THE COMPLETE

# Risk Register GUIDE

BEMI TECH SOLUTIONS

From Risk Identification to Governance & Compliance

**Risk Identification**
Threats, Vulnerabilities, STRIDE

**Risk Assessment**
Likelihood × Impact, Scoring

**Risk Matrix**
5×5 Grid, Heat Maps, Zones

**Risk Response**
Accept, Avoid, Transfer, Mitigate

**Risk Governance**
Ownership, RACI, 3 Lines of Defense

**Risk Monitoring**
KRIs, Review Cycles, Escalation

**Compliance Frameworks**
ISO 31000, NIST RMF, COSO ERM

**Risk Register Build**
Fields, Tools, Templates

**GRC Platforms**
ServiceNow, Archer, Vanta, Drata

**Risk Careers**
CRISC, CISM, vCISO Pathways

| 10 | 50+ | 6 | $4.45M |
|---|---|---|---|
| Chapters | Pages | Frameworks | Avg Breach Cost |


**Ransford Slater**

Cybersecurity Educator | Bemi Tech Solutions | 2026 Edition

## TABLE OF CONTENTS

# 01 Introduction to Risk Management

Risk Types | Lifecycle | Why Risk Registers Matter | Terminology

Risk is the potential for loss or harm arising from the interaction between a threat and a vulnerability. Every organization — from a solo startup to a Fortune 500 — faces risk every day. The question is not whether you have risk, but whether you have a structured, repeatable way to identify, assess, and manage it before it becomes an incident.

| $4.45M | 277 | 83% | 3.5M |
|---|---|---|---|
| Avg. Breach Cost 2023 | Days to Identify Breach | Orgs Hit Multiple Times | Unfilled Cyber Jobs |

## WHAT IS RISK?

A risk is NOT the same as a threat or an issue. Understanding these three concepts is the foundation of any risk management practice. Confusing them leads to mis-prioritized controls, wasted budget, and security gaps that attackers exploit.

### Threat

Any circumstance or event with the potential to adversely impact assets. Example: ransomware group targeting healthcare organizations.

### Vulnerability

A weakness that can be exploited by a threat. Example: unpatched server running outdated OS. Threat × Vulnerability = Risk.

### Risk

The potential that a threat will exploit a vulnerability and cause harm. Measured by Likelihood × Impact. Risks are managed, not eliminated.

### Issue

A risk that has already materialized. An active incident. Issues are resolved, not just monitored. Tracking issues separately keeps the risk register clean.

## TYPES OF ORGANIZATIONAL RISK

Risk comes in many forms. A comprehensive risk register addresses all risk categories — not just technical or cyber risks. Organizations that only track IT risk leave significant exposure unmanaged.

| Strategic | Operational | Financial | Compliance |
|---|---|---|---|
| Market shifts, competition, M&A failures | Process failures, people, systems, events | Fraud, credit, liquidity, FX exposure | Regulatory breaches, GDPR, PCI DSS, HIPAA |

| Reputational | Cyber | Legal | Third-Party |
|---|---|---|---|
| Brand damage, PR crises, social media | Breaches, ransomware, phishing, DDoS | Contracts, IP disputes, employment law | Vendor failures, supply chain compromise |

## THE RISK MANAGEMENT LIFECYCLE

Risk management is a continuous cycle, not a one-time audit. Organizations that treat it as an annual checkbox exercise fail to detect emerging threats and lose the confidence of regulators, customers, and boards. The lifecycle has five core stages:


1. Identify — systematically find and document all potential risks using workshops, interviews, threat intelligence, and historical incident data.
2. Assess — evaluate each risk for likelihood of occurrence and impact if it materializes. Calculate a risk score to enable prioritization.
3. Respond — select and implement an appropriate treatment: accept, avoid, transfer, or mitigate. Document the chosen strategy and rationale.
4. Monitor — track risk indicators continuously, review control effectiveness, and watch for new risks emerging from changes in the environment.
5. Review — conduct formal periodic reviews (quarterly minimum), report to governance, update the register, and capture lessons learned.

## KEY RISK TERMINOLOGY

### ESSENTIAL RISK MANAGEMENT TERMS

- Inherent Risk — risk level BEFORE any controls are applied. The raw, untreated exposure.
- Residual Risk — risk level AFTER controls are applied. What remains even with mitigations in place.
- Risk Appetite — the amount and type of risk an organization is willing to accept in pursuit of objectives.
- Risk Tolerance — the acceptable variation around the risk appetite threshold (the operational boundary).
- Control — any safeguard or countermeasure that reduces the likelihood or impact of a risk event.
- Risk Owner — the individual accountable for managing a specific risk and ensuring treatment is effective.
- Key Risk Indicator (KRI) — a metric that signals when a risk is increasing to an unacceptable level.
- Risk Register — a structured document/tool that records identified risks, assessments, and treatments.

## WHY RISK REGISTERS MATTER

A risk register is the single source of truth for your organization's risk posture. Without one, risks are managed informally, inconsistently, and invisibly — creating blind spots that regulators, auditors, and attackers will find before you do.

### BUSINESS VALUE OF A RISK REGISTER

- Regulatory compliance — ISO 27001, SOC 2, GDPR, HIPAA, and PCI DSS all require formal risk assessment
- Board-level reporting — gives leadership a quantified, prioritized view of organizational exposure
- Budget justification — evidence-based security investment decisions replace gut-feel spending
- Audit readiness — auditors expect to see a maintained, reviewed register with historical entries
- Incident response — pre-mapped risks accelerate response when an incident occurs
- Insurance premiums — well-documented risk management can lower cyber insurance costs

## RISK MANAGEMENT IN DIFFERENT ORGANIZATION SIZES

### Small Organizations (<100 staff)

Start with a simple spreadsheet. Focus on top 10 risks. One risk owner per risk. Quarterly review. ISO 27001 Annex A as your risk checklist.

### Mid-Market (100–1,000 staff)

Structured methodology, tiered vendor program, dedicated risk function. Consider a GRC platform. Report to leadership monthly.

### Enterprise (1,000+ staff)

Full ERM program, multiple frameworks, board-level risk committee, quantitative analysis (FAIR), integrated GRC platform, continuous monitoring.

### Regulated Industries

Financial services, healthcare, and critical infrastructure face mandatory requirements (DORA, HIPAA, NERC CIP) with prescribed risk assessment processes and audit evidence requirements.

## CONNECTING RISK MANAGEMENT TO BUSINESS STRATEGY

The most mature risk programs tie directly to strategic planning. Every major strategic initiative — a new product launch, a market entry, an acquisition — should trigger a formal risk assessment BEFORE commitment of resources. This positions risk management as a strategic enabler rather than a compliance burden.

### STRATEGIC RISK INTEGRATION POINTS

- Annual strategic planning — risk assessment of proposed objectives; risk-informed resource allocation
- New product/service launch — pre-launch risk assessment covering regulatory, reputational, and operational risks
- M&A due diligence — target company's risk register and security posture assessed before close
- New market entry — jurisdictional risk, regulatory compliance, and third-party landscape assessed upfront
- Technology adoption — cloud migration, AI integration, and new SaaS tools assessed before deployment

# 02 Risk Identification

Threat vs Vulnerability | STRIDE | Identification Methods | Categories

You cannot manage a risk you haven't identified. Risk identification is the most critical — and most commonly rushed — phase of risk management. A systematic, structured approach ensures coverage across all risk categories, not just the obvious technical threats that come to mind first.

## THREAT VS VULNERABILITY VS EXPOSURE

These three terms are frequently conflated. Getting them right ensures your risk register entries are accurate, actionable, and consistently understood across teams.

### Threat

A potential danger to an asset. Threats are external to the asset — e.g., an attacker, a natural disaster, a disgruntled employee, a ransomware group.

### Vulnerability

A weakness in the asset that makes it susceptible to a threat. Examples: missing patch, weak password policy, unencrypted storage, misconfigured firewall.

### Exposure

The degree to which an asset is subject to harm from a threat. An internet-facing server has higher exposure than an air-gapped system even with the same vulnerabilities.

### Risk = T × V × E

Risk is the intersection of Threat, Vulnerability, and Exposure. Reducing any one of the three reduces overall risk — even if you can't eliminate the threat itself.

## RISK IDENTIFICATION METHODS

No single method captures all risks. Best-in-class organizations combine multiple techniques to achieve comprehensive coverage. Document the method used for each risk entry in your register — it helps future reviewers understand how the risk was surfaced.

### IDENTIFICATION TECHNIQUES

- Workshops & Brainstorming — cross-functional sessions with business, IT, legal, and operations teams
- Risk Checklists — pre-built industry checklists (ISO 27001 Annex A, CIS Controls, NIST SP 800-30)
- Interview Techniques — structured interviews with process owners, system admins, and department leads
- Historical Incident Analysis — past incidents and near-misses are the highest-signal source of future risks
- Threat Intelligence — commercial feeds, OSINT, MITRE ATT&CK, US-CERT, sector-specific ISACs
- Process Mapping — review business process flows to identify where failures or attacks could cause harm
- Vulnerability Scanning — automated tools that surface technical weaknesses to feed the risk register
- Red Team Exercises — adversarial testing reveals risks that checklists and interviews miss

## THE STRIDE THREAT MODEL

STRIDE is a threat classification framework developed by Microsoft. It categorizes threats into six types and maps them to security properties. Use STRIDE during design-phase risk identification for applications and systems to ensure you consider every attack angle.

