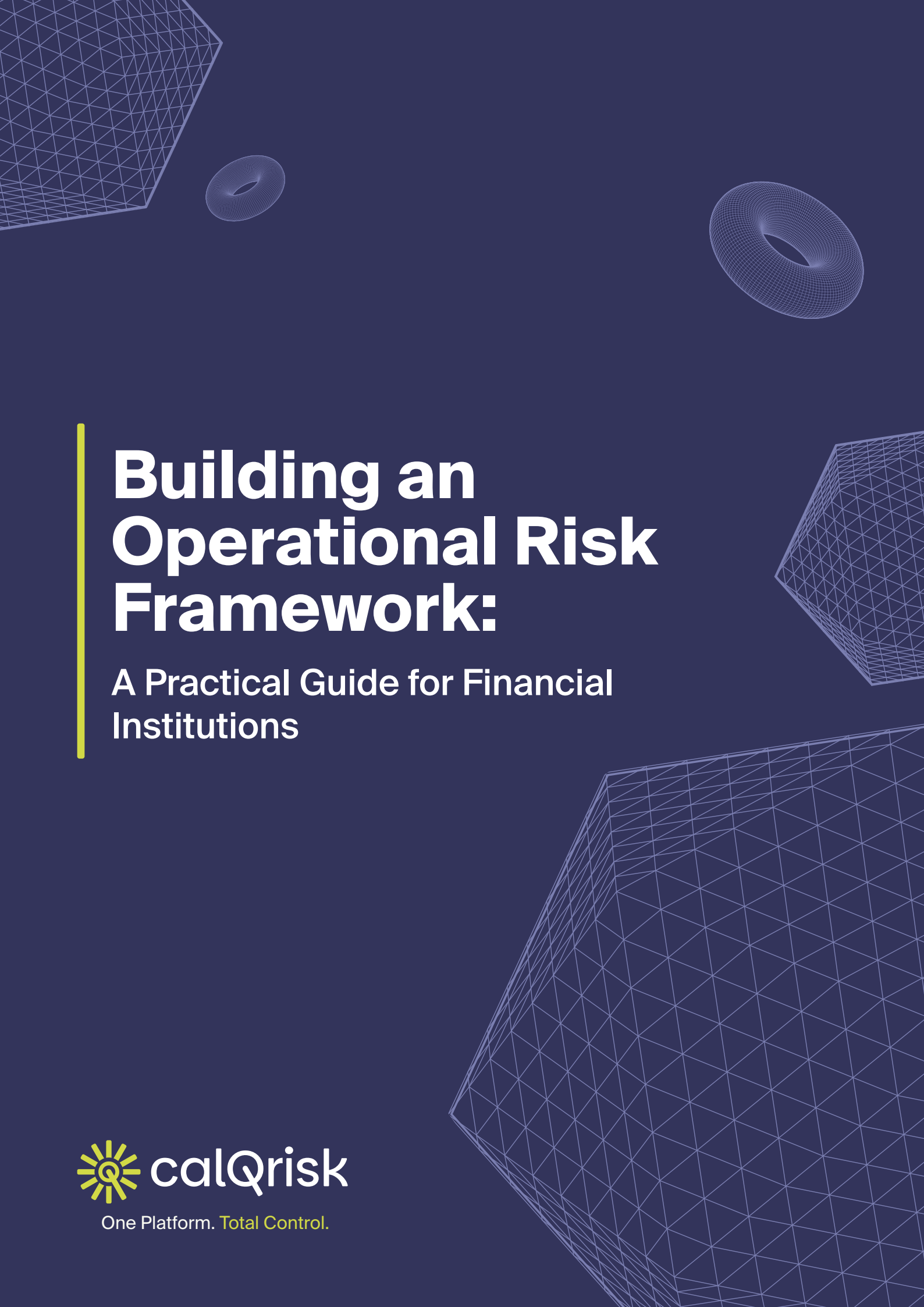
Building an Operational Risk Framework:

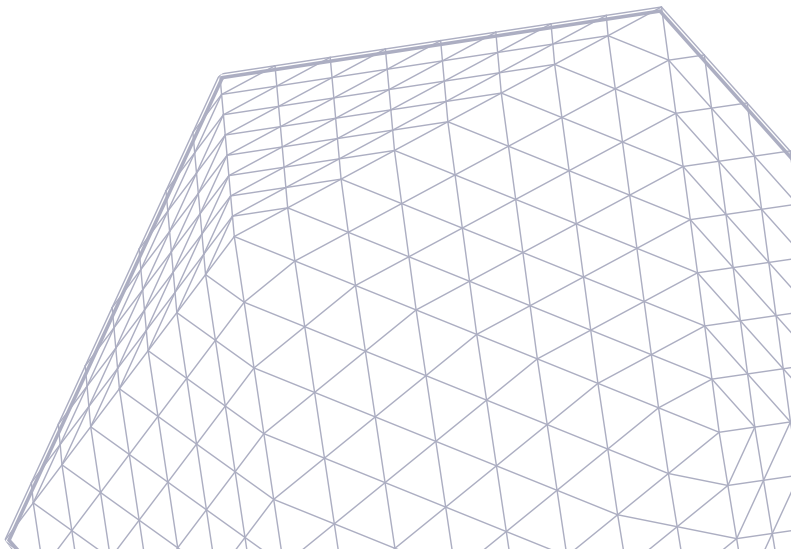
A Practical Guide for Financial Institutions



calQrisk

One Platform. Total Control.

