SAI360
CONNECTED ETHICS RISK & COMPLIANCE

Managing Operational Risk in 2026: From Compliance to Operational Resilience

Navigating Interconnected Risk, AI Governance, and Proof-Based Regulatory Compliance

Executive Summary

As organizations navigate 2026, operational risk management (ORM) has undergone a fundamental transformation. What was once treated as a defensive compliance discipline focused on preventing isolated operational failures has evolved into a strategic business capability that enables operational resilience. Today's hyper-connected business ecosystem means that cyber intrusions, third-party vendor outages, regulatory shifts, and rapid AI adoption no longer occur in isolation; they cascade and amplify one another across enterprise value chains.

Global regulatory authorities have responded accordingly. Mandates across Europe, the United Kingdom, Australia, and North America have shifted their focus from asking whether firms have documented policies to requiring demonstrable evidence that critical business services can withstand severe operational disruption.

This eBook explores the operational risk trends shaping 2026 and provides practical strategies to help risk leaders, compliance officers, and executive boards strengthen operational resilience through a more integrated approach to risk management.

1. The Era of Interconnected Risk Convergence

Operational risk management has traditionally focused on responding to isolated events such as technology outages, third-party disruptions, or compliance breaches. Today, these risks rarely occur in isolation. Cyber threats, third-party failures, regulatory change, and emerging technologies increasingly intersect, creating cascading operational impacts across the enterprise.

Key Industry Realignment:

In 2026, operational risk management is no longer merely a defensive compliance exercise. It has evolved into a strategic business capability that enables operational resilience and supports long-term business performance.

CASCADING IMPACT PATHWAYS

A disruption involving a critical technology provider can trigger cascading operational, regulatory, financial, and reputational impacts across the enterprise. Understanding these interconnected effects is essential to building operational resilience:

1. Critical customer: Critical business services and customer-facing applications become unavailable, disrupting core operations and degrading the customer experience.

2. Regulatory Exposure: Non-compliance with strict downtime tolerances triggers mandatory notification timelines and regulatory penalties.

3. Reputational Damage: Customer dissatisfaction and public scrutiny can erode brand trust, increase customer attrition, and negatively impact market confidence.

4. Third-Party Liability: Fourth-party and subcontractor failures expose hidden dependencies and increase operational risk across the extended enterprise.

THREE IMPERATIVES FOR ENTERPRISE LEADERSHIP

To strengthen operational resilience in an increasingly interconnected risk landscape, organizations should focus on three foundational operational risk management principles:

- **Operational Resilience by Design:** Moving from legacy, rigid core architecture toward resilient, fault-tolerant modular architecture capable of absorbing unexpected shocks.
- **Continuous Risk Monitoring:** Replacing static, binder-based disaster recovery plans with live failover mechanisms and continuous scenario testing.
- **Connected Risk Governance:** Establishing multi-channel crisis communication protocols to maintain trust with customers, regulators, and financial markets during an event.

2. The 2026 Operational Risk Landscape

Operational disruptions continue to increase in frequency and complexity, exposing organizations to financial loss, regulatory scrutiny, reputational damage, and prolonged business disruption. Understanding these interconnected risks is essential to strengthening operational resilience and prioritizing mitigation efforts before disruptions occur.

Top Operational Risks Matrix for 2026

The table below outlines the primary risk domains facing organizations in 2026, their emerging threat vectors, and recommended focus areas for risk mitigation.

Risk Domain	2026 Threat Description	Strategic Risk Response
Advancing Cybercrime & Ransomware	AI-driven attacks targeting core infrastructure, software supply chains, and data integrity.	Zero-trust architecture, automated threat intelligence, and continuous control monitoring.
AI & Generative Technology Risk	Unsanctioned "Shadow AI" usage, model bias, toxic training data, and data privacy leaks.	Enterprise AI governance frameworks, AI risk registers, and employee usage policies.
Extended Supply Chain Dependency	Deep, unmapped fourth- and N-party vendor dependencies creating hidden single points of failure.	Dynamic dependency mapping, real-time vendor risk telemetry, and contractual SLAs.
Critical Business Service Failure	Inability to maintain operational delivery within strict, time-bound impact tolerances.	End-to-end service mapping, outcome-based stress testing, and real-time failovers.
Regulatory & Enforcement Pressure	Heightened scrutiny with direct executive accountability for operational non-compliance.	Automated regulatory change tracking, policy lifecycle management, and proof-based audit trails.

3. Global Regulatory Evolution: From Policy to Proof

Regulators across major financial and commercial jurisdictions are shifting beyond policy documentation to require organizations to demonstrate operational resilience through measurable evidence. Organizations must not only define controls, but also prove they can withstand and recover from operational disruption.

GLOBAL REGULATORY ALIGNMENT IN 2026

EUROPE (DORA / NIS2)
- Mandatory cyber testing
- Strict vendor oversight
- 24-hr incident reporting

UNITED KINGDOM (FCA / PRA)
- Defined impact tolerances
- Important business services
- Annual self-assessments

AUSTRALIA (APRA CPS 230)
- Integrated ORM frameworks
- Service provider management
- Comprehensive risk registers

NORTH AMERICA (OCC / FED)
- Focus on critical service providers
- Third-party risk baselines
- Executive board accountability

Key Regional Mandates

EUROPE: DIGITAL OPERATIONAL RESILIENCE ACT (DORA) & NIS2 DIRECTIVE

- Strengthens digital operational resilience requirements for financial entities and critical infrastructure organizations.
- Enforces standardized major incident notification timelines (initial notification within 24 hours).
- Mandates threat-led penetration testing and third-party risk management for critical ICT providers.

UNITED KINGDOM: FCA/PRA OPERATIONAL RESILIENCE POLICY

- Requires firms to identify important business services that, if disrupted, could cause intolerable harm to consumers or market stability.
- Mandates firms to set explicit Impact Tolerances and demonstrate they can operate within them under severe but plausible scenarios.

AUSTRALIA: APRA CPS 230 (OPERATIONAL RISK MANAGEMENT)

- Integrates operational risk management, business continuity, and third-party oversight into a unified operational resilience framework.
- Holds boards directly responsible for overseeing operational risk profiles and approving resilience strategies.

NORTH AMERICA: INTERAGENCY GUIDANCE & REGULATORY ALIGNMENT

- U.S. banking agencies (OCC, Federal Reserve, FDIC) continue to intensify oversight surrounding third-party risk management and operational resilience standards.
- Emphasizes baseline operational resilience expectations for large financial institutions and their critical third-party service providers.

4. Governance in the Age of AI and Risk Convergence

Effective governance in 2026 requires more than passive oversight. Executive boards and executive leaders need integrated visibility into how technology, third-party relationships, and business operations intersect to make informed, risk-based decisions.

Integrating AI Governance into the GRC Framework

With the rapid proliferation of Generative AI tools and automated decision engines, organizations face new vectors of operational risk. AI governance can no longer operate in a technology silo; it must be embedded directly into core Enterprise Risk Management (ERM) programs.

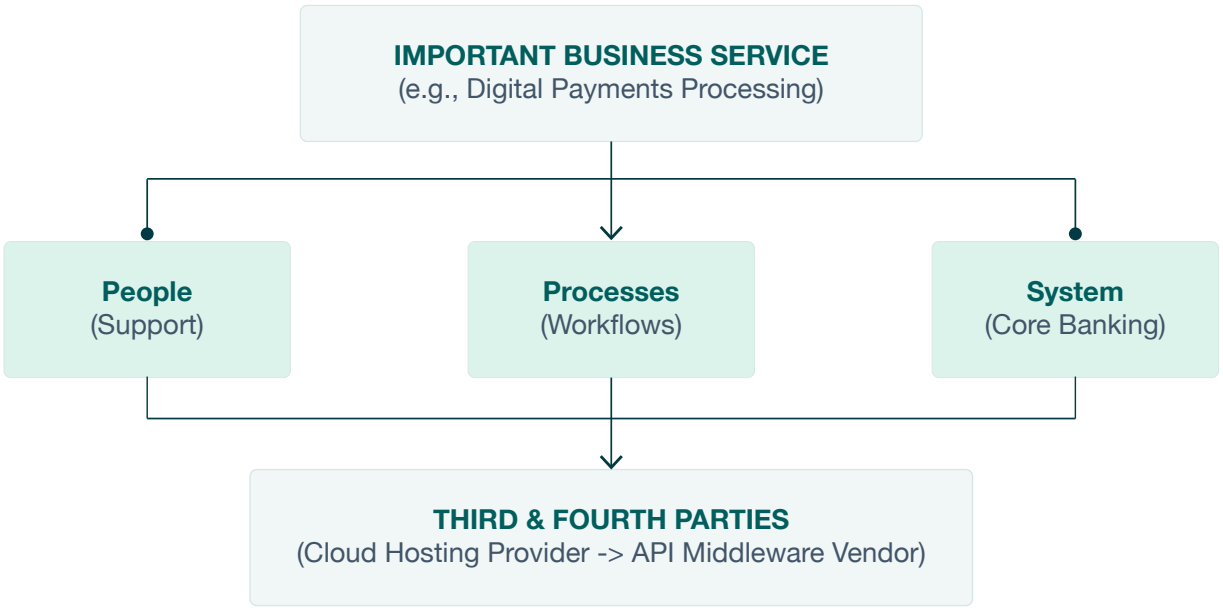
GOVERNANCE PRIORITIES FOR 2026:

- **Define Explicit Accountabilities:** Assign clear operational risk ownership at both board committee and executive management levels.
- **Implement Real-Time Executive Dashboards:** Replace periodic paper reporting with live dashboards that aggregate operational risk indicators, incident status, and compliance metrics.
- **Establish an AI Risk Oversight Committee:** Monitor AI deployment across the organization, ensuring data privacy compliance, model validation, and mitigation of "Shadow AI."
- **Align Governance Structures with Regulatory Evolution:** Conduct bi-annual reviews of corporate governance policies to maintain alignment with shifting global standards.

5. Modern Resilience: Replacing Static Recovery Plans

Disaster recovery binders and static spreadsheets are incapable of supporting modern operational resilience requirements. Organizations must transition toward active, data-driven resilience models built around critical business services.

END-TO-END CRITICAL BUSINESS SERVICE DEPENDENCY MAP



Defining Multi-Dimensional Impact Tolerances

Impact tolerances define the maximum level of disruption an organization is willing to accept before critical business services are materially affected. Leading organizations assess these impacts across four key dimensions:

- **Consumer Harm:** Assessing potential financial loss, inability to access funds, or data vulnerability experienced by end customers.
- **Financial Loss:** Quantifying direct revenue loss, contractual penalties, and recovery expenditures.
- **Market & Systemic Impact:** Measuring secondary systemic impacts on interconnected financial or market ecosystems.
- **Reputational Damage:** Evaluating brand sentiment, client attrition risks, and public confidence fallout.

6. Enterprise Dependency Management: Managing N-Party Risk

Modern organizations increasingly rely on third parties, SaaS providers, and cloud infrastructure to deliver critical business services. While operational activities can be outsourced, accountability for managing operational risk and resilience remains with the organization.

Vendor Risk Management Best Practices Checklist

- **Dynamic Inventory Management:** Maintain a centralized, continuously updated register of all material third-party and fourth-party relationships.
- **Contractual SLA Enforcement:** Embed legally binding Service Recovery Time Objectives (SRTOs), security standards, and mandatory incident notification windows into vendor agreements.
- **Integrated Risk Intelligence:** Combine internal vendor assessment questionnaires with automated external threat telemetry and continuous security rating feeds.
- **Fourth-Party Mapping:** Identify critical subcontractors relied upon by key vendors to eliminate unmonitored concentration risks.
- **Joint Resilience Testing:** Include tier-1 technology partners and material vendors in annual joint scenario testing.

7. Scenario Testing as Empirical Proof

Regulators increasingly expect organizations to move beyond tabletop exercises and demonstrate operational resilience through realistic, multi-scenario stress testing. These exercises validate an organization's ability to withstand, respond to, and recover from operational disruption.

The Operational Resilience Lifecycle

Recommended Test Scenarios for 2026

1. Ransomware Event on Critical Infrastructure: Simulating severe malware infection on primary transaction databases alongside secondary cloud backup corruption.

2. Major Cloud Provider Outage: Testing failover processes during an extended regional outage affecting primary SaaS or hosting vendors.

3. Simultaneous Cyber Attack & Supply Chain Failure: Evaluating cross-functional incident response when a core vendor suffers a data breach during an active internal IT disruption.

8. SAI360's Unified Approach to Integrated Risk & Compliance

Managing operational risk in today's interconnected environment requires a unified view of risk across the enterprise. Fragmented systems and disconnected data create blind spots that limit visibility, slow decision-making, and weaken operational resilience.

SAI360 helps organizations replace fragmented point solutions with a connected GRC platform that brings operational risk, compliance, cyber risk, third-party risk, business continuity, and ethics together in a single source of truth. With greater visibility across interconnected risks, organizations can make more informed decisions, strengthen operational resilience, and demonstrate compliance with confidence. Visit www.sai360.com to learn more.

SAI360 GRC PLATFORM	
RISK MANAGEMENT SOFTWARE	ETHICS & COMPLIANCE LEARNING
• Enterprise & Operational Risk • IT & Cybersecurity Risk • Third-Party / Vendor Risk • Business Continuity Management (BCM) • Incident & Regulatory Change Mgmt	• Anti-Bribery & Corruption • Data Protection & Privacy • Conflicts of Interest • Code of Conduct & Ethics Training • Harassment Prevention & Culture

Why SAI360 Sets the Standard in 2026

- **Centralized View of Risk:** Consolidates operational risk assessment, incident tracking, vendor risk telemetry, and policy management into a single intuitive view.
- **Operationalize Resilience:** Replace manual, siloed work with connected workflows that help teams identify emerging risks, respond faster, and continuously strengthen operational resilience.
- **Audit-Ready Compliance:** Generates comprehensive reporting and audit trails aligned with DORA, FCA, APRA CPS 230, and U.S. regulatory expectations.

Take the Next Step Toward Operational Resilience

Operational resilience isn't built through disconnected tools or one-time compliance efforts. It requires connected risk intelligence, continuous visibility, and the ability to adapt as your business and regulatory landscape evolve. SAI360 helps organizations bring these capabilities together through a unified GRC platform built for today's interconnected risk environment.

Ready to turn operational risk into resilience?

Request a demo

SAI360
CONNECTED ETHICS RISK & COMPLIANCE

SAI360 is giving companies a new perspective on risk management. By integrating ethics, governance, risk, and compliance within a single platform, SAI360 helps companies broader their risk horizon so they can manage risk from every angle.
Visit sai360.com to learn more.