### STRIDE CATEGORIES

- S — Spoofing: attacker impersonates another user or system. Violates Authentication.
- T — Tampering: attacker modifies data in transit or at rest. Violates Integrity.
- R — Repudiation: attacker denies performing an action. Violates Non-Repudiation.
- I — Information Disclosure: attacker accesses unauthorized data. Violates Confidentiality.
- D — Denial of Service: attacker disrupts availability. Violates Availability.
- E — Elevation of Privilege: attacker gains unauthorized permissions. Violates Authorization.

## COMMON RISK CATEGORIES FOR IT/CYBER RISK REGISTERS

A well-structured risk register organizes risks into categories. This enables filtering, reporting by domain, and assignment to the right subject-matter experts for assessment. The following categories cover the most common entries in a cyber risk register:

### Access & Identity

Unauthorized access, privileged account misuse, weak authentication, over-permissioned accounts, orphaned accounts.

### Data & Privacy

Data breaches, PII exposure, data residency violations, unencrypted backups, insider data theft, GDPR non-compliance.

### Infrastructure

Unpatched systems, misconfigured cloud, end-of-life hardware/software, insecure network architecture, DNS hijacking.

### Application

OWASP Top 10 vulnerabilities, insecure APIs, injection flaws, broken access controls, insecure SDLC practices.

### Third-Party / Supply Chain

Vendor breaches, insecure SaaS integrations, shared credentials, unvetted open-source dependencies.

### People & Process

Phishing susceptibility, shadow IT, policy non-compliance, inadequate security training, insider threats.

## DOCUMENTATION STANDARDS FOR RISK ENTRIES

Every risk entered into the register should meet a minimum documentation standard. Vague entries like 'hacking' or 'data loss' are not actionable. A well-documented risk entry enables accurate assessment, clear ownership, and effective treatment.

### MINIMUM FIELDS FOR A RISK ENTRY

- Risk ID — unique identifier (e.g., R-001) for tracking and cross-referencing
- Risk Title — concise, descriptive name (e.g., 'Unauthorized access to production database')
- Risk Description — detailed explanation of what could happen, to what asset, and how
- Threat Source — the actor or event driving the risk (e.g., external attacker, insider, system failure)
- Vulnerability — the specific weakness that makes the risk possible
- Potential Impact — what happens if the risk materializes (financial, operational, reputational, legal)
- Date Identified — when the risk was first logged; important for trend analysis and audit trails

## ASSET INVENTORY — THE FOUNDATION OF RISK IDENTIFICATION

You cannot assess risk to assets you haven't catalogued. An asset inventory is the prerequisite for a meaningful risk register. Without knowing what you have, where it is, and how critical it is, risk identification is incomplete and risk scoring is unreliable.

### Information Assets

Customer PII, financial records, intellectual property, contracts, strategic plans, credentials, encryption keys. Highest regulatory exposure.

### Technology Assets

Servers, workstations, cloud instances, network devices, SaaS applications, APIs, databases, IoT devices. Map data flows between them.

### ASSET INVENTORY BEST PRACTICES

- Classify by sensitivity: Public / Internal / Confidential / Restricted — drives risk scoring and control requirements
- Assign an asset owner for each entry — ownership drives accountability for risk management
- Link assets to business processes — enables impact assessment when an asset is compromised
- Review quarterly — cloud environments change rapidly; shadow IT appears constantly
- Include data flows — map where sensitive data travels between assets; breach paths follow data flows
- Use CMDB or asset management tooling for large estates — manual spreadsheets fail at scale

# 03 Risk Assessment & Scoring

Qualitative | Quantitative | FAIR Model | ALE & SLE | Scoring Scales

Risk assessment translates identified risks into a format that enables prioritization and resource allocation. Without a consistent scoring methodology, every risk feels equally urgent — or equally unimportant. Assessment gives the risk register its analytical power.

## QUALITATIVE VS QUANTITATIVE ASSESSMENT

**Qualitative**

Uses descriptive scales (Low/Medium/High/Critical) or numeric proxies (1–5). Fast, accessible, widely used. Best for initial assessment and non-financial risks.

**Quantitative**

Assigns financial values (ALE, SLE, ARO). More accurate but data-intensive. Required for insurance, board reporting, and ROI justification of security investments.

## THE LIKELIHOOD × IMPACT FORMULA

The most widely used risk scoring formula multiplies two independent dimensions: how likely is this risk to occur, and how severe would the impact be if it does? Both dimensions are rated on a 1–5 scale. The resulting score (1–25) maps to a risk level.

| 1–3 | 4–8 | 9–15 | 16–25 |
|---|---|---|---|
| Low Risk | Medium Risk | High Risk | Critical Risk |

### LIKELIHOOD SCALE (1–5)

- 1 — Rare: May occur only in exceptional circumstances. Less than once every 5 years.
- 2 — Unlikely: Could occur at some time. Once every 2–5 years.
- 3 — Possible: Might occur at some time. Once per year.
- 4 — Likely: Will probably occur in most circumstances. Multiple times per year.
- 5 — Almost Certain: Expected to occur in most circumstances. Weekly or monthly.

### IMPACT SCALE (1–5)

- 1 — Negligible: Minimal disruption, no financial loss, quickly remediated.
- 2 — Minor: Limited impact on operations, small financial loss, manageable without escalation.
- 3 — Moderate: Significant disruption, moderate financial loss, requires management attention.
- 4 — Major: Serious impact, significant financial loss, regulatory notification may be required.
- 5 — Critical: Catastrophic impact, severe financial/reputational damage, potential business failure.

## QUANTITATIVE RISK ASSESSMENT

Quantitative methods calculate financial exposure in dollar terms, enabling direct comparison between risk treatment costs and potential losses. The three core formulas are SLE, ARO, and ALE — used together they give a complete financial picture of any risk.

### SLE — Single Loss Expectancy

SLE = Asset Value × Exposure Factor. The expected financial loss from a single risk event. E.g., $500K server × 40% damage = $200K SLE.

### ARO — Annual Rate of Occurrence

How many times per year the risk event is expected to occur. E.g., 0.5 = once every 2 years. Based on historical data or threat intelligence.

### ALE — Annual Loss Expectancy

ALE = SLE × ARO. The expected yearly financial loss from a risk. E.g., $200K SLE × 0.5 ARO = $100K ALE. Use to justify security spend.

### Control Cost Justification

A security control is financially justified when its annual cost < ALE reduction it provides. E.g., $20K firewall justified if it reduces $100K ALE by 30%+.

## THE FAIR MODEL

Factor Analysis of Information Risk (FAIR) is the international standard for quantitative cyber risk analysis. It provides a formal ontology for understanding and measuring information risk in financial terms. FAIR underpins many enterprise GRC platforms.

### FAIR KEY COMPONENTS

- Risk = Probable Frequency of Loss Events × Probable Magnitude of Loss
- Threat Event Frequency (TEF) — how often a threat agent acts against an asset
- Vulnerability (Vuln) — probability that a threat event results in a loss event
- Loss Event Frequency (LEF) = TEF × Vulnerability
- Loss Magnitude — the financial impact when a loss event occurs (Primary + Secondary loss)
- Primary Loss — direct costs: response, recovery, breach notification, fines
- Secondary Loss — indirect costs: reputation damage, customer churn, partner trust erosion

## PRIORITIZING YOUR RISK REGISTER

Not all risks can be treated simultaneously. A prioritization framework ensures your team focuses resources on the highest-value threats first. Use a combination of risk score, asset criticality, and strategic impact to sequence your treatment backlog.

### PRIORITIZATION CRITERIA

- Risk Score — highest Likelihood × Impact scores treated first (quantitative threshold)
- Asset Criticality — risks to crown jewel assets (production DB, customer PII, financial systems) prioritized
- Regulatory Obligation — compliance-driven risks (GDPR, PCI DSS) have non-negotiable deadlines
- Proximity — risks with short detection-to-exploitation windows prioritized over slow-burn risks
- Treatment Cost vs Risk Reduction — quick wins (low-cost, high-reduction) prioritized in backlog
- Business Continuity Impact — risks that could halt core revenue-generating operations escalated to critical

## WORKED EXAMPLE — SCORING A REAL RISK

Let's walk through scoring a real-world risk end-to-end using both qualitative and quantitative methods. The risk: ransomware attack on the organization's file server containing customer contracts and financial records.

### STEP 1 — QUALITATIVE SCORING

- Threat: Ransomware group targeting professional services firms via phishing (confirmed OSINT)
- Vulnerability: 23% of staff failed last phishing simulation; backups not tested in 6 months
- Likelihood: 4 — Likely (multiple industry peers hit this year; phishing vectors active)
- Impact: 5 — Critical (customer contracts, financial records, regulatory notification required)
- Inherent Risk Score: 4 × 5 = 20 — CRITICAL
- Controls in place: EDR on all endpoints, email filtering, regular patching, quarterly backups
- Control effectiveness: Moderate — reduces likelihood from 4 to 2 and impact from 5 to 4
- Residual Risk Score: 2 × 4 = 8 — MEDIUM (within appetite after controls)

### STEP 2 — QUANTITATIVE SCORING (ALE)

- Asset Value (AV): file server + contained data = $2.4M (replacement + data reconstruction + regulatory fines)
- Exposure Factor (EF): 60% — estimated loss of asset value in a successful ransomware event
- SLE = AV × EF = $2.4M × 60% = $1.44M Single Loss Expectancy
- ARO: 0.25 (once every 4 years for organizations of this size with these controls)
- ALE = SLE × ARO = $1.44M × 0.25 = $360,000 Annual Loss Expectancy
- Treatment cost: $45K/year for immutable backup solution + phishing training enhancement
- Control ROI: reduces ARO from 0.25 to 0.05 ’ new ALE = $1.44M × 0.05 = $72K ’ saves $288K/year
- ROI justification: $45K control cost eliminates $288K annual risk exposure = 640% ROI

# 04 The Risk Matrix

5×5 Grid | Color Zones | Heat Maps | Risk Appetite | Plotting Risks

The risk matrix is the most universally recognized tool in risk management. It provides a visual representation of the entire risk landscape on a single page, enabling instant communication of risk posture to stakeholders at all levels — from developers to board members.

