SOC 2, NIST CSF, or any other framework, a well-maintained risk register is essential.

This guide provides a ready-to-use risk register template, 20 example risks across multiple categories, the 5x5 risk matrix methodology, treatment options, and best practices for ongoing risk management.

1. Risk Register Template

Column Definitions

Column	Description
Risk ID	Unique identifier (e.g., RISK-001). Use a consistent numbering scheme.
Risk Name	Short, descriptive name for the risk.
Category	Classification of the risk (Information Security, Operational, Compliance, Third-Party, Human, Technology).
Description	Detailed description of the risk scenario — what could happen and why.
Likelihood (1-5)	Probability of the risk materializing. See the Likelihood Scale below.
Impact (1-5)	Severity of consequences if the risk materializes. See the Impact Scale below.
Risk Score	Likelihood x Impact. Ranges from 1 to 25.
Risk Level	Derived from the risk score: Critical, High, Medium, or Low.
Risk Owner	The individual accountable for managing this risk.
Mitigation Strategy	The planned or implemented controls to reduce the risk.
Target Risk Score	The expected risk score after mitigation is fully implemented.
Status	Current state: Open, In Treatment, Accepted, Closed.
Last Reviewed	Date of the most recent review of this risk entry.

2. The 5x5 Risk Matrix

Likelihood Scale

Score	Level	Description
1	Rare	Unlikely to occur; no history of occurrence; less than 5% probability within 12 months
2	Unlikely	Could occur but not expected; limited history; 5-25% probability within 12 months
3	Possible	Might occur; has occurred before in similar organizations; 25-50% probability within 12 months
4	Likely	Will probably occur; has occurred in this organization; 50-80% probability within 12 months
5	Almost Certain	Expected to occur; occurs regularly; greater than 80% probability within 12 months

Impact Scale

Score	Level	Description
1	Negligible	Minimal operational disruption; no financial loss of note; no reputational harm
2	Minor	Short-term disruption (hours); minor financial loss (< $10K); limited internal awareness
3	Moderate	Noticeable disruption (days); moderate financial loss ($10K-$100K); some customer awareness
4	Major	Significant disruption (weeks); substantial financial loss ($100K-$1M); media attention; regulatory scrutiny

5	Severe	Extended disruption (months); critical financial loss (> $1M); significant reputational damage; regulatory penalties; potential business viability threat

Risk Score Matrix

	Impact 1	Impact 2	Impact 3	Impact 4	Impact 5
Likelihood 5	5 (Medium)	10 (High)	15 (High)	20 (Critical)	25 (Critical)
Likelihood 4	4 (Low)	8 (Medium)	12 (High)	16 (Critical)	20 (Critical)
Likelihood 3	3 (Low)	6 (Medium)	9 (Medium)	12 (High)	15 (High)
Likelihood 2	2 (Low)	4 (Low)	6 (Medium)	8 (Medium)	10 (High)
Likelihood 1	1 (Low)	2 (Low)	3 (Low)	4 (Low)	5 (Medium)

Risk Level Thresholds

Risk Score	Risk Level	Action Required
20-25	Critical	Immediate executive attention; mandatory treatment; escalate to board
12-19	High	Senior management attention; treatment plan required within 30 days
5-11	Medium	Management attention; treatment plan required within 90 days
1-4	Low	Monitor; accept with documented justification or treat opportunistically

3. Risk Appetite Guidance

Risk appetite defines how much risk the organization is willing to accept in pursuit of its objectives. It should be formally documented and approved by senior leadership.

Setting Risk Appetite

- **Strategic level**: Define overall appetite statements (e.g., "We have a low appetite for risks that could result in regulatory penalties" or "We have a moderate appetite for risks associated with innovation and new market entry").
- **Operational level**: Define acceptance thresholds (e.g., "Risks scoring 8 or below may be accepted with risk owner approval" or "Risks scoring above 15 require board-level acceptance").
- **Category-specific**: Different categories may have different appetites. You may accept higher operational risk than compliance risk.

Risk Appetite Statement Template

"[Organization Name] has a [low/moderate/high] appetite for [risk category] risks. Risks in this category with an inherent score above [threshold] require formal treatment. Residual risks above [threshold] require approval by [authority level]."

4. Risk Treatment Options

Accept

Formally acknowledge the risk without implementing additional controls. Appropriate when:

- The risk score is within the organization's risk appetite.
- The cost of mitigation exceeds the potential impact.
- The risk cannot be practically reduced further.

Requirements: Document the acceptance decision, the rationale, and obtain sign-off from the appropriate authority.

Mitigate

Implement controls to reduce the likelihood, impact, or both. This is the most common treatment option. Examples:

- Deploying multi-factor authentication to reduce unauthorized access likelihood.
- Implementing automated backups to reduce data loss impact.

- Conducting security awareness training to reduce phishing success likelihood.

Transfer

Shift the risk (or a portion of it) to a third party. Examples:

- Purchasing cyber insurance to transfer financial impact of breaches.
- Outsourcing data center operations to a provider with superior physical security.
- Using a managed security operations center (SOC) to transfer detection and response responsibilities.

