SAI360
RISK FROM EVERY ANGLE

Best Practices Managing Operational Risk in 2025

Table of Contents

Introduction

Barclays Bank began 2025 on shaky ground, triggering a media frenzy across global news sites; "Barclays digital services go down on payday", "Barclays customers "unable to make payments"".

An IT outage on 31st January had halted the bank's digital services, leaving customers in a state of financial paralysis. With no ability to access mobile and online banking functionalities or make and receive payments, the timing couldn't have been worse—payday for many, and the due date for critical financial obligations like bills and self-assessment tax payments.

Barclays swiftly confirmed that the disruption was not cyber-related, alleviating immediate fears of a data breach. Yet this technical reassurance did little to soothe the mounting frustration of affected customers who formed lengthy queues outside physical branches and took to social media to voice their anguish. Many vowed to terminate their relationship with the bank at the first available opportunity.

Persistent issues plagued customers throughout the subsequent days, and it wasn't until February 2nd that Barclays finally resolved the technical glitch and processed delayed payments.

It will take some time for the full financial and reputational impact of this outage to materialize, but the incident serves as a pertinent reminder of the far-reaching consequences of digital service disruptions, affecting not just an institution but millions of customers relying on timely access to their funds.

Some key lessons emerge:

1. **The need for robust IT infrastructure:** The outage revealed weaknesses in Barclays' core banking systems, emphasizing the importance of resilient, scalable, and fault-tolerant IT architecture.
2. **The importance of contingency planning:** The cascading effects of the disruption highlight the necessity for redundant systems and alternative processing channels to ensure continuity of critical services. Banks must implement failover mechanisms, real-time backup solutions, and cross-functional incident response teams to mitigate extended downtime.
3. **The role of clear communication strategies to maintain trust:** Firms need predefined crisis communication plans, leveraging multiple channels (mobile alerts, website updates, customer service lines, and social media) to keep customers informed and mitigate reputational damage.

The Operational Risk Landscape

Unfortunately, incidents of this nature are not uncommon. A 2024 Cockroach Labs Survey revealed that organizations experience an average of 86 outages annually, with 55% facing weekly disruptions. The financial toll is substantial, with per-outage losses ranging from $10,000 to over $1 million. For large enterprises, the impact is compounded by prolonged recovery times—70% of outages take over an hour to resolve, and nearly half extend beyond two hours.

Beyond direct costs, operational disruptions erode investor confidence. McKinsey's analysis of 500 operational risk events (2006-2020) found equity losses five times greater than direct financial losses.[1] This disproportionate impact on shareholder value reflects a deeper erosion of investor confidence. To some, operational disruptions signal potential systemic weaknesses in a company's risk management frameworks, casting doubt on its ability to navigate future challenges effectively.

Operational resilience is essential for survival, and though firms have made remarkable strides since the pandemic in maintaining service delivery during unforeseen crises, the focus must now shift to creating robust, future-ready strategies. The most successful organizations will reimagine their operations and supply chains, implementing controls informed by detailed operational risk assessments. This will enable institutions to better withstand acute shocks, some of which are highlighted below.

Top Operational Risks	
IT disruption	A disruption in the availability or performance of critical IT systems
Data compromise	The unauthorized access, theft, or loss of sensitive or critical data
Resilience risk	The risk that an organization cannot withstand, recover from, or adapt to adverse events
Third-party risk	The risk posed by external vendors, suppliers, or service providers
Theft and fraud	The intentional act of unlawfully taking or misrepresenting information, assets, or resources
Conduct risk	The risk of unethical, inappropriate, or unlawful behavior by employees or agents
Regulatory risk	The potential for harm due to non-compliance with laws, regulations, or standards
Organizational change	Risks arising from the implementation of significant internal changes
Geopolitical risk	The risk of impact due to political instability, economic sanctions, or conflicts
Employee wellbeing	The risk associated with poor physical, mental, or emotional health of employees

1. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/response-and-resilience-in-operational-risk-events