## THE 5×5 RISK MATRIX

The standard risk matrix plots Likelihood (x-axis, 1–5) against Impact (y-axis, 1–5). Each cell represents a risk score. Color coding translates scores into action levels. The matrix is read from top-right (critical) to bottom-left (low).

| IMPACT | 1 Rare | 2 Unlikely | 3 Possible | 4 Likely | 5 Almost Certain |
|---|---|---|---|---|---|
| 5 Critical | 5 | 10 | 15 | 20 | 25 |
| 4 Major | 4 | 8 | 12 | 16 | 20 |
| 3 Moderate | 3 | 6 | 9 | 12 | 15 |
| 2 Minor | 2 | 4 | 6 | 8 | 10 |
| 1 Negligible | 1 | 2 | 3 | 4 | 5 |

!• LIKELIHOOD !’

### Ø=ßâ Low (1–3)

Accept or monitor. Document in register. Review annually. No immediate action required unless clustering of low risks detected.

### Ø=ßá Medium (4–8)

Treat within 90 days. Assign owner. Document treatment plan. Review quarterly. Escalate if treatment is delayed.

### Ø=ßà High (9–15)

Treat within 30 days. Requires management sign-off. Weekly progress tracking. Board notification if treatment is blocked.

### Ø=Ý4 Critical (16–25)

Immediate action. Executive escalation. Daily tracking. Consider emergency controls. Board and regulator notification may be required.

## RISK APPETITE AND RISK TOLERANCE

The risk matrix must be calibrated against your organization's risk appetite — the level of risk the board is willing to accept. Without a defined appetite, 'high' and 'critical' are subjective. A well-defined appetite turns the matrix into a governance tool, not just a visualization.

### Risk Appetite

The total amount and type of risk an organization is prepared to take in pursuit of its strategic objectives. Set by the board. Reviewed annually.

### Risk Tolerance

The acceptable deviation from the risk appetite boundary in day-to-day operations. The operational buffer between appetite and a breach requiring escalation.

#### RISK APPETITE STATEMENT EXAMPLES

- We accept LOW risks without treatment but monitor quarterly for any increases in likelihood or impact.
- We have ZERO tolerance for risks that would result in a reportable data breach under GDPR Article 33.
- We will accept MEDIUM risks in emerging market operations where controls are not yet cost-effective.
- We will NOT accept any risk that threatens the continuity of our core payment processing platform.
- We tolerate HIGH inherent risk in innovation projects where controls can be implemented iteratively.

## HEAT MAPS AND RISK REPORTING

A heat map is a populated risk matrix — your actual risks plotted as dots. The distribution of dots tells a story: clustering in the top-right signals under-investment in controls; clustering in the bottom-left signals either strong controls or incomplete identification.

#### HEAT MAP BEST PRACTICES

- Plot both Inherent Risk (before controls) AND Residual Risk (after controls) to show control effectiveness
- Use risk IDs as labels on the map so stakeholders can trace dots back to the register
- Re-plot quarterly — movement of dots over time demonstrates the program's effectiveness
- Flag risks moving toward the top-right — these are emerging threats requiring urgent attention
- Include a 'target' risk zone that represents where residual risks should sit after treatment
- Present the heat map at every board/risk committee meeting as the primary risk summary

## COMMON RISK MATRIX MISTAKES

#### AVOID THESE RISK MATRIX ERRORS

- Using a 3×3 matrix — too coarse; merges meaningfully different risk levels into the same bucket
- Inconsistent scoring — different assessors rating the same risk differently without calibration
- Only tracking IT/cyber risks — strategic, financial, and third-party risks are excluded
- Never updating residual scores — the matrix shows inherent risk only, ignoring control changes
- No risk appetite overlay — risks plotted with no context of what level is acceptable
- Treating the matrix as a static artifact — it should be a living, quarterly-updated document

## CVSS AND VULNERABILITY SCORING INTEGRATION

The Common Vulnerability Scoring System (CVSS) provides standardized severity scores for technical vulnerabilities (0–10). CVSS scores from vulnerability scans should feed directly into your risk register's likelihood and impact scoring. A CVSS 9.8 critical vulnerability on an internet-facing server maps to Likelihood 5, Impact 5 = Risk Score 25.

### CVSS Score !' Risk Register

CVSS 9–10 = Likelihood 5. CVSS 7–8.9 = Likelihood 4. CVSS 4–6.9 = Likelihood 3. CVSS 1–3.9 = Likelihood 2. Adjust for asset exposure.

### Exploitability Metrics

Attack Vector (network vs local), Complexity (low vs high), Privileges Required, User Interaction — all reduce real-world likelihood when conditions are strict.

# 05 Risk Response Strategies

Accept | Avoid | Transfer | Mitigate | Residual Risk | Controls

Once a risk has been assessed and scored, a response strategy must be selected and documented. There are four fundamental strategies. Choosing the right one requires balancing cost of treatment against risk severity, organizational risk appetite, and regulatory obligations.

## THE FOUR RESPONSE STRATEGIES

### ACCEPT

Acknowledge the risk and take no action. For low risks below appetite threshold.

### AVOID

Eliminate the risk by removing the activity or asset that creates it.

### TRANSFER

Shift financial impact to a third party via insurance or contract.

### MITIGATE

Implement controls to reduce likelihood, impact, or both.

## ACCEPT

Risk acceptance is a conscious, documented decision — NOT inaction or ignorance. When a risk score falls within the organization's risk appetite, or when treatment costs exceed potential losses, acceptance is the appropriate and defensible choice.

### WHEN TO ACCEPT A RISK

- Risk score falls below the organization's defined appetite threshold (e.g., below 6 on a 25-point scale)
- Cost of treatment significantly exceeds the ALE — e.g., $500K control for a $10K ALE risk
- Risk is inherent to the business model and cannot be avoided without abandoning core operations
- Compensating controls reduce residual risk to an acceptable level without full treatment
- Regulatory guidance permits acceptance for specific low-severity risk categories

Accepted risks must still be formally documented with: the date of acceptance decision, the risk owner, the score at time of acceptance, and a scheduled review date. Undocumented acceptance is not acceptance — it is negligence.

## AVOID

Risk avoidance eliminates the root cause of the risk by discontinuing the activity, technology, or business relationship that creates the exposure. It is the most effective strategy — but often the most costly to the business.

### When to Avoid

Risk score is Critical (16–25). No cost-effective control exists. Regulatory non-compliance risk. Reputational risk to core brand.

### How to Avoid

Discontinue a product line. Exit a market. Decommission a legacy system. Terminate a vendor relationship. Drop a non-compliant process.

## TRANSFER

Risk transfer moves the financial consequences of a risk event to a third party. It does not eliminate the underlying risk — the threat and vulnerability remain. Transfer is most effective for high-impact, low-likelihood risks where insurance premiums are manageable.

### Cyber Insurance

Covers breach response costs, regulatory fines, business interruption, extortion payments, and reputational damage up to policy limits.

### Contractual Transfer

Indemnity clauses, SLAs, vendor liability provisions, and data processing agreements shift responsibility to the appropriate party.

### CYBER INSURANCE COVERAGE CHECKLIST

- First-party coverage: incident response costs, forensics, notification, credit monitoring, business interruption
- Third-party coverage: customer lawsuits, regulatory fines, media liability, network security liability
- Extortion coverage: ransomware payments, negotiation costs, crisis communication
- Verify: the policy covers cloud environments, third-party vendors, and social engineering attacks
- Exclusions to watch: acts of war, prior known vulnerabilities, intentional acts, unencrypted data

## MITIGATE

Mitigation is the most common risk response. Controls are implemented to reduce either the likelihood of the risk occurring (preventive controls) or the impact if it does occur (detective and corrective controls). A layered control approach — defense in depth — is most effective.

### Preventive Controls

Stop the risk from materializing. Examples: MFA, firewalls, patch management, access reviews, security training, code reviews.

### Detective Controls

Identify when a risk event occurs. Examples: SIEM alerts, IDS/IPS, vulnerability scanning, audit logs, anomaly detection.

### Corrective Controls

Reduce impact after an event. Examples: backups, disaster recovery, incident response playbooks, business continuity plans.

### Compensating Controls

Alternative controls when primary controls cannot be implemented. Documented in SOC 2 and PCI DSS as acceptable temporary measures.

## RESIDUAL RISK

Residual risk is the risk that remains after controls have been applied. No control eliminates risk entirely. The goal of risk treatment is to reduce residual risk to within your organization's risk appetite — not to zero. Zero risk is neither achievable nor cost-effective.

### RESIDUAL RISK MANAGEMENT

- Always document residual risk score separately from inherent risk score in your risk register
- If residual risk remains above appetite after mitigation, consider a secondary treatment (transfer)
- Review residual risk scores whenever controls change — new tools, removed controls, configuration changes
- Communicate residual risk explicitly to risk owners — they must accept it in writing
- Use inherent vs residual comparison to demonstrate control ROI to the board

## SECURITY CONTROL FRAMEWORKS

When selecting mitigating controls, reference established control frameworks rather than inventing controls from scratch. The three most widely used are NIST SP 800-53, CIS Controls, and ISO 27001 Annex A. These frameworks provide pre-validated controls that align with regulatory requirements and auditor expectations.

### NIST SP 800-53

800+ controls across 20 families. Required for US federal systems. Comprehensive but complex. Maps directly to NIST RMF. Best for large, regulated organizations.

### CIS Controls v8

18 controls, 153 safeguards organized into 3 Implementation Groups (IG1–IG3). Prioritized by risk impact. Best for organizations starting their control program.

### MAPPING RISKS TO CIS CONTROLS — EXAMPLES

- Unauthorized access risk !’ CIS Control 5 (Account Management) + CIS Control 6 (Access Control)
- Phishing risk !’ CIS Control 9 (Email & Browser) + CIS Control 14 (Security Awareness Training)
- Ransomware risk !’ CIS Control 11 (Data Recovery) + CIS Control 10 (Malware Defenses)
- Patch risk !’ CIS Control 7 (Continuous Vulnerability Management)
- Cloud misconfiguration risk !’ CIS Control 4 (Secure Configuration) + Control 3 (Data Protection)

06

# Risk Ownership & Governance

RACI | Three Lines of Defense | Risk Committee | Roles & Responsibilities

Risk management without clear ownership fails. Risks sit untreated, owners are unclear, escalations stall, and auditors find gaps. A governance structure defines who is responsible for what — from individual risk owners to the board — and ensures accountability at every level.

## THE THREE LINES OF DEFENSE MODEL

The Three Lines of Defense (3LoD) is the internationally recognized model for organizing risk governance. It defines three distinct roles in managing risk, each with different accountability levels. ISO 31000, IIA standards, and most regulatory frameworks reference this model.

**1st Line — Business Operations**

Risk owners, process controls, day-to-day management

**2nd Line — Risk & Compliance**

Risk framework, oversight, policy, monitoring & testing

**3rd Line — Internal Audit**

Independent assurance, objective testing, board reporting

### THREE LINES — KEY POINTS

- 1st Line owns the risk: business units operate controls day-to-day and are accountable for risk outcomes
- 2nd Line oversees the risk: Risk & Compliance provides the framework, tools, and oversight — does NOT own risks
- 3rd Line provides independent assurance: Internal Audit reports directly to the Audit Committee, not management
- Separation is critical: 2nd line cannot audit controls it designed; 3rd line cannot own controls it audits
- Board/Audit Committee sits ABOVE all three lines — receives independent assurance from the 3rd line

## RISK ROLES AND RESPONSIBILITIES

Clear role definitions prevent the most common governance failure: everyone thinks someone else owns the risk. These roles are standard across ISO 31000, NIST RMF, and most enterprise GRC frameworks.

### KEY RISK ROLES

- Chief Information Security Officer (CISO) — accountable for the overall cyber risk posture; reports to CEO/Board
- Risk Manager / CIRO — owns the risk management framework, register, and reporting cadence
- Risk Owner — responsible for a specific risk; must have authority and budget to implement treatment
- Control Owner — accountable for implementing and maintaining a specific control; reports to Risk Owner
- Data Protection Officer (DPO) — owns GDPR/privacy risk; required for public authorities and large-scale processors
- Internal Auditor — independently tests and reports on control effectiveness; reports to Audit Committee
- Risk Committee — executive-level body that sets appetite, approves treatment decisions, and reviews the register

## RACI MATRIX FOR RISK MANAGEMENT

A RACI matrix (Responsible, Accountable, Consulted, Informed) makes roles explicit for each risk management activity. Apply RACI at the risk register level (who manages the register) and at individual risk level (who owns each entry).

### R — Responsible

Does the work. For a risk: implements the treatment controls. May be delegated to a team or vendor. One or more people.

### A — Accountable

The Risk Owner. Signs off on the risk assessment and treatment decision. One person only. Cannot be delegated.

### C — Consulted

Provides input before decisions are made. Two-way communication. Examples: Legal, Compliance, affected business units.

### I — Informed

Notified of decisions and outcomes. One-way communication. Examples: Board, executives, regulators where required.

## RISK COMMITTEE STRUCTURE

A risk committee provides the governance layer that ensures risk management is not just an IT or compliance function but an enterprise-wide discipline tied to strategic decision-making.

### RISK COMMITTEE BEST PRACTICES

- Meet at least quarterly — monthly for organizations in highly regulated sectors (financial, healthcare)
- Attendees: CEO or COO (chair), CISO, CRO, CFO, Legal Counsel, Head of Internal Audit
- Standard agenda: risk register review, new critical risks, treatment updates, KRI dashboard, appetite review
- Board reporting: risk committee should report to the full board at least twice per year
- Escalation triggers: any risk moving from High to Critical automatically escalates to the next committee meeting
- Minutes must be retained: regulators and auditors will request evidence of risk governance meetings

## COMMON GOVERNANCE FAILURE PATTERNS

### WHY RISK GOVERNANCE PROGRAMS FAIL

- Risk committee meets annually — too infrequent; emerging risks go undetected for months
- No named risk owners — 'security team' owns all risks; nobody is personally accountable
- Risk manager reports to IT — organizational placement limits independence and board access
- Treatment approvals blocked by budget — no pre-approved risk treatment budget forces lengthy approval cycles
- Risk reporting is too technical — board receives technical metrics they cannot act on
- First and second lines are the same team — no separation; creates audit conflicts
- Risk register never presented to the board — governance value is zero if leadership cannot act on the data

07

# Risk Monitoring & Key Risk Indicators

KRIs | Appetite vs Tolerance | Review Cycles | Escalation | Reporting

Identifying and assessing risks is only half the battle. Risks evolve. Threats change. Controls weaken over time. A robust monitoring program detects these changes before they cause incidents. Key Risk Indicators transform your risk register from a static document into a dynamic early-warning system.

| 43% | 68% | 2.5× | 90d |
|---|---|---|---|
| Risks Materialize Due to Poor Monitoring | Orgs Without Formal KRI Program | Higher Breach Cost Without Monitoring | Median Detection Gap Without KRIs |

## KEY RISK INDICATORS (KRIS)

A Key Risk Indicator (KRI) is a metric that provides advance warning that a risk is increasing. Unlike Key Performance Indicators (KPIs) which measure outcomes, KRIs are forward-looking — they measure conditions that predict a risk event before it occurs.

### Leading KRI

Predicts future risk events. Example: rising number of failed login attempts predicts a credential stuffing attack. Acts as an early warning signal.

### Lagging KRI

Confirms that a risk has materialized or is materializing. Example: number of security incidents this month. Used for trend analysis and reporting.

### EXAMPLE KRIS BY RISK CATEGORY

- Access Risk: % of accounts with MFA enabled; number of privileged accounts without recent review
- Patch Risk: % of critical patches applied within SLA; count of systems running EOL software
- Phishing Risk: phishing simulation click rate; number of credential theft reports this quarter
- Vendor Risk: % of critical vendors with current security assessments; number of overdue questionnaires
- Incident Risk: mean time to detect (MTTD); mean time to respond (MTTR); repeat incident count
- Compliance Risk: % of policies reviewed within schedule; number of open audit findings > 90 days
- Data Risk: number of DLP policy violations; % of sensitive data encrypted at rest

## RISK APPETITE VS RISK TOLERANCE

These two concepts are closely related but distinct. Confusing them leads to poor escalation decisions and governance failures. Both must be formally defined, approved by the board, and communicated to all risk owners.

### Risk Appetite

The strategic boundary. 'We are willing to accept up to X level of risk to achieve objective Y.' Set annually by the board. Expressed as a threshold or statement.

### Risk Tolerance

The operational boundary. The acceptable variance around the appetite. 'We tolerate residual risk scores up to 8 in this domain.' The trigger for escalation.

## REVIEW CYCLES AND TRIGGERS

Risk registers require both scheduled reviews and event-triggered reviews. Scheduled reviews ensure the register stays current with the evolving threat landscape. Event-triggered reviews respond to changes that may invalidate previous assessments.

### REVIEW SCHEDULE

- Full risk register review — minimum quarterly; monthly in regulated industries (FSI, healthcare)
- Individual risk re-assessment — whenever a control changes, an incident occurs, or the environment shifts
- Risk appetite review — annually, or whenever a material change in business strategy occurs
- New system/process onboarding — risk assessment required before go-live, not after
- Post-incident review — all risks related to an incident must be immediately re-assessed and updated
- Third-party risk review — annual security assessments for critical vendors; triggered by vendor incidents

## ESCALATION FRAMEWORK

Without a defined escalation path, critical risks sit in the register unresolved until an incident occurs. An escalation framework specifies who is notified when risk thresholds are breached and what actions are required within what timeframe.

### ESCALATION TRIGGERS AND PATHS

- Risk score moves to Critical (16–25) !' immediate escalation to CISO and Risk Committee
- KRI breaches tolerance threshold !' notify Risk Owner and 2nd line within 24 hours
- Treatment deadline missed by 30+ days !' escalate to department head; add to next board report
- New regulatory requirement identified !' compliance team notified; risk register updated within 5 days
- Third-party incident affecting critical vendor !' vendor risk reassessed within 48 hours
- Audit finding rated High or Critical !' treatment plan required within 30 days; tracked in register

## KRI THRESHOLD SETTING AND CALIBRATION

A KRI is only useful if its threshold is correctly calibrated. Thresholds that are too sensitive generate false alarms — risk owners start ignoring alerts. Thresholds that are too lenient miss real risk increases. Calibrate using historical baseline data and industry benchmarks.

### KRI THRESHOLD CALIBRATION APPROACH

- Step 1 — Establish baseline: measure current KRI values over a 3-month period to establish normal range
- Step 2 — Set Green threshold: values within normal operating range (no action required)
- Step 3 — Set Amber threshold: values 20–30% above baseline (monitor closely; notify risk owner)
- Step 4 — Set Red threshold: values 50%+ above baseline or absolute limits (escalate immediately)
- Step 5 — Review annually: baselines change as the organization and threat landscape evolve
- Step 6 — Document rationale: auditors will ask why specific threshold values were chosen

# 08 Compliance Frameworks

ISO 31000 | ISO 27005 | NIST RMF | COSO ERM | COBIT | Selection Guide

Compliance frameworks provide the structure, vocabulary, and process guidance for implementing risk management. Using a recognized framework demonstrates due diligence to regulators, auditors, customers, and insurers. It also provides a ready-made blueprint rather than reinventing the wheel.

## ISO 31000 — RISK MANAGEMENT STANDARD

ISO 31000:2018 is the international standard for risk management principles and guidelines. It is not certifiable (unlike ISO 27001) but provides the universal foundation that most other frameworks build upon. It applies to any organization regardless of size, sector, or industry.

### ISO 31000 CORE PRINCIPLES

- Integrated — risk management is embedded into all organizational activities and decision-making
- Structured and Comprehensive — a consistent, comparable approach produces reliable and comparable results
- Customized — the framework is tailored to the organization's context, objectives, and risk profile
- Inclusive — stakeholder knowledge and perspectives are incorporated into risk assessment
- Dynamic — risk management anticipates and responds to changes in the internal and external environment
- Best Available Information — decisions based on historical data, expert judgment, and stakeholder input
- Human and Cultural Factors — recognizes the significant influence of human behavior on risk outcomes

## ISO 27005 — INFORMATION SECURITY RISK MANAGEMENT

ISO 27005 provides guidelines for information security risk management, directly supporting ISO 27001 implementation. It defines a structured process for identifying, assessing, and treating information security risks. ISO 27001 certification requires evidence of ISO 27005-aligned risk assessment.

### Risk Assessment Process

Systematic process of risk identification, analysis (likelihood + impact), and evaluation against acceptance criteria defined in the risk appetite.

### Risk Treatment Process

Selection and implementation of options to modify risk. Documents the Risk Treatment Plan (RTP) — a core ISO 27001 evidence artifact.

## NIST RISK MANAGEMENT FRAMEWORK (RMF)

NIST RMF (SP 800-37) is the US federal standard for managing cybersecurity risk in information systems. Mandatory for US federal agencies; widely adopted by defense contractors, healthcare organizations, and enterprises seeking a rigorous, structured approach.

| | | |
|---|---|---|
| 1 Categorize | 2 Select | 3 Implement |
| 4 Assess | 5 Authorize | 6 Monitor |

### NIST RMF 6 STEPS

- 1. Categorize — classify the information system using FIPS 199/NIST SP 800-60 impact levels (Low/Mod/High)
- 2. Select — choose the appropriate security controls from NIST SP 800-53 based on the impact level
- 3. Implement — put the selected controls into practice; document implementation details
- 4. Assess — evaluate whether the controls are implemented correctly and operating as intended
- 5. Authorize — senior official accepts residual risk and authorizes the system to operate (ATO)
- 6. Monitor — continuously track control effectiveness, changes, and new vulnerabilities

## COSO ENTERPRISE RISK MANAGEMENT

The Committee of Sponsoring Organizations (COSO) ERM framework integrates risk management with strategy and performance. The 2017 update emphasizes the connection between risk management and value creation — positioning risk as a business enabler, not just a compliance function.

### 5 COSO ERM Components

1. Governance & Culture 2. Strategy & Objective-Setting 3. Performance 4. Review & Revision 5. Information & Communication.

### Key Differentiator

COSO ERM explicitly links risk appetite to strategy. Every strategic decision requires an assessment of the risk types and amounts the organization is willing to accept.

## COBIT & FRAMEWORK SELECTION

COBIT (Control Objectives for IT) governs IT risk within the broader enterprise context. Created by ISACA, it maps IT processes to business goals and aligns with ISO 31000, ITIL, and ISO 27001. Use it when IT governance and risk management need to be unified.

### WHICH FRAMEWORK TO CHOOSE

- ISO 27001/27005 !’ best for: organizations seeking certification; security-focused risk management
- NIST RMF !’ best for: US federal contractors, defense, healthcare — where NIST compliance is required
- ISO 31000 !’ best for: enterprise-wide risk management; any sector; foundational principles
- COSO ERM !’ best for: publicly traded companies; strong board-level focus; strategy-linked risk
- COBIT !’ best for: IT-heavy organizations; aligning IT governance with business risk
- Combine frameworks: most mature organizations use ISO 31000 as the umbrella with 27005 or NIST for cyber

**ServiceNow GRC** | **Archer RSA** | **Vanta** | **Drata** | **OneTrust** | **Secureframe**

**MetricStream** | **LogicGate** | **6clicks** | **Diligent** | **Tugboat Logic**

**AuditBoard**

## MAPPING FRAMEWORKS TO RISK REGISTER FIELDS

Most organizations operate in environments that touch multiple frameworks simultaneously — ISO 27001 for certification, GDPR for privacy compliance, NIST for technical rigor, and COSO for board-level governance. Mapping your risk register fields to multiple frameworks from the start avoids duplication and streamlines audits.

### FRAMEWORK FIELD MAPPING

- Risk ID !’ ISO 27001 clause 6.1.2 (risk identification); NIST RMF Step 1 (Categorize assets)
- Likelihood & Impact !’ ISO 27005 section 8 (risk analysis); NIST SP 800-30 Table D-5
- Control Reference !’ ISO 27001 Annex A control number; CIS Control number; NIST 800-53 control ID
- Risk Owner !’ ISO 27001 clause 6.1.3 (risk treatment); COSO ERM Component 3 (Performance)
- Review Date !’ ISO 27001 clause 9.3 (management review); NIST RMF Step 6 (Monitor)
- Treatment Plan !’ ISO 27001 Statement of Applicability; NIST RMF Authorization Package

## DORA — DIGITAL OPERATIONAL RESILIENCE ACT

DORA came into force across the EU financial sector in January 2025. It mandates a comprehensive ICT risk management framework for banks, insurers, investment firms, and their critical ICT third-party providers. If you operate in EU financial services, DORA is your most pressing risk register obligation.

### DORA KEY RISK REGISTER REQUIREMENTS

- ICT Risk Management Framework — documented policies covering identification, protection, detection, response, recovery
- ICT Asset Classification — all ICT assets supporting critical functions catalogued and classified
- Third-Party ICT Provider Register — dedicated registry of all ICT third-party dependencies with risk scores
- Incident Classification — mandatory classification of ICT-related incidents as major/non-major with reporting obligations
- Digital Operational Resilience Testing — penetration testing and threat-led testing feeding back into risk register
- Concentration Risk — identification and assessment of single-vendor dependency risks at systemic level

# 09 Risk Register in Practice

Register Components | Sample Register | GRC Tools | ISMS Integration

A risk register is only as useful as its implementation. Theory is straightforward — practice is where most organizations struggle. This chapter covers the essential components of a production-ready risk register, a worked example, tool selection, and integration with your broader security management system.

## RISK REGISTER FIELDS

Every risk register entry should capture a minimum set of fields. Too few fields and the register lacks actionability; too many and it becomes a bureaucratic burden that nobody maintains. The following is the recommended baseline for a cyber risk register:

### CORE RISK REGISTER FIELDS

- Risk ID — unique identifier (R-001 format) for tracking, cross-referencing, and audit trails
- Risk Title — short descriptive name, max 10 words, unambiguous
- Risk Description — detailed narrative: what could happen, to which asset, via which threat vector
- Risk Category — domain classification (Access, Data, Infrastructure, Application, Vendor, Compliance, etc.)
- Likelihood (1–5) — rated against the organization's likelihood scale with justification note
- Impact (1–5) — rated against the organization's impact scale with justification note
- Inherent Risk Score — Likelihood × Impact BEFORE any controls
- Controls in Place — list of existing controls that reduce the inherent risk
- Residual Risk Score — Likelihood × Impact AFTER existing controls
- Response Strategy — Accept / Avoid / Transfer / Mitigate
- Treatment Plan — specific actions, owner, deadline for each treatment step
- Risk Owner — named individual accountable for managing and reporting on this risk
- Review Date — next scheduled reassessment date
- Date Identified / Last Updated — for trend tracking and audit evidence

## SAMPLE RISK REGISTER

The following sample register demonstrates how the above fields translate into practice. Note the use of inherent vs residual scores to show control effectiveness, and the variety of response strategies applied based on risk level:

| ID | Risk Description | Category | L | I | Score | Response | Owner |
|---|---|---|---|---|---|---|---|
| R-001 | Unauthorized access to customer PII | Data | 4 | 5 | 20 | Mitigate | CISO |
| R-002 | Ransomware attack on file servers | Cyber | 3 | 5 | 15 | Mitigate | IT Mgr |
| R-003 | Vendor data breach (third party) | Supply | 3 | 4 | 12 | Transfer | Risk Mgr |
| R-004 | System outage — core banking app | Ops | 2 | 5 | 10 | Mitigate | CTO |
| R-005 | Non-compliance with GDPR | Comp. | 2 | 4 | 8 | Avoid | DPO |
| R-006 | Phishing — staff credential theft | Cyber | 4 | 3 | 12 | Mitigate | CISO |

## GRC PLATFORM SELECTION

A spreadsheet works for small organizations with fewer than 50 risks. Beyond that, a dedicated GRC platform provides version control, workflow automation, risk owner notifications, real-time dashboards, and audit trail capabilities that spreadsheets cannot match.

### Spreadsheet (Excel/Sheets)

Best for: startups, small teams, initial implementation. Pros: free, flexible. Cons: no workflow, version control issues, no real-time dashboard.

### GRC Platform

Best for: >50 risks, regulated industries, multi-department programs. Pros: automation, audit trails, dashboards. Cons: cost, implementation time.

### GRC TOOL COMPARISON

- ServiceNow GRC — enterprise-grade; deep ITSM integration; best for large organizations already on ServiceNow
- Archer RSA — comprehensive; used in financial services and government; steep learning curve
- Vanta / Drata — compliance-focused; excellent for SOC 2, ISO 27001; strong automation; SMB/mid-market
- OneTrust — privacy + GRC; strong for GDPR compliance; growing risk management capabilities
- 6clicks — AI-powered; strong multi-framework support; competitive pricing for mid-market
- AuditBoard — audit-centric; excellent workflow for 3rd line; integrates with risk registers

## INTEGRATING THE RISK REGISTER WITH YOUR ISMS

ISO 27001 requires a formal information security risk assessment. Your risk register IS that assessment. To pass an ISO 27001 audit, the register must demonstrate systematic identification, assessment with documented methodology, treatment decisions, and owner sign-off.

### ISO 27001 RISK REGISTER AUDIT CHECKLIST

- Clause 6.1.2 — information security risk assessment process is defined and documented
- Clause 6.1.3 — risk treatment plan with selected controls mapped to ISO 27001 Annex A
- Annex A mapping — each risk in the register linked to applicable Annex A control categories
- Statement of Applicability (SoA) — all Annex A controls documented as applicable or excluded with justification
- Risk owner sign-off — evidence that risk owners have reviewed and accepted their assigned risks
- Review history — date-stamped record of all previous risk register reviews (minimum annual)

## RISK REGISTER AUTOMATION AND AI

Modern GRC platforms are embedding AI to accelerate risk identification, auto-populate scoring suggestions, and flag anomalies in KRI trends. AI-assisted risk management is not replacing human judgment — it is augmenting the speed and completeness of risk processes that previously took weeks to complete.

### AI CAPABILITIES IN RISK MANAGEMENT

- Automated risk identification — AI scans policies, incident logs, and threat intelligence to suggest new register entries
- Intelligent scoring — ML models suggest likelihood and impact scores based on asset criticality and historical incidents
- Anomaly detection in KRIs — AI flags unusual patterns in risk indicators before they cross manual thresholds
- Natural language processing — extract risks from board minutes, audit reports, and incident tickets automatically
- Continuous control monitoring — automated testing of controls against policy, alerting when gaps emerge
- Regulatory change management — AI monitors regulatory feeds and maps new requirements to affected risk entries

## RISK REGISTER FOR CLOUD ENVIRONMENTS

Cloud environments introduce unique risk characteristics: rapid change velocity, shared responsibility models, and ephemeral infrastructure that traditional risk registers struggle to track. Cloud risk requires additional fields and a higher review frequency than on-premises risks.

### Cloud-Specific Risks

Misconfigured S3 buckets, over-permissioned IAM roles, public snapshots, unencrypted data at rest, shadow SaaS, container escape vulnerabilities.

### Shared Responsibility Gaps

The boundary between cloud provider responsibility and customer responsibility is the most commonly misunderstood — and most commonly exploited — aspect of cloud security.

# 10 Building & Maintaining Your Risk Register

Step-by-Step | Common Mistakes | Careers | Certifications | Roadmap

Everything in this guide comes together in this final chapter. Building a risk register for the first time is manageable in 30 days. Maintaining it as a living, board-facing governance tool is a career-long discipline. Both are within reach with the right approach.

## 30-DAY RISK REGISTER BUILD PLAN

You do not need a perfect risk register on day one. You need a good-enough register that is reviewed, maintained, and improved over time. Perfection is the enemy of a functioning risk program. Start here:

1. Days 1–5: Define scope, methodology, and scoring scales. Get board/management approval on risk appetite. Select your tool (spreadsheet or GRC platform).
2. Days 6–10: Conduct risk identification workshops with key stakeholders. Review historical incidents. Run STRIDE analysis on critical systems. Produce initial risk longlist.
3. Days 11–15: Score all identified risks using Likelihood × Impact. Calculate inherent risk scores. Identify existing controls and calculate residual scores.
4. Days 16–20: Select response strategies for all risks above appetite threshold. Assign risk owners. Document treatment plans with deadlines.
5. Days 21–25: Define KRIs for your top 10 risks. Set review dates. Configure dashboards or reports. Prepare initial board/management presentation.
6. Days 26–30: Present to board/risk committee. Capture feedback. Establish quarterly review cadence. Assign treatment ownership formally in writing.

## COMMON RISK REGISTER MISTAKES TO AVOID

### TOP RISK REGISTER FAILURES

- Building it once, never reviewing it — a static register is an audit liability, not a governance tool
- No defined risk appetite — scores are meaningless without a threshold defining what is acceptable
- Assigning ownership to 'the security team' — every risk needs a named individual, not a group
- Only tracking IT/cyber risks — operational, financial, compliance, and reputational risks are excluded
- Using different scoring scales across assessors — calibrate all assessors before populating the register
- No board visibility — a risk register that never reaches the board has zero governance value
- Conflating issues with risks — completed incidents should move to an issues log, not stay in the register
- No link to business objectives — risks not tied to specific assets or processes are not actionable

## CAREERS IN RISK MANAGEMENT

Risk management is one of the highest-growth areas in cybersecurity. The GRC (Governance, Risk, and Compliance) career track offers excellent compensation, clear seniority progression, and the ability to work across industries.

### Risk Analyst

Entry-level. Maintains the register, coordinates assessments, prepares reports. Avg. salary: $65K–$90K. Pathway to Risk Manager.

### Risk Manager / CRO

Owns the framework and program. Manages the team. Reports to CISO/C-suite. Avg. salary: $110K–$175K+.

### GRC Consultant

External advisory. Builds programs for multiple clients. High variety, high demand. Avg. daily rate: $800–$1,500+.

### vCISO

Virtual CISO. Provides fractional executive leadership including risk governance. Rapidly growing market. $150K–$300K+ equivalent.

## RISK COMMUNICATION TEMPLATES

Consistent communication templates reduce preparation time and ensure every stakeholder receives the information they need in the format they expect. Standardize these templates in your GRC platform or document library.

### EXECUTIVE RISK SUMMARY TEMPLATE — MONTHLY

- HEADER: Risk Program Health — [Month Year] | Overall Posture: [Green/Amber/Red]
- SECTION 1: Portfolio Summary — Total risks by level: [X] Critical | [X] High | [X] Medium | [X] Low
- SECTION 2: Movement — Risks increased: [X] | Decreased: [X] | New this month: [X] | Closed: [X]
- SECTION 3: Top 3 Risks — For each: Risk title, current score, owner, treatment status, target date
- SECTION 4: KRI Dashboard — Traffic light status for each KRI with 1-sentence explanation for Amber/Red
- SECTION 5: Overdue Treatments — Risks past treatment deadline with responsible owner and escalation plan
- FOOTER: Next review date | Contact: [Risk Manager name] | Register version: [X.X]

## POST-INCIDENT RISK REVIEW PROCESS

Every security incident is intelligence about your risk register. A post-incident review (PIR) should update risk scores, add new risks surfaced by the incident, and improve control assessments. Organizations that skip PIRs miss the most valuable signal available for risk program improvement.

### POST-INCIDENT RISK REGISTER UPDATE PROTOCOL

- Within 24 hours: Identify all risk register entries related to the incident vector and asset
- Within 72 hours: Re-assess likelihood scores — the incident proves the threat is active and real
- Within 1 week: Evaluate control effectiveness — which controls failed? Which helped? Update ratings.
- Within 2 weeks: Add any new risks identified during incident investigation to the register
- Within 30 days: Complete root cause analysis; update treatment plans to address identified gaps
- Within 90 days: Verify that new/updated treatment actions have been implemented; re-score residual risk
- All entries: Document the incident reference number in the register for audit trail continuity

## RISK PROGRAM METRICS AND KPIS

Beyond KRIs (which measure risk levels), your risk program itself should be measured. Program KPIs demonstrate to leadership that risk management is delivering value and improving over time — essential for budget retention and organizational credibility.

| !“ | 95%+ | 100% | Q |
|---|---|---|---|
| Avg Residual Risk Score Trend | Risks with Named Owner | High/Critical with Treatment Plans | Register Review Frequency |

### RISK PROGRAM KPIS

- % of risks with residual score within risk appetite !’ target 100%; measures control effectiveness
- Mean time to treatment (MTTT) for High risks !’ target <30 days; measures responsiveness
- % of risk owners with completed annual training !’ target 100%; measures governance maturity
- % of critical vendors with current assessments !’ target 100%; measures TPRM program health
- Risk register coverage — risks per $1M revenue compared to industry benchmark !’ measures completeness
- % reduction in average residual risk score year-over-year !’ primary indicator of program value

## RISK MANAGEMENT CERTIFICATIONS

### TOP CERTIFICATIONS

- CRISC (Certified in Risk and Information Systems Control) — ISACA; gold standard for IT risk; requires 3 years exp.
- CISM (Certified Information Security Manager) — ISACA; management-level; covers risk governance and program mgmt
- CISSP — ISC2; covers risk management domain; requires 5 years; most prestigious general security cert
- ISO 31000 Lead Risk Manager — PECB; framework-specific; excellent for GRC consulting roles
- ISO 27001 Lead Implementer — PECB; includes risk assessment; required for ISO 27001 implementation projects
- CIPP/E (Privacy) — IAPP; excellent for GDPR risk management roles; fastest-growing privacy certification

## YOUR NEXT STEPS

Risk management is not a project with an end date — it is a program that matures over time. Start small, build momentum, and compound your gains. The organizations that get risk management right are the ones that treat the register as a living tool, not a compliance artifact.

### Get the Full Risk Register Guide — PDF Download

kokumorix.gumroad.com/l/bmuaev | bemitechsolutions.com | @insightswithrayslater

### Subscribe for more training content

YouTube: @insightswithrayslater | TikTok: @ransfordslater | 2026 Edition

# 11 Third-Party Risk Management (TPRM)

Vendor Risk | Due Diligence | Contracts | Fourth-Party Risk | Tools

Third-party risk is now one of the top five risks in every enterprise risk register. The SolarWinds breach impacted 18,000 organizations. The MOVEit exploit hit hundreds of firms through a single vendor. Your security posture is only as strong as your weakest vendor's. TPRM is no longer optional.

| 98% | 3.9× | 60% | 280d |
|---|---|---|---|
| Orgs Breached via Third Party | Higher Breach Cost (Third-Party) | Orgs Cannot List All Vendors | Avg. Detection Time via Vendor |

## WHY THIRD-PARTY RISK IS DIFFERENT

Internal risks are within your control — you can patch your own systems, train your own staff, and enforce your own policies. Third-party risks are partially outside your control. You depend on the vendor's security posture, their subcontractors, and their incident response capability. This requires a dedicated management approach.

### Third-Party Risk

Risk arising from the security posture, practices, or failures of direct vendors, suppliers, and service providers you share data or systems with.

### Fourth-Party Risk

Risk from your vendors' vendors. If your cloud provider uses a sub-processor that is breached, you are impacted — even though you have no direct relationship.

## VENDOR RISK TIERING

Not all vendors require the same level of scrutiny. A risk-based tiering model ensures you apply due diligence proportionate to the actual risk exposure. Over-assessing low-risk vendors wastes resources; under-assessing critical vendors creates gaps.

| Tier 1 — Critical | Tier 2 — High | Tier 3 — Medium | Tier 4 — Low |
|---|---|---|---|
| PII, financial & production access. Full assessment, annual review, right-to-audit. Cloud providers, payment processors. | Internal systems, limited data. Simplified questionnaire, biannual review. IT suppliers, marketing platforms. | No sensitive data. Self-attestation, annual review. Office supplies, training vendors, non-integrated SaaS. | No data access. Register and review on contract renewal only. Couriers, facilities, print services. |

## THIRD-PARTY DUE DILIGENCE

Due diligence is performed before onboarding a vendor and repeated periodically throughout the relationship. The depth of assessment is proportionate to the vendor tier. A structured questionnaire combined with evidence review provides the most reliable picture of vendor security posture.

### DUE DILIGENCE CHECKLIST — TIER 1 VENDORS

- Security questionnaire — SIG Lite or CAIQ aligned; covers 18+ security domains
- Evidence review — SOC 2 Type II report, ISO 27001 certificate, or equivalent independent assessment
- Penetration test results — request latest external pen test summary and remediation evidence
- Incident history — any material breaches in the past 3 years; response times and customer notification
- Sub-processor list — identify all fourth parties with access to your data; request their assessments
- Business continuity — DR plan, RTO/RPO targets, last test date and results
- Data residency — confirm data is processed and stored in jurisdictions permitted by your compliance requirements

## CONTRACTUAL RISK CONTROLS

Contracts are your primary mechanism for managing third-party risk. A vendor with excellent questionnaire responses but weak contractual obligations leaves you exposed. These clauses must be in every Tier 1 and 2 vendor contract:

### Data Processing Agreement (DPA)

Required under GDPR for any vendor processing EU personal data. Specifies purpose limitation, sub-processor controls, data deletion, and breach notification obligations.

### Right to Audit

Contractual right to audit the vendor's security controls. Most vendors will resist — escalate to a right to receive third-party audit reports as a minimum.

### Breach Notification SLA

Vendor must notify you within 24–72 hours of discovering a security incident affecting your data. Align with your regulatory notification obligations.

### Security Baseline Requirements

Minimum security standards the vendor must maintain: MFA, encryption at rest/in-transit, patch management SLA, vulnerability disclosure program.

## CONTINUOUS VENDOR MONITORING

Annual assessments are insufficient for Tier 1 vendors. Continuous monitoring surfaces emerging risks — new CVEs in the vendor's products, dark web mentions, certificate expirations, and changes in their security posture — before they become incidents.

### CONTINUOUS MONITORING SOURCES

- Security ratings platforms — BitSight, SecurityScorecard, RiskRecon provide real-time vendor scorecards
- Threat intelligence — OSINT, FS-ISAC, sector ISACs for sector-specific vendor threat intelligence
- Dark web monitoring — alerts when vendor credentials or data appear in breach databases
- News & breach databases — HaveIBeenPwned API, Recorded Future for vendor incident alerts
- Certificate monitoring — detect unexpected SSL certificate changes that may indicate supply chain compromise

BitSight | SecurityScorecard | RiskRecon | OneTrust TPRM | ProcessUnity | Prevalent | Archer | ServiceNow TPRM | Venminder | Whistic | Panorays

## RESPONDING TO THIRD-PARTY INCIDENTS

When a vendor suffers a breach, your response speed is constrained by your relationship with them. Organizations with mature TPRM programs have pre-defined playbooks that activate the moment a vendor incident is announced. Those without TPRM scramble to understand their exposure while the clock is ticking.

### THIRD-PARTY INCIDENT RESPONSE PLAYBOOK

- Hour 0–4: Identify all business processes and data sharing with the affected vendor
- Hour 4–8: Assess potential data exposure — what data does this vendor hold? Under what agreement?
- Hour 8–24: Contact vendor's incident response team directly; request breach scope and timeline
- 24–48 hours: Assess regulatory notification obligations (GDPR 72hr, HIPAA 60-day, SEC 4-day rules)
- 48–72 hours: Implement interim controls — suspend vendor API access, rotate shared credentials
- Ongoing: Update vendor's risk register entry; document decisions and communications for audit trail

## EMERGING THIRD-PARTY RISK VECTORS

The threat landscape for third-party risk is rapidly expanding beyond traditional vendor relationships. New attack vectors require your TPRM program to evolve beyond questionnaire-based assessments.

### Open Source Dependencies

Log4Shell affected 93% of enterprise cloud environments via a single open-source library. Track your software bill of materials (SBOM) for every application.

### AI Model Supply Chain

Third-party AI models and APIs introduce new risks: training data poisoning, model inversion attacks, and unauthorized data processing by AI providers.

# 12 Risk Communication & Reporting

Board Reporting | Dashboards | Stakeholder Communication | Risk Culture

The most technically rigorous risk register has zero value if it cannot be understood by the people who need to act on it. Risk communication is the bridge between analysis and decision-making. Getting it right accelerates treatment approvals, secures budget, and builds a risk-aware culture.

## COMMUNICATING RISK TO THE BOARD

Boards are not security experts. They are responsible for governance — setting appetite, approving major treatment decisions, and holding management accountable. Board-level risk communication must be strategic, visual, and quantified. Technical jargon destroys credibility at this level.

### BOARD RISK REPORT — ESSENTIAL ELEMENTS

- Executive Summary — 1 paragraph: current risk posture, top 3 risks, trend vs last quarter
- Risk Heat Map — visual plot of current residual risks; show movement since last board report
- Top 5 Risks — narrative description, score, treatment status, owner, and projected residual date
- KRI Dashboard — traffic-light indicators; flag any KRIs in amber or red with brief explanation
- Treatment Progress — % of risks with active treatment plans on track vs overdue
- Incidents & Near-Misses — summary of any security events since last report; risk register updates made
- Budget Ask (if applicable) — quantified ROI: cost of control vs ALE reduction it achieves

## RISK DASHBOARD DESIGN

A well-designed risk dashboard provides at-a-glance visibility into the risk program's health. The goal is to answer five questions instantly: How many risks do we have? Where are they distributed? Are we trending better or worse? Are treatments on track? Are any KRIs breaching thresholds?

### Summary Metrics

Total risks by level (Critical/High/Medium/Low). Trend vs last quarter. % with active treatment. % overdue for review.

### KRI Traffic Lights

Green/Amber/Red status for each defined KRI. Amber = approaching tolerance. Red = tolerance breached. Requires immediate attention.

### Treatment Pipeline

Risks by treatment status: Not Started / In Progress / Completed / Accepted. Overdue treatments highlighted in red with owner names.

### Residual Risk Trend

Time-series chart showing average residual risk score over the past 4 quarters. Downward trend demonstrates program maturity and ROI.

## STAKEHOLDER COMMUNICATION

Different stakeholders need different views of the same risk data. Risk owners need operational detail. Department heads need a filtered view of their domain's risks. The board needs the strategic picture. A good GRC platform generates these tailored views automatically.

### COMMUNICATION BY STAKEHOLDER

- Board / Audit Committee — quarterly; strategic heat map, top 5 risks, KRI dashboard, budget impact
- Executive Team (CISO, CFO, COO) — monthly; full register summary, treatment pipeline, KRI alerts
- Risk Owners — weekly/monthly; their specific risks, treatment tasks, upcoming review dates, KRI thresholds
- Department Heads — monthly; their department's risk profile, overdue treatments, new risks added
- Internal Audit — quarterly; risk methodology, scoring consistency, governance evidence, treatment evidence
- Regulators / External Auditors — on request; formal risk assessment documentation, treatment plans, review history

## BUILDING A RISK-AWARE CULTURE

Tools and processes create a risk program. Culture makes it sustainable. Organizations where risk management is seen as a compliance burden — rather than a business enabler — have registers that are never updated, owners who avoid accountability, and boards that treat risk reports as box-ticking exercises.

### CULTURE BUILDING TACTICS

- Link risk management to business outcomes — show how treated risks enabled a new product launch or saved $X
- Celebrate risk wins — when a treated risk's KRI moves from red to green, communicate the success widely
- Make risk visible — monthly 'top risk of the month' communication to all staff, in plain language
- Reward identification — recognize staff who identify new risks before they become incidents
- Train all risk owners — annual risk management training is not enough; embed in onboarding for every manager
- Leadership modelling — when the CISO and CFO visibly engage with the risk register, it signals importance to the organization

## RISK PROGRAM MATURITY

Maturity models help organizations understand where they are and what's needed to improve. The Risk Management Maturity Model (RM3) and CMMI-based frameworks provide a structured path from ad-hoc to optimized risk management. Assess your maturity level annually.

### Level 1 — Ad Hoc

Risks managed informally. No formal register. Reactive approach. Assessment is inconsistent. No defined ownership or governance.

### Level 2 — Repeatable

Basic risk register exists. Scoring methodology defined. Risk owners assigned. Annual review conducted. Not yet fully integrated.

### Level 3 — Defined

Formal framework documented. All risk categories covered. KRIs defined. Board reporting in place. TPRM program active.

### Level 4 — Optimized

Quantitative risk analysis (FAIR). Continuous monitoring. Integrated with ISMS, BCP, and strategic planning. Risk culture embedded.

A

# Appendix — Glossary & Quick Reference

Key Terms | Risk Scoring Guide | Frameworks Matrix | Resources

## RISK MANAGEMENT GLOSSARY

### CORE TERMINOLOGY — A TO I

- ALE (Annual Loss Expectancy) — expected annual financial loss = SLE × ARO
- ARO (Annual Rate of Occurrence) — expected frequency of a risk event per year
- Asset — anything of value to the organization (data, systems, people, processes, brand)
- Audit Trail — chronological record of risk register changes for governance and compliance evidence
- Control — a safeguard that reduces the likelihood or impact of a risk materializing
- COSO ERM — Committee of Sponsoring Organizations Enterprise Risk Management framework
- CRISC — Certified in Risk and Information Systems Control (ISACA certification)
- DPA (Data Processing Agreement) — contractual document required by GDPR for data processors
- Exposure Factor — percentage of asset value likely lost in a single risk event
- Inherent Risk — risk level before any controls are applied
- ISO 31000 — international standard for risk management principles and guidelines

### CORE TERMINOLOGY — K TO Z

- KRI (Key Risk Indicator) — metric providing advance warning that a risk is increasing
- NIST RMF — NIST Risk Management Framework; 6-step process for managing system risk
- Probability — likelihood that a specific risk event will occur within a defined time period
- Residual Risk — risk level remaining after controls have been applied
- Risk Appetite — amount and type of risk an organization is willing to accept
- Risk Owner — individual accountable for monitoring and treating a specific risk
- Risk Register — structured repository of all identified, assessed, and treated organizational risks
- Risk Tolerance — operational boundary around the risk appetite threshold
- SLE (Single Loss Expectancy) — expected financial loss from a single risk event = AV × EF
- STRIDE — Microsoft threat model: Spoofing, Tampering, Repudiation, Info Disclosure, DoS, Elevation
- TPRM (Third-Party Risk Management) — systematic management of risks from vendors and suppliers

## FRAMEWORK QUICK REFERENCE

### ISO 31000

Universal risk principles. Not certifiable. Best for establishing enterprise risk culture and governance. Any sector.

### ISO 27005

Information security risk assessment. Directly supports ISO 27001 certification. Cyber-focused.

### NIST RMF

6-step federal standard. Required for US government/defense. Best quantitative process available. SP 800-37.

### COSO ERM

Strategy-linked enterprise risk. Required for publicly listed companies. Aligns risk to business value creation.

### COBIT

IT governance + risk. Aligns IT processes to business goals. Strong for large IT-heavy organizations.

### FAIR

Quantitative cyber risk analysis. Produces financial risk estimates. Industry standard for risk quantification.

## RECOMMENDED RESOURCES

### FURTHER LEARNING

- NIST SP 800-30 — Guide for Conducting Risk Assessments (free download at csrc.nist.gov)
- ISO 31000:2018 — Risk Management Guidelines (iso.org)
- ISACA CRISC Review Manual — official study guide for the CRISC certification
- FAIR Institute — fairinstitute.org — free resources for quantitative risk analysis
- CISA Risk Management Resources — cisa.gov/risk-management — US government free guidance
- OWASP Risk Rating Methodology — practical risk scoring for application security contexts
- bemitechsolutions.com — cybersecurity training, risk management guides, and ebook library

## RISK REGISTER AUDIT CHECKLIST

Use this checklist to assess whether your risk register meets the requirements of ISO 27001, SOC 2, and most regulatory frameworks. Auditors will verify these items — ensuring you can demonstrate compliance before the audit saves significant time and cost.

### REGISTER DESIGN & METHODOLOGY

- & Risk appetite is formally documented and board-approved
- & Risk scoring methodology is defined with written likelihood and impact scales
- & All risk categories are represented (cyber, operational, compliance, financial, third-party)
- & Asset inventory exists and is linked to risk entries
- & Risk identification method is documented for each register entry

### RISK ASSESSMENT QUALITY

- & Inherent risk scores are separated from residual risk scores for all entries
- & Controls are listed for each risk with effectiveness ratings
- & All risks are assigned a named owner (individual, not team)
- & Scoring is consistent — same risk rated the same by different assessors
- & High and critical risks have documented treatment plans with deadlines

### GOVERNANCE & REVIEW EVIDENCE

- & Risk register reviewed at minimum quarterly (date-stamped records retained)
- & Risk owners have formally acknowledged and accepted their assigned risks
- & Board/risk committee has received at least one risk report in the past 12 months
- & KRIs are defined for top risks with documented thresholds
- & Post-incident reviews have resulted in register updates where applicable

### COMPLIANCE & THIRD-PARTY

- & ISO 27001 Annex A mapping completed (Statement of Applicability in place)
- & Critical vendor risk assessments completed and dated within the past 12 months
- & Data processing agreements in place for all Tier 1 and 2 vendors
- & Regulatory notification obligations documented for high/critical risks
- & Risk register version history retained for audit evidence

## INDUSTRY-SPECIFIC RISK CONSIDERATIONS

While the risk management process is universal, the most critical risks vary significantly by industry. Tailor your risk identification workshops and risk categories to reflect your sector's specific threat landscape, regulatory environment, and operational dependencies.

### Financial Services

Fraud, market manipulation, DORA compliance, third-party concentration risk, algorithmic trading failures, AML/KYC process gaps. High regulatory scrutiny.

### Healthcare

Patient data breaches, ransomware on clinical systems, HIPAA non-compliance, medical device vulnerabilities, supply chain (pharma/device vendors).

### Retail & E-Commerce

PCI DSS compliance, payment fraud, DDoS on peak trading days, customer PII exposure, third-party checkout scripts (Magecart-style attacks).

### Critical Infrastructure

OT/ICS vulnerabilities, nation-state threats, NERC CIP (energy), physical-cyber convergence, cascade failures, long recovery windows.

### Technology / SaaS

Code pipeline compromise (supply chain), API security, multi-tenant data isolation, uptime SLA risk, AI model integrity, open source dependencies.

### Professional Services

Client data confidentiality, credential theft, ransomware (high-value target), conflict of interest, regulatory advice liability, remote workforce.

## RISK REGISTER IMPLEMENTATION ROADMAP BY MATURITY

Where you start depends on where you are. Use this roadmap to find your current maturity level and identify your priority next steps. Every organization at every level can build toward optimized risk management incrementally.

### IF YOU HAVE NO RISK REGISTER YET — START HERE

- Week 1: Define scope (cyber risk only, or enterprise-wide?). Choose tool (start with Excel).
- Week 2: Hold a 2-hour risk identification workshop with IT, compliance, and a business lead
- Week 3: Score all identified risks using a simple 5×5 qualitative matrix
- Week 4: Assign owners to top 10 risks. Document response strategies for high/critical.
- Month 2: Present to leadership. Get sign-off on risk appetite. Schedule quarterly review.
- Month 3: Add KRIs for top 5 risks. Begin vendor inventory for TPRM.

### IF YOU HAVE A BASIC REGISTER — LEVEL UP HERE

- Add quantitative scoring (ALE/SLE) for your top 5 critical risks
- Implement a GRC platform to replace spreadsheets and enable workflow
- Define formal KRI thresholds and automate monitoring where possible
- Expand to all risk categories — most basic registers only cover IT risk
- Establish a formal risk committee with documented terms of reference
- Begin continuous vendor monitoring for Tier 1 suppliers