Note: You can transfer the financial impact of a risk, but you cannot transfer accountability. The risk owner remains responsible.

Avoid

Eliminate the risk by removing the activity, process, or technology that creates it. Examples:

- Discontinuing a legacy application that cannot be adequately secured.
- Not entering a market with prohibitive regulatory requirements.
- Removing functionality that processes sensitive data unnecessarily.

5. Example Risk Register (20 Risks)

Information Security Risks

Risk ID	Risk Name	Category	Description	L	I	Score	Level	Mitigation Strategy
RISK-001	Ransomware Attack	Information Security	Ransomware encrypts critical systems, causing operational disruption and potential data loss	4	5	20	Critical	Endpoint detection and response (EDR), immutable backups, network segmentation, incident response plan, regular backup testing
RISK-002	Phishing-Based Credential Theft	Information Security	Employees deceived by phishing emails, leading to credential compromise and unauthorized access	4	4	16	Critical	Security awareness training, phishing simulations, MFA on all systems, email filtering, DMARC/SPF/DKIM
RISK-003	Data Breach via Misconfigured Cloud Storage	Information Security	Publicly accessible cloud storage buckets expose sensitive customer or corporate data	3	5	15	High	Cloud security posture management (CSPM), automated misconfiguration detection, access reviews, encryption at rest
RISK-004	Insider Data Exfiltration	Information Security	Malicious or negligent insider copies or transmits sensitive data outside the organization	3	4	12	High	Data loss prevention (DLP), least privilege access, user activity monitoring, offboarding procedures, NDAs

Operational Risks

Risk ID	Risk Name	Category	Description	L	I	Score	Level	Mitigation Strategy
RISK-005	Critical System Downtime	Operational	Core business systems become unavailable due to hardware failure, software bug, or infrastructure issue	3	4	12	High	Redundant architecture, failover mechanisms, SLA-backed hosting, disaster recovery plan, RTO/RPO targets defined and tested
RISK-006	Loss of Key Personnel	Operational	Departure of critical staff results in knowledge loss and operational disruption	3	3	9	Medium	Cross-training, documentation of key processes, succession planning, knowledge management systems
RISK-007	Business Continuity Failure	Operational	Organization unable to maintain operations during a disruptive event (natural disaster, pandemic, cyber incident)	2	5	10	High	Business continuity plan, annual BCP testing, alternate work locations, communication plan, recovery procedures

RISK-008	Change Management Failure	Operational	Uncontrolled changes to systems or processes cause outages, security gaps, or data integrity issues	3	3	9	Medium	Formal change management process, change advisory board, testing requirements, rollback procedures

Compliance Risks

Risk ID	Risk Name	Category	Description	L	I	Score	Level	Mitigation Strategy
RISK-009	GDPR Non-Compliance	Compliance	Failure to meet GDPR requirements results in regulatory fines (up to 4% of global revenue) and reputational damage	3	5	15	High	Data protection officer appointed, DPIA process, consent management, data subject rights procedures, privacy impact assessments
RISK-010	Regulatory Change Undetected	Compliance	New or updated regulatory requirements are missed, leading to non-compliance	3	4	12	High	Regulatory monitoring service, compliance calendar, quarterly compliance reviews, legal counsel engagement
RISK-011	Audit Finding Recurrence	Compliance	Corrective actions from previous audits are ineffective, resulting in repeat findings	2	3	6	Medium	Root cause analysis requirements, corrective action tracking, effectiveness verification, management review of findings

Third-Party Risks

Risk ID	Risk Name	Category	Description	L	I	Score	Level	Mitigation Strategy
RISK-012	Third-Party Data Breach	Third-Party	A vendor or supplier suffers a breach that exposes the organization's data	3	4	12	High	Vendor risk assessments, security questionnaires, contractual security requirements, ongoing monitoring, incident notification clauses
RISK-013	Vendor Lock-In	Third-Party	Over-reliance on a single vendor creates dependency and limits flexibility	3	3	9	Medium	Multi-vendor strategy where feasible, data portability requirements, exit clauses in contracts, regular market assessment
RISK-014	Supply Chain Compromise	Third-Party	Compromised software supply chain introduces malware or vulnerabilities into the organization's environment	2	5	10	High	Software composition analysis, vendor security assessments, code signing verification, dependency monitoring

Human Risks

Risk ID	Risk Name	Category	Description	L	I	Score	Level	Mitigation Strategy
RISK-015	Social Engineering Attack	Human	Employees manipulated through pretexting, vishing, or in-person social engineering into divulging information or granting access	4	3	12	High	Security awareness training, social engineering simulations, verification procedures for sensitive requests, clean desk policy
RISK-016	Inadequate Security Awareness	Human	Employees lack sufficient security knowledge, leading to poor security behaviors	3	3	9	Medium	Mandatory security awareness program, role-based training, regular phishing simulations, security culture assessments