Content



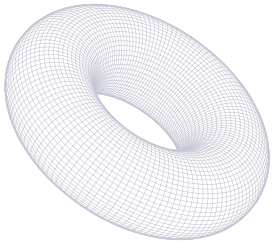
About calQrisk

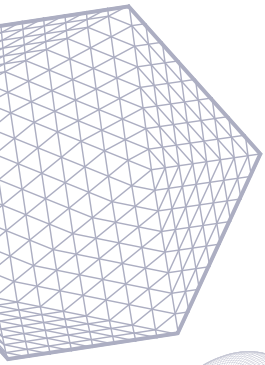
calQrisk is a practical Governance, Risk and Compliance platform created by experienced risk professionals to simplify complex regulatory demands. Built around a connected data model, the platform brings together risk, compliance and governance processes in one intuitive environment.

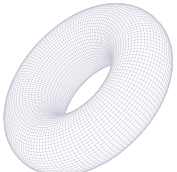
Our modular, scalable software allows organisations to adopt the capabilities they need as their risk maturity develops. Pre-configured frameworks and flexible configuration enable rapid implementation while supporting long-term growth.

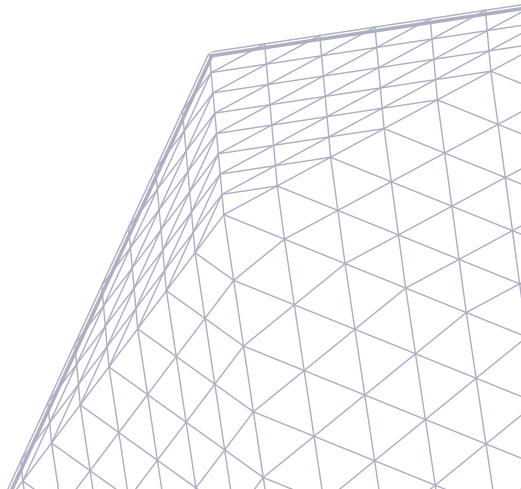
By joining up risks, controls, incidents, third-party oversight and reporting, calQrisk provides clear, real-time insight into how risk is managed across the organisation. This reduces manual effort, improves transparency and supports stronger decision-making at senior leadership and board level.

Trusted by organisations across financial services, the public sector and other regulated industries, calQrisk can be deployed out of the box or tailored to existing governance frameworks. The result is a more resilient, confident, widespread approach to managing risk and compliance.









calQrisk

One Platform. Total Control.

Executive Summary

The rise of importance in operational risk management has been hard to ignore over recent years – the European Banking Authority recently estimated that total materialised losses from new operational risk loss events reached €17.5 billion in 2023 and increased 23% when compared to the previous year.

This paper aims to outline a sample comprehensive operational risk framework tailored for small-to-mid-sized financial institutions in the UK, Ireland, and the EU. It integrates regulatory requirements across various jurisdictions with practical processes. While some of the regulatory requirements referenced throughout the paper may not be relevant to every firm, the examples described can be applied to almost any financial services firm in any jurisdiction.

Key elements include a clear **governance structure** (Board oversight, risk committees, Three Lines, etc.), **Risk & Control Self-Assessments (RCSAs)**, defined **Risk Appetite** and **Key Risk Indicators (KRIs)**, formal **policy management**, robust **scenario analysis**, rigorous **control testing**, structured **incident management**, operational resilience planning, and strict **outsourcing/third-party risk management**. Throughout, we emphasise proportionality for smaller firms and cite relevant supervisory guidance.

Governance & The Three Lines Model

Effective governance begins with the Board and senior management team setting the "tone at the top". Boards (or governing bodies) must explicitly approve the firm's risk strategy, appetite and tolerance levels while also ensuring adequate resources for risk management.

In practice, first-line management owns daily operations and controls (business / process owners), while second-line functions (risk and compliance function) provide independent oversight and challenge, and third-line (audit) assures the overall framework. This aligns with European Banking Authority (EBA) guidance and UK equivalents - "the business lines... as first line... have appropriate processes and controls... and are subject to monitoring by the independent risk management and compliance function".

In smaller firms, operating a strict three lines model may be more difficult due to resource constraints. For example, the head of risk may also act as the head of compliance, or an external professional services firm may act as the independent internal audit function while fulfilling the role of the third line. Nonetheless, senior management should formally delineate and document these roles, with clear reporting lines to a Risk Committee or the Board. Board committees must receive regular reports on operational risk management, control effectiveness and other relevant management information.

In summary, the three lines are defined below:

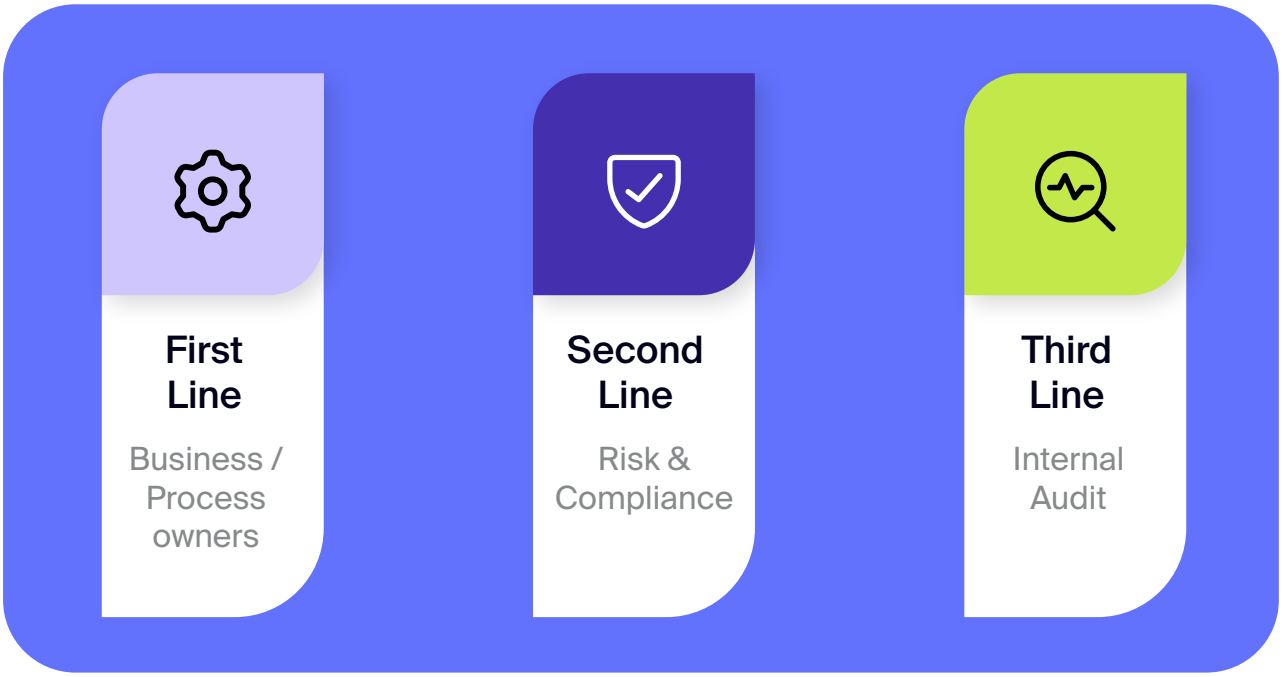
Board / Committee Oversight: The Board must approve high-level risk strategy and appetite / tolerance, including the extent of outsourcing while fulfilling the three lines model. They must regularly review (at least annually) the risk framework, risk appetite statements, and other relevant processes to ensure alignment with the overall risk strategy.

First line: Business / process owners identify and manage risks in their areas on a day-to-day basis, embedding controls into processes. They are accountable for identifying and mitigating risks as they know their business area better than anyone else possibly could.

Second line: The risk management and compliance function(s) are staffed (at least proportionally) to challenge first-line assessments and provide independent monitoring, while also ensuring the risk framework is appropriate for the firm. They review the outputs of risk assessment, propose KRIs, and conduct independent control testing. Even small firms should strive for some independence - e.g. risk officers reporting directly to the board.

Third line: Internal Audit (or outsourced equivalent) provides independent assurance on the first and second lines, testing the effectiveness of controls and governance. In smaller firms, external firms may cover this role. Regular audit reports should feed back into the Risk Committee and Board's agenda.

Regulators explicitly endorse this model. For example, the Prudential Regulation Authority (PRA) states it "expects first line risk ownership, with oversight and challenge by independent second and third lines". The EBA's Internal Governance Guidelines likewise note that firms should align with the three lines model when assigning risk roles. Strong role clarity and documented governance (charters, mandates) are essential. In summary, small firms should set up a scaled 3LoD model with clear ownership, ensure independence of oversight functions, and embed risk governance into regular management processes.



Risk & Control Self-Assessment (RCSA)

Risk & Control Self-Assessment (RCSA) is a cornerstone of operational risk management. It is the process in which each business unit / department identifies its potential risks and the controls in place to mitigate them. The goal is to identify risks, rate their likelihood and impact, determine control effectiveness, and arrive at residual risk levels. This provides all levels within the organisation with a detailed view of risk across the organisation that supports the firm's strategic plan and reassures other stakeholders (e.g. regulators) of a robust control environment.

Key steps in an effective RCSA process include:

Define Scope & Objectives: Determine which processes or units will be assessed (often starting with highest-volume or highest-risk areas). Clarify objectives (e.g. operational resilience, compliance).

Risk Identification: Workshops or questionnaires engage risk owners to list risks. This should cover the likes of people, processes, systems, third-parties, and external events including climate.

Assessment & Rating: For each risk, assess inherent impact and likelihood (often on a 1–5 scale). Document potential impact (financial loss, service disruption, regulatory impact, reputational damage). This should be done in line with the firm's risk criteria or risk impact matrix.

Control Identification: List existing controls that mitigate each risk together with ownership, control type, systems and other relevant information as deemed appropriate.

Control Evaluation: Rate controls for design effectiveness and operational effectiveness (e.g. strong, adequate, weak). Evidence of testing or past incidents may inform this and should be logged alongside the control information.

Residual Risk & Risk Treatment: Determine the residual risk after controls. If residual risk exceeds the firm's appetite, identify actions. This could be strengthening controls or introducing new controls (Treat). Alternatively, a firm may Tolerate the risk and decide against introducing new controls due to resource constraints, risk levels, etc.

Documentation: Maintain a risk register or database capturing risk descriptions, assessments, controls, and associated action plans. Ideally, this should be flexible enough to satisfy stakeholders at all levels, both inside and outside the organisation.

Review Triggers: Establish triggers for a risk assessment refresh. For example, changes in regulation, new product / service, control failures, audit outcomes or on a time-based cycle.

Throughout, the first line should lead the RCSA process with support and challenge from the second-line team. The second line should sample and validate results, appropriately challenge ratings and ensure consistency across the firm.

In summary, conducting RCSAs is the bare minimum in the eyes of the regulators. It is what firms do after the RCSA exercise that shows how impactful the RCSA really is – moving from a 'tick box' exercise to RCSAs impacting strategic decisions can be difficult, particularly in smaller firms. However, the benefits far outweigh the costs to remedy and / or regulatory sanction.

Control Testing

A logical follow on from a robust RCSA process is control testing. Testing controls verifies that they actually work in reality. In practice, firms should review both the design effectiveness and operating effectiveness of controls.

A practical framework includes:

Control Library:
An outcome of the RCSA process should be a comprehensive control library. Key pieces of information should be logged for each control including control type, frequency, owner and failure mode.

Risk-based Prioritisation:
For most firms, it's not plausible to test every single control on an annual basis. Instead, firms should identify their key controls. This may be done by identifying controls that mitigate high impact risks, ones that are linked to important or critical business services, etc. These may merit a more frequent test than those controls deemed to be not so critical to the firm.

Test Procedures:
Each control test should have a documented plan - what is being tested (control objective), method (e.g. sample transaction review) and criteria for success. Testing can include design effectiveness (whether the control is well designed) and operating effectiveness (whether it is functioning over time).

Documentation:
Firms should record both successful and unsuccessful test results in detail. If a control fails, documenting the finding and severity is key. Many firms will link findings back to RCSAs and this in turn may potentially trigger a risk assessment refresh.

Remediation and Follow-up:
Control failures must be remediated. Owners should implement fixes by enhancing the existing control or introducing a new control and potentially retiring the old control. It is best practice that all remediation plans should have target completion dates and ownership. Best practice indicates that control testing should be repeated once remediation plans have been have been complete.

Continuous Monitoring:
Many firms have introduced automated control monitoring. This is typically easier to achieve for IT-related or tech (e.g. system alerts when transactions exceed thresholds). Manual tests should be supplemented by ongoing checks (e.g. a monthly check by a second person).

Regulatory expectations are rising, and documentation is key. Auditors and regulators expect clear records showing which controls were tested, who tested them, and what was found. In summary, control testing closes the loop on RCSAs and is critical to demonstrating to supervisors that controls are not just documented but proven to actually work.

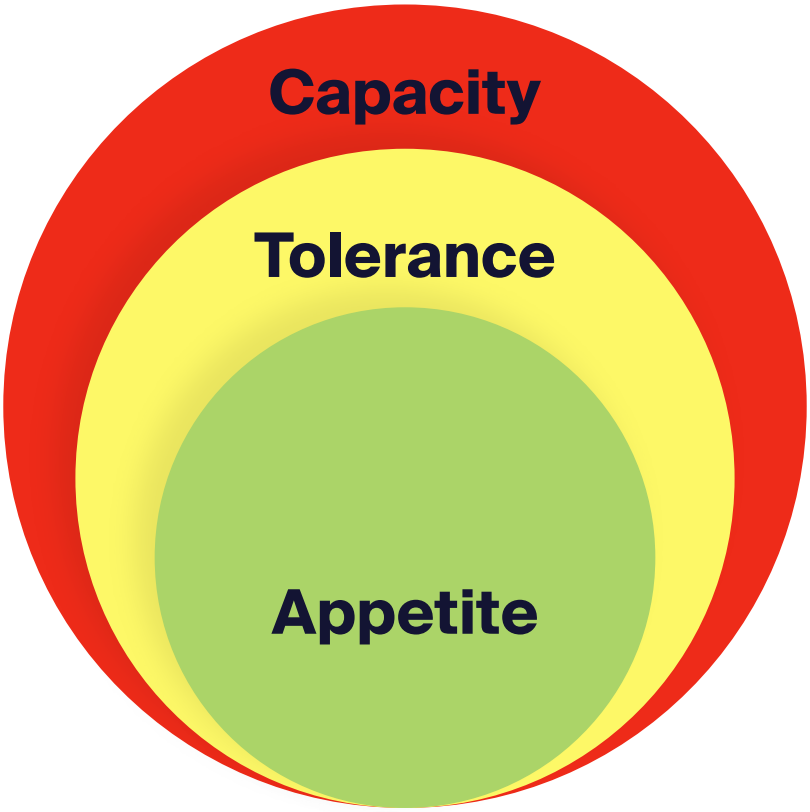
Risk Appetite

A clear Risk Appetite defines “the amount and type of risk an organisation is prepared to pursue, retain or take” (ISO 31000) in order to achieve its objectives. Typically, boards are required to formalise this appetite and ensure the organisation stays within it. In practice, operational risk appetite may include quantitative limits (e.g. number and length of system outages, total lost due to incidents, etc.) and qualitative boundaries (e.g. no material compliance breaches). The Board should calibrate these metrics in line with the firm’s strategy. For example, this could be done using historical loss data and scenario stress tests to set tolerances. Once established, risk appetite and tolerance should be communicated throughout the organisation. It is good practice for the Board to periodically review the firm’s risk appetite, for example, this could be on an annual basis and / or as part of the creation of a new strategic plan.

Risk Appetite is linked to Key Risk Indicators (KRIs). These are usually measurable metrics that indicate how the firm operates versus the board approved risk appetite. KRIs act as early-warning triggers designed to flag rising risk exposures and potential breaches of the risk appetite. For each risk appetite statement (e.g. low appetite for IT outages impacting our customers), corresponding KRIs should be identified and threshold levels set.

Design and management of KRIs should follow these best practices:

In summary, the risk appetite framework ensures that all risk-taking is bounded and monitored. As per Basel guidance notes, the Board should explicitly define the risk tolerance and how it keeps risks within it. KRIs operationalise this framework by continuously measuring where the firm stands relative to those limits.



KRI	Frequency	Risk Levels	Amber - Plan	Red - Plan
Key System Uptime	Monthly	<96% 97% - 98% >99%	Prepare report on options for the Board and call meeting within 3 days of breach	Trigger BCP to ensure customer service is maintained where possible

Policy Management

Comprehensive policies and procedures underpin all operational risk activities. Each individual policy addresses an area of risk. They are often the starting point of any audit or regulatory inspection and can be invaluable for demonstrating compliance with regulatory requirements and a vital component in establishing a robust control environment.

A robust policy management process should include:

Policy Creation: Policies are drafted by the relevant function or specialist and approved by the Board or senior management team. The policy owner (typically a senior manager within the firm) and sponsor must be identified. For example, the Operational Risk Policy might be owned by the Chief Risk Officer, Head of Risk or equivalent.

Documentation and Approval: Each policy should document its purpose, scope, and key requirements. The governing body (Board or relevant Committee) formally approves new policies or major updates.

Version Control & Register: Maintain a centralised policy register with clear version numbers and review dates. Every new version should be date-stamped and old versions archived for audit.

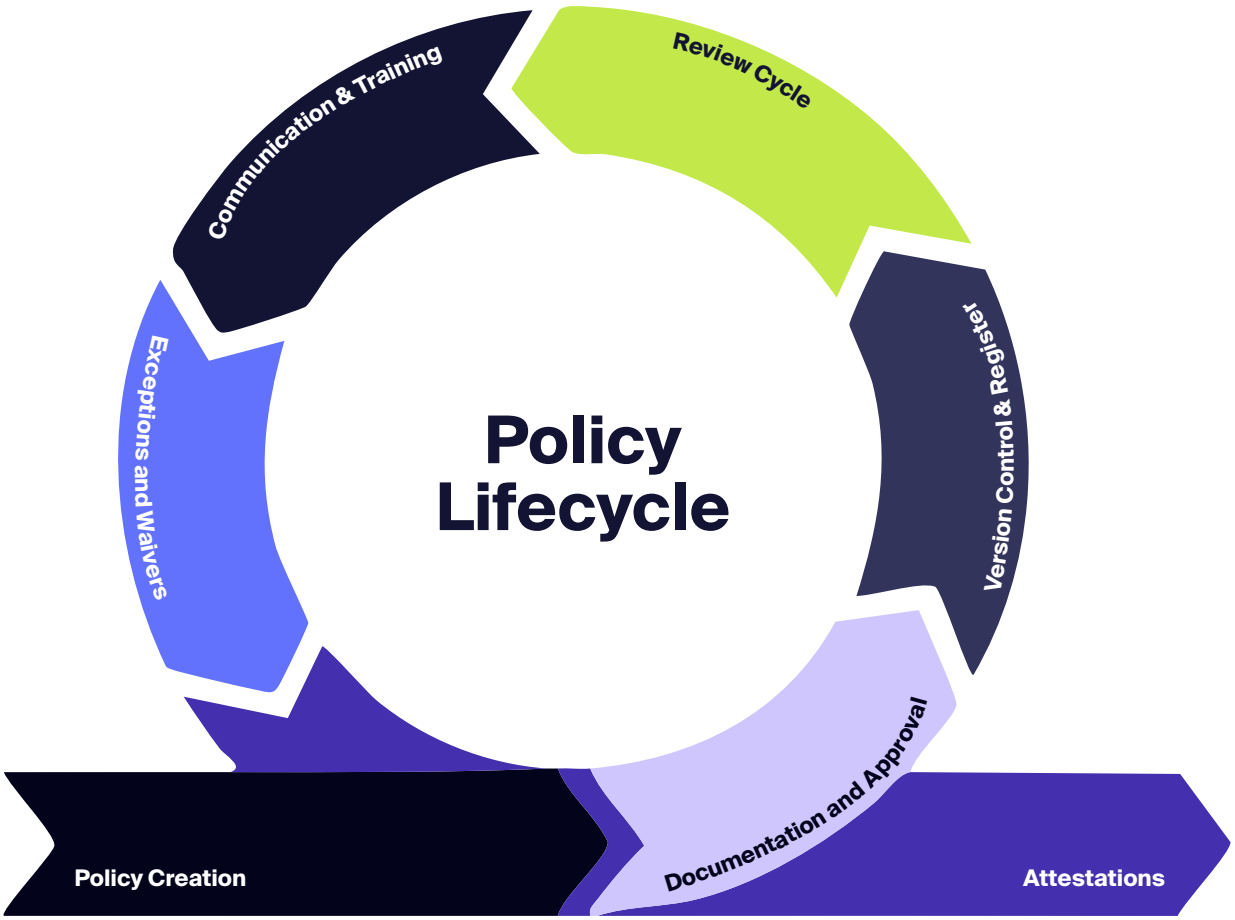
Review Cycle: Policies should have scheduled reviews or be reviewed when triggered by significant changes (e.g. new regulations, major incidents, business changes). A review plan ensures no policy lapses go unnoticed.

Communication & Training: Upon issuance or update, policies must be communicated to all relevant staff. This often involves mandatory training or attestations. For instance, all employees might be required to confirm (electronically or on paper) that they have read and understood the Operational Risk Policy. Training sessions or e-learning modules reinforce key policy points. This is often a key point flagged as part of audits and regulatory inspections.

Exceptions and Waivers: A formal exception process should capture any approved deviations from policy. Exceptions must be documented, time-bound, and approved at an appropriate level (e.g. senior management or board), with compensating controls identified. Tracking open exceptions and expiration is essential. And confirmation when the expiry date arrives the policy is fully implemented.

Attestations: Senior managers should periodically attest to compliance with key policies in their areas. This cascades accountability and embeds a compliance culture.

In practice, small firms should tailor the policy suite to their size (e.g. combined policies) but still follow formal lifecycle steps. All policy documents should explicitly link back to regulatory requirements (e.g. cite relevant pieces of legislation or regulation) to demonstrate compliance.



Scenario Analysis

Scenario analysis is the practice of envisioning extreme but plausible events to test resilience and estimate potential losses. While many firms conduct these exercises for regulatory reasons (e.g. ICAAP), they are extremely useful from an operational resilience perspective also.

Key aspects include:

Scenario Selection: Identify severe operational risk events (internal or external) that could impact objectives. Typical examples include a large cyber-attack, pandemic-like absenteeism or a failure of a third-party provider. Scenarios should be severe but plausible and can be often inspired by past industry events. In fact, some firms often conduct these exercises after a regulatory sanction or outage in another firm becomes public.

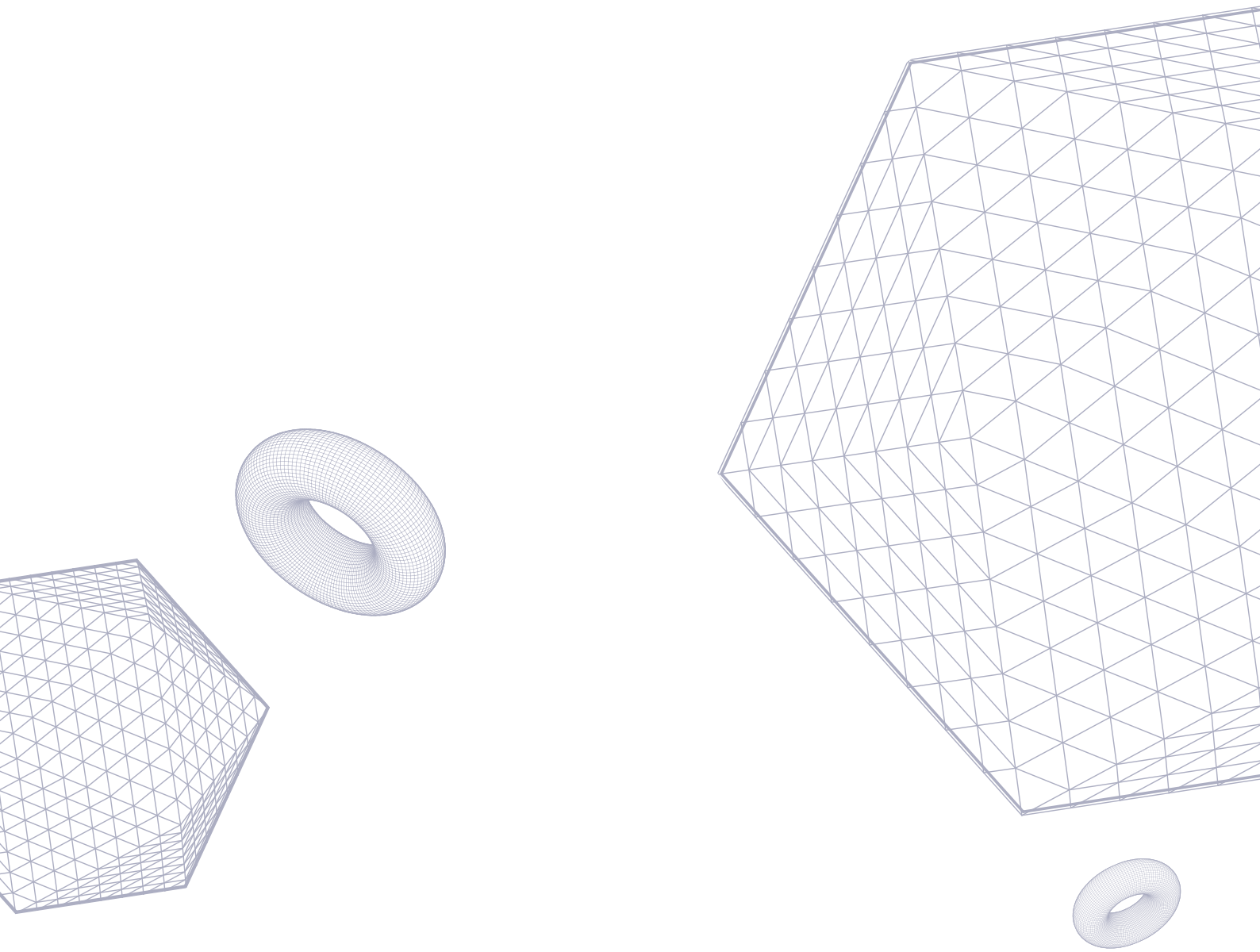
Quantification: For each scenario, estimate the potential impact (e.g. financial loss, reputational damage, operational disruption, regulatory sanction, etc.) and the time to recovery. This may involve conducting workshops with different people within the firm, financial modelling, and gathering / analysing publicly available data, e.g. internal loss data or relevant external statistics.

Integration with Internal Capital Adequacy Assessment Process (ICAAP) / Stress Testing: Larger firms include operational scenarios in ICAAP and firm-wide stress tests. The outputs will feed into capital adequacy calculations and can have significant impacts on the capital a firm is required to hold. Smaller firms might use scenario results more qualitatively, for example, to test the effectiveness of a disaster recovery plan.

Governance: Senior management and the Board (and relevant sub-committees) should endorse the scenario methodology and review scenario outcomes. While they don't necessarily need to review all the information about the scenario, documentation is key when it comes to the assumptions and decisions the scenario is based on.

Documentation and Review: Firms should maintain a comprehensive scenario library with descriptions, assumptions, results and other relevant information. While some firms must conduct scenario analysis exercises on a periodic basis, for those who don't, it's always wise to revisit them periodically anyway – particularly where business or regulatory context shifts. For instance, a change in macroeconomics or technology might prompt vary scenarios analysis exercise.

Supervisory guidelines encourage firms to document scenarios and ensure testing is purposeful. For example, firms should ensure scenario testing of an important service has been performed with impact tolerances in mind and to identify vulnerabilities in time for remediation. Results should be communicated to the Board, with action plans for any identified weaknesses. In summary, scenario analysis embeds forward-looking rigor into the Operational Risk Management Framework.



Incident Management

A formal Incident Management process ensures that operational issues (loss events, control failures, security breaches, etc.) are captured, analysed and addressed systematically.

The typical lifecycle is:

Recording: Promptly record every operational incident or near-miss in a central system or register. Classify incidents by type (e.g. IT outage, fraud, process error) and severity. Even minor incidents ("near misses") should be logged, as they can act as an early warning indicator.

Assessment & Escalation: Assess impact (financial, regulatory, etc.) and urgency. For certain incidents, regulatory rules may require notification to authorities and should be escalated accordingly.

Remediation Plan: It may not be practical to define a remediation plan for every single incident due to resource constraints, severity of the incident and other factors. However, incidents with a higher severity rating should have a remediation plan that outlines both the corrective and preventative actions the organisations is taking.

Tracking & Closure: Monitor the remediation plan progress and only close an incident once all actions are completed and validated.

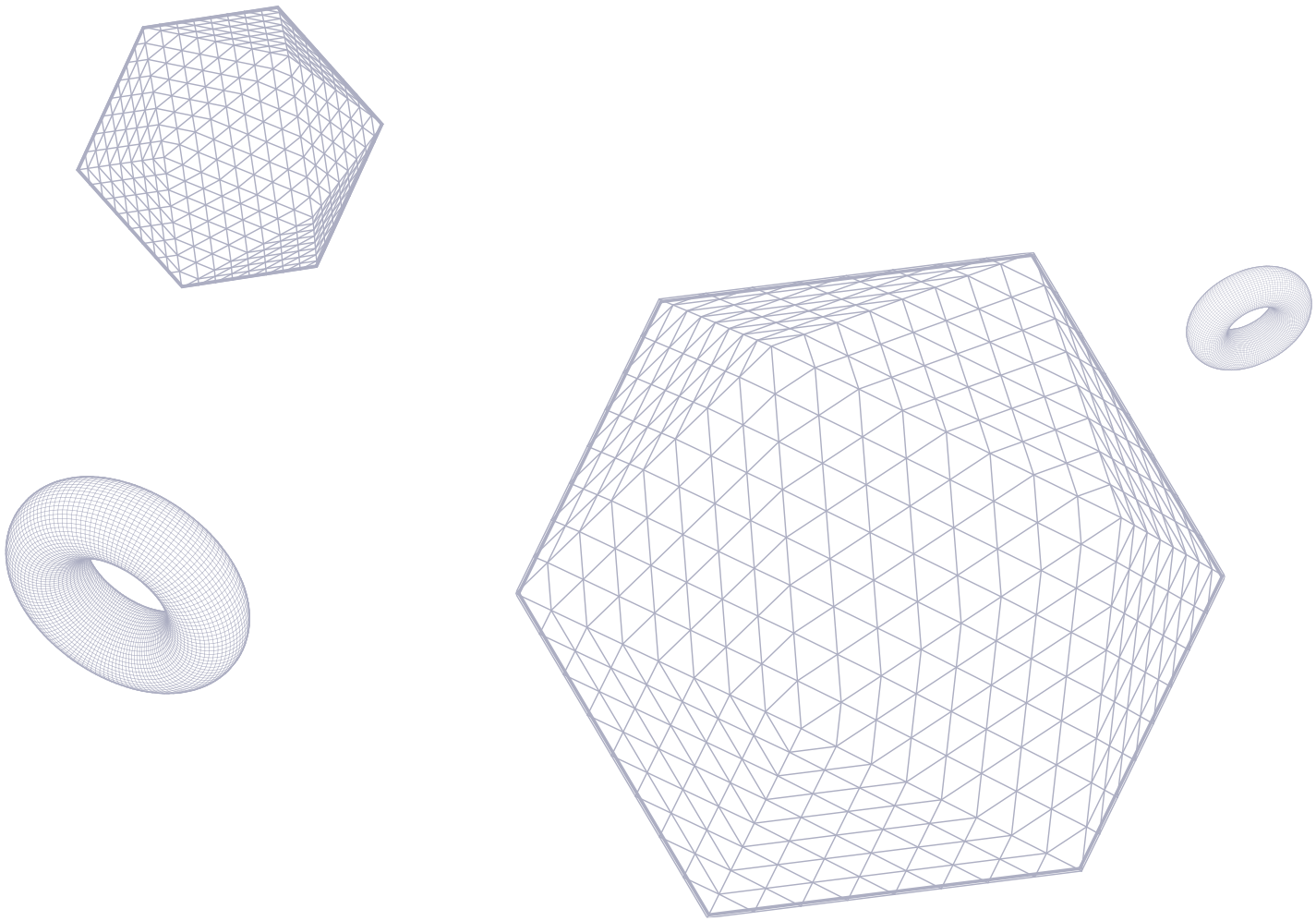
Reporting: Maintain regular management reports on incidents (e.g. by category and severity). Highlight any "near misses" that could have escalated. Report any major incidents to the Board and regulators as required.

Root-Cause Analysis (RCA): Investigate each incident to identify underlying causes (using techniques like "5 Whys" or fishbone diagrams). Determine which control(s) failed or what weakness was exploited and define a root cause for each incident.

Lessons Learned: Periodically review incident trends and RCA insights at risk or audit committee meetings. Document "lessons learned" and integrate them into RCSAs, control enhancements, or scenario updates. When designing and implementing your third-party risk management programme.

As mentioned above, certain incidents must be reported to regulatory authorities depending on the jurisdiction in which you operate. For example, under the EU Digital Operational Resilience Act (DORA), firms must report major ICT-related incidents to their competent authority if thresholds are exceeded. The technical standards require an initial notification within 4 hours of detection and detailed follow-ups within 24 hours. Similarly, in the UK, the FCA and PRA also impose incident reporting requirements. Firms should therefore define criteria for “reportable” incidents (based on volume, customer impact, etc.) and ensure compliance with these timelines.

Overall, a rigorous incident management process helps to contain any damage while also feeding continual improvement.



Outsourcing & Third-Party Management

Many operational risks crystallise through outsourcing and third-party relationships.

Firms must manage these risks via comprehensive governance and controls as outlined below:

Policy and Register: Maintain an up-to-date register of all outsourcing and material third-party relationships. Define materiality criteria to identify which arrangements warrant more stringent oversight than others. This, and more, should all be laid out in a robust board-approved outsourcing policy.

Due Diligence: Before entering or renewing contracts, conduct risk assessments and due diligence on third parties (financial stability, controls, regulatory compliance, etc.). Most firms will apply a risk-based approach here and have a more robust due diligence process for key service providers / outsourced functions and new third parties.

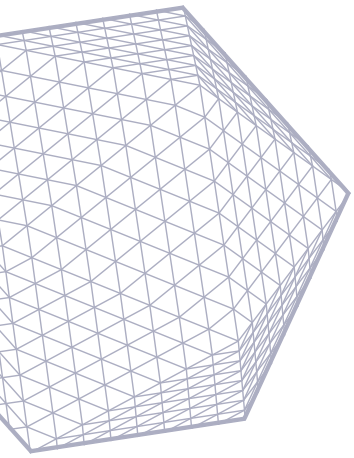
Contracts: Material outsourcing agreements must cover key items such as defined service levels, access and audit rights, data security, exit strategies, business continuity, and (for critical functions) resolution clauses.

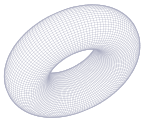
Ongoing Monitoring: Establishing a third-party monitoring programme is often overlooked by firms once due diligence is complete. Collecting KPIs from service providers and tracking them against agreed thresholds is not only good practice, it's also a regulatory requirement in many jurisdictions. Conducting periodic audits or control assessments of vendors can be useful for more material vendors where service disruption is expected should they have an outage.

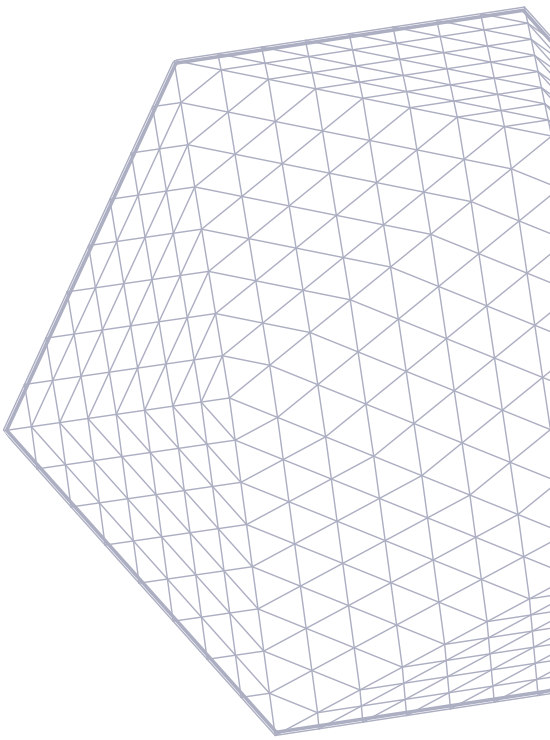
Incident Handling: Contracts and processes should require vendors to report incidents promptly. The firm's incident response plan must include third-party failures. Major ICT incidents at vendors (e.g. cloud outages) may trigger the same reporting obligations as internal incidents (per DORA).

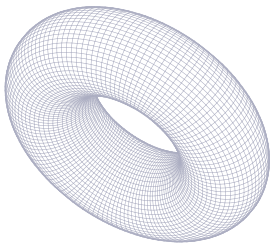
Regulatory Alignment: While the effective management of third parties is good for business, it is also a regulatory requirement in pretty much all jurisdictions too. Adhering to the likes of DORA, EBA Guidelines on the Sound Management of Third-Party Risk, FCA and PRA requirements should all be taken into consideration when designing and implementing your third-party risk management programme.

In summary, outsourcing risk management has an end-to-end lifecycle - from initial assessment and contract negotiation, through continuous monitoring, to exit planning. The focus should be on critical services and high-impact vendors. Documentation should cover risk assessments, decision to outsource or accept risk, and supplier performance reviews. Sound third-party governance is vital for compliance (PRA/FCA expect this), and to protect the firm's customers and stability.









Conclusion

In today's complex landscape, even smaller institutions face significant operational risks. The framework covered in this paper – combining governance, RCSA, risk appetite, policies, scenario analysis, control testing, incident management, resilience, and outsourcing oversight – provides a structured approach to manage those risks end-to-end.

Key recommendations include:

Board Engagement: Ensure the Board explicitly sets risk appetite, approves assessment methodologies, regularly reviews resilience metrics and approves the ownership for each required workstream.

Proportionality: Scale all the processes included in this paper to suit the needs of your own firm. For example, a mid-sized bank may have a dedicated risk team whereas a smaller firm might combine risk, compliance and outsourcing.

Documentation & Metrics: Build a strong documentation culture. Maintain clear records (e.g. RCSA register, incident log, policy attestations) to demonstrate to regulators that processes are real and ongoing.

Continuous Improvement: Treat operational risk management as dynamic. Update risk registers with new risks, adjust KRIs as business changes, and refresh scenarios after actual disruptions.

Regulatory Awareness: Stay abreast of evolving rules and align internal frameworks accordingly.

Regulatory expectations around operational risk and resilience are only rising. Firms that build and maintain this framework will be better prepared for disruptions and supervisory scrutiny. By integrating best practices with the applicable regulations – from the FCA Handbook to EBA guidelines and DORA – small and mid-tier firms can achieve a robust yet proportionate operational risk programme.

calQrisk

One Platform. Total Control.

Contact Us +353 61 477 888 www.calQrisk.com in @calQrisk resilience@calQrisk.com