Global Regulatory Approaches to Operational Resilience

Operational risk management (ORM) and resilience form two interconnected layers of organizational protection. While risk management focuses on preventing disruptions through systematic identification and mitigation of threats, resilience ensures the organization can maintain essential operations when disruptions inevitably occur. Regulators understand this symbiotic relationship, requiring organizations to both proactively manage risks and develop robust recovery capabilities. Key frameworks include:

- **Europe:** Digital Operational Resilience Act (DORA) - aims to strengthen the IT security of financial entities such as banks, insurance companies and investment firms and make sure that the financial sector in Europe can stay resilient in the event of a severe operational disruption. Comparable requirements for cyber-related risk management across all European industries are present within NIS2.
- **UK:** FCA Operational Resilience Act - The Operational Resilience Act was produced in partnership with the FCA, Bank of England and Prudential Regulatory Authority to strengthen the operational resilience of the UK financial sector. The Act aims to ensure that firms can prevent, adapt to, respond to, recover from and learn from operational disruptions.
- **Australia:** APRA CPS 230 - a comprehensive framework for APRA-regulated entities to identify, assess, manage and report on operational risks in a systematic and effective way. It emphasizes the importance of proactive risk identification, robust controls, and transparent reporting and disclosure.
- **Singapore:** MAS Guidelines on Business Continuity Management (BCM) - The Guidelines detail how firms should approach the establishment of policies, plans and procedures to minimize disruptions to critical business services.
- **North America:** Sound Practices to Strengthen Operational Resilience - This document consolidates current regulations, guidelines, and industry norms, offering a holistic strategy for companies to enhance and sustain their operational resilience. At the core of this strategy is the principle of effective governance, which underpins the recommended practices.

U.S. Rules are on the Horizon

Following the publication of the 'Sound Practices to Strengthen Operational Resilience,' U.S. regulators have closely monitored enhancements to resilience requirements in other jurisdictions. Michael Hsu, the Acting Comptroller of the Currency, has hinted at potential changes to the U.S. framework, with a focus on baseline requirements for large banks and critical operations, including third-party providers.[2]

Examining the regulations set by international counterparts reveals a clear alignment in approaches to managing and mitigating risk. U.S.-based firms should prepare for stricter rulemaking focused on identifying critical activities and associated operational risks, setting disruption tolerances, testing resilience, managing third-party risks, ensuring effective stakeholder communication, and reinforcing governance for critical service providers.

Drawing on these frameworks, what follows is an overview of the key requirements. By understanding and aligning with these principles, firms can adopt best practices to mitigate operational risks and enhance their overall resilience, regardless of jurisdiction or industry.

2. https://www.occ.gov/news-issuances/news-releases/2024/nr-occ-2024-23.html

Governance and Accountability

Regulators are unequivocal in their desire for senior management to play an active role in overseeing the development, implementation and continuous refinement of the organization's ORM framework. The interconnectedness of operational risks demands not only a strategic mind, but a degree of technical competence in order to truly understand the mechanisms in which people, processes and systems interact and amplify risk.

It's this level of comprehension that allows senior management to drive the necessary cultural and structural change by prioritizing those investments that enhance resilience and foster a mindset attuned to risk mitigation and adaptability.

Best Practices:

- **Define and document risk management responsibilities** at the Board and senior management levels, ensuring ownership of outcomes.
- **Implement real-time dashboards** to provide senior leadership with actionable insights into technological and operational risks, supporting informed decision-making.
- **Periodically review and update governance structures** to align with risks and regulations as they evolve.

Assess Inherent and Residual Risk for Important Business Services

Regulators consistently define "important" or "critical" business services as those whose disruption could result in intolerable harm to consumers or pose systemic risk to the broader financial ecosystem.

Intolerable harm refers to adverse outcomes from which consumers cannot easily recover. For example, the UK's FCA defines it as a situation where, following a disruption, a firm is unable to restore a client to their correct financial position, or where there are significant non-financial impacts that cannot be effectively remediated.

Systemic risk is the possibility that an event at the company level could trigger severe instability or collapse in an entire industry or economy. It refers to the risk of a breakdown of an entire system rather than simply the failure of individual parts.

Firms must go beyond surface-level mapping, instead documenting detailed and dynamic process maps which illustrate the people, processes, technology, facilities, and information integral to the delivery of each service. Mapping must be end-to-end, capturing not just immediate third-party dependencies but also fourth-party relationships and potential cascading risks within dependency networks.

Once critical services and associated dependencies are mapped, organizations need to assess the impact and likelihood of pre-defined operational risk to determine an inherent risk score. Residual risk should then be calculated by accounting for the efficacy of existing controls.

Best Practices:

- **Identify and document dependencies for all critical services,** including direct and indirect third- and fourth-party providers, to reveal potential single points of failure.
- **Regularly update dependency maps** to reflect changes in operations, technology, supply chains, or third-party relationships, ensuring they remain accurate and actionable.
- **Maintain a dynamic and centralized risk repository** for storing and managing information pertaining to potential operational risks.
- **Prioritize remediation efforts** by residual risk score to focus mitigation efforts on risks posing the greatest threat to the organization, after existing controls are accounted for.

Set and Maintain Impact Tolerances

Regardless of control efficacy, disruptions are inevitable. Impact tolerances serve to quantify the point at which such disruptions would cause intolerable harm to consumers or pose systemic risk. Organizations must consider factors such as consumer impact, financial loss, and reputational damage.

Mature frameworks like DORA emphasize the importance of time-based metrics, such as recovery time objectives (RTOs) or service recovery time objectives (SRTOs), to guide and prioritize recovery efforts. Firms must also ensure that third-party providers can adhere to these tolerances through enforceable service-level agreements (SLAs), robust audits, and joint testing.

Additional considerations include customer segmentation (e.g., vulnerable customers or those with higher exposure) and estimated losses from prolonged disruptions. Impact tolerances should be integrated into the broader risk management framework and linked to triggers within business continuity plans.

Best Practices:

- **Set multi-dimensional impact tolerances**, not only based on time, but on metrics such as consumer vulnerability, financial thresholds and potential reputational fallout.
- **Develop specific and measurable terms for third-party adherence to SRTOs**, with regular audits and performance monitoring.
- **Engage in collaborative scenario testing** with key providers to validate their ability to meet predefined tolerances under stress.

Scenario Testing and Business Continuity Planning

Scenario testing helps firms to understand how disruptions can unfold across technology, operations, and people. These scenario tests build on the ORM framework, moving beyond prevention, so organizations can test their ability to stay within their defined impact tolerances when severe but plausible disruptions occur.

This means shifting from theoretical exercises to real-world stress tests—assuming that failures will happen and evaluating how well the business can respond and recover. Simulating real-world crises, identifying control caps and assessing RTO's directly informs business continuity plans by refining response strategies, improving coordination, and ensuring alignment with evolving risks and operational dependencies.

To be truly effective, scenario testing must evolve beyond static checklists. Firms need adaptive, intelligent frameworks that keep pace with emerging threats, regulatory changes, and shifts in their own operations.

Best Practices:

- **Develop scenarios that reflect realistic, high-impact disruption events**, including cyberattacks, supply chain failures, and simultaneous multi-domain incidents.
- **Systematically integrate scenario test results** into future operational risk assessments, updating risk registers, refining impact analyses, and adjusting control frameworks.
- **Implement a schedule of periodic and ad-hoc testing** that evolves with the threat landscape, regulatory expectations, and organizational changes.

Third-party risk management

Third parties can be deemed material either through single critical dependencies or cumulative involvement across multiple services. Identifying and managing these risks begins with a top-down approach, mapping critical operations to understand how third parties contribute to key processes and outcomes. For single critical arrangements, it's crucial to evaluate the direct impact of provider failure on core operations. Conversely, for cumulative dependencies, assess how multiple engagements with the same provider create a broader operational risk.

To manage these risks effectively, adopt a data-driven, dual-perspective approach—combining internal assessments with external risk intelligence from available tools. Use targeted, automated questionnaires focusing on critical controls and ensure due diligence extends to fourth-party risks. Additionally, leverage documentation such as SOC reports and business continuity plans to satisfy both internal risk oversight and regulatory expectations.

Best Practices:

- **Develop a comprehensive, living register of material service providers** that captures detailed interdependencies, including core technology providers, data hosting services, and high-risk technology consultants.
- **Create legally binding Service Level Agreements (SLAs) that explicitly define risk management provisions**, including subcontractor oversight, regulatory access, and clear termination protocols.
- **Implement continuous monitoring mechanisms** that dynamically assess supplier performance, track risk indicators, and conduct regular scenario analyses to validate the resilience of critical service providers.

Incident Reporting

Regulations require that "major" incidents be reported promptly, typically within 24 hours of detection, with additional detailed reports due within 72 hours and a final report submitted within a month.

Incident reporting frameworks must encompass internal and external communication strategies, including clearly defined escalation paths and stakeholder engagement plans, to facilitate a coordinated and informed response.

Best Practices:

- **Notify competent authorities** within the required timeframe, providing clear and accurate initial information about the incident and its immediate impact.
- **Establish internal and external communication strategies,** including:
  - Defined escalation pathways for internal teams.
  - Regular updates for external stakeholders, such as regulators, clients, and partners.
- **Be prepared to submit multiple incident reports,** including:
  - An initial notification with essential details such as the nature, scope, and immediate impacts of the incident.
  - Intermediate reports as soon as the status of the incident changes, including updates on mitigation efforts and preliminary findings.
  - A final report once the root cause analysis has been completed.

Continuous Improvement and Monitoring

ORM is not a one-time exercise but an ongoing effort requiring continuous improvement. Global regulators highlight proactive monitoring of the threat landscape, with automated horizon scanning, performance reviews and audits forming a cornerstone of ORM and resilience programs.

Regulatory frameworks like DORA advocate for cross-industry collaboration, including the sharing of cyber-threat intelligence, to enhance collective resilience. Similarly, the FCA mandates annual self-assessments to document compliance with operational resilience requirements.

Best Practices:

- **Integrate resilience measures into business-as-usual processes**, ensuring they are not treated as standalone exercises but as part of the organization's operational fabric.
- **Implement advanced monitoring tools to track the threat landscape in real time**, enabling faster identification and mitigation of risks.
- **Review and analyze incidents and test results to derive actionable insights**. Update business continuity and operational resilience plans to reflect these learnings, preventing recurrence of past failures.

The Need for Integrated Risk Management

79% of organizations feel ill-equipped to comply with new operational resilience regulations, and only 20% of executives believe their firms are fully prepared to prevent or respond to outages. [3]

Despite consensus among regulators on what resilience looks like, the path to achieving it is fraught with complexity. Operational risk spans every corner of an organization, from internal processes to third- and fourth-party ecosystems. Managing these risks effectively—and ensuring compliance with the aforementioned regulations—simply isn't possible with antiquated systems and data silos.

This is where the importance of a centralized risk management tool becomes clear. Such a solution consolidates data across the organization, enabling a holistic view of risks, dependencies, and vulnerabilities. It supports comprehensive data-driven risk assessments, continuous monitoring and empowers proactive decision-making by providing real-time insights into operational risks.

In the next paper, we'll examine exactly how technology bridges the gap, shifting ORM and resilience from a reactive necessity to a strategic advantage. From advanced data analytics to visual dashboards and automated third-party risk management, we will present the solution for organizations to not only navigate the complexities of 2025 but also thrive in the years that follow.

3. https://www.cockroachlabs.com/blog/the-state-of-resilience-2025-reveals-the-true-cost-of-downtime/

SAI360's unified approach to risk sets us apart

Today's complex risk landscape demands more. SAI360 leads the way with an integrated GRC platform and Learning solution that spans the entire risk and compliance spectrum.

Risk Management Solutions

- Risk & Compliance Management Solutions
- Enterprise & Operational Risk Management
- Regulatory Compliance
- Policy Management
- Third-Party / Vendor Risk Management
- Internal Controls
- Internal Audit
- Incident Management
- Conflicts of Interest (COI)
- Gifts and Hospitality
- IT & Cybersecurity
- Business Continuity Management

Ethics & Compliance Learning Solutions

- Anti-Bribery & Anti-Corruption
- Competition & Anti-Trust
- Conflicts of Interest
- Data Protection & Privacy