RISK-017	Accidental Data Disclosure	Human	Employee inadvertently sends sensitive data to the wrong recipient or publishes it in an insecure location	4	3	12	High	DLP controls, email encryption, classification labels, training on data handling, technical controls to prevent misdirected emails

Technology Risks

Risk ID	Risk Name	Category	Description	L	I	Score	Level	Mitigation Strategy
RISK-018	Unpatched Vulnerabilities	Technology	Known vulnerabilities remain unpatched, providing exploitable attack vectors	4	4	16	Critical	Vulnerability management program, patch management policy (critical patches within 14 days), automated scanning, risk-based prioritization
RISK-019	Legacy System Exploitation	Technology	End-of-life systems no longer receive security updates, creating permanent vulnerabilities	3	4	12	High	Legacy system inventory, migration roadmap, compensating controls (network isolation, enhanced monitoring), risk acceptance where migration is pending
RISK-020	API Security Weakness	Technology	Insecure APIs expose data or functionality to unauthorized parties	3	4	12	High	API security testing, authentication and authorization controls, rate limiting, input validation, API gateway, regular penetration testing

6. Best Practices for Maintaining a Risk Register

Governance

1. **Assign clear ownership**: Every risk must have a named risk owner who is accountable for monitoring and treating that risk. Risk owners should be at a management level with authority to allocate resources.
2. **Define review cadences**: Establish regular review cycles — quarterly at minimum for all risks, monthly for Critical and High risks. Document review dates in the register.
3. **Integrate with management review**: Present the risk register summary at management review meetings. Highlight new risks, escalated risks, overdue treatments, and changes in the risk landscape.

Process

4. **Keep it current**: The risk register is a living document. Update it whenever a new risk is identified, a risk materializes, controls change, or the business context shifts. Stale risk registers are worse than useless — they create a false sense of security.
5. **Link risks to controls**: Map each risk to the specific controls that mitigate it. This creates traceability and helps identify control gaps or redundancies.
6. **Track risk trends**: Monitor how risk scores change over time. Are your treatments reducing risk as expected? Are certain categories trending upward? Use trend data to inform strategy.
7. **Document risk acceptance formally**: When a risk is accepted, require written approval from the appropriate authority level based on the risk score. Maintain an acceptance log for audit purposes.

Quality

8. **Write meaningful descriptions**: A risk description should clearly articulate the threat, vulnerability, and potential impact. Avoid vague entries like "cybersecurity risk" — be specific.
9. **Validate scores consistently**: Use calibration sessions where risk owners collectively assess risks to ensure consistent application of the likelihood and impact scales. One person's "Likely" should not be another's "Possible."
10. **Separate inherent and residual risk**: Record both the inherent risk score (before controls) and the residual risk score (after controls). This demonstrates the value of your controls and highlights where further treatment may be needed.
11. **Include emerging risks**: Do not limit your register to known, established risks. Actively scan for emerging

threats — AI-powered attacks, new regulatory requirements, geopolitical changes, supply chain disruptions — and add them proactively.

12. **Audit the register itself**: Periodically audit the quality of your risk register. Are descriptions adequate? Are scores justified? Are treatments progressing? Are reviews happening on schedule?

Integration

13. **Connect to incident management**: When a risk materializes (an incident occurs), update the risk register. Adjust likelihood scores based on actual occurrence data. Feed lessons learned back into the risk assessment.
14. **Align with compliance frameworks**: If you are certified or seeking certification (ISO 27001, SOC 2, NIST, etc.), ensure your risk register maps to the relevant framework requirements. This avoids duplicate effort and demonstrates compliance.
15. **Use tooling**: Spreadsheets work for small organizations, but they quickly become unmanageable. Purpose-built GRC platforms provide automated scoring, dashboards, notifications, audit trails, and integration with other compliance activities.

7. Reporting on Risk

Executive Dashboard Metrics

- Total number of risks by level (Critical, High, Medium, Low).
- Risk trend over time (are total risks increasing or decreasing?).
- Treatment progress (percentage of risks with completed treatments).
- Overdue treatments (treatments past their target completion date).
- Top 10 risks by score.
- New risks identified since last report.
- Risks accepted vs. treated vs. transferred vs. avoided.

Board-Level Reporting

Keep board reporting concise and focused on:

- Material changes to the risk profile.
- Critical and High risks requiring executive attention or resources.
- Key risk indicators (KRIs) trending in the wrong direction.
- Risk appetite breaches.
- Significant incidents and their link to identified risks.

Conclusion

A well-maintained risk register transforms risk management from a theoretical exercise into a practical, actionable discipline. It provides visibility into your organization's risk landscape, enables informed decision-making, and demonstrates to auditors, regulators, and clients that you take risk seriously.

Start with the template and examples in this guide, customize them to your organization's context, and commit to treating the register as a living, breathing document. The investment in maintaining it properly pays dividends in avoided incidents, faster compliance, and greater organizational resilience.

Ready to Transform Your Compliance Program?

27 modules • 261+ frameworks • 157 templates • 40+ integrations • AI-powered • From $999/yr

Schedule a Demo

Start Free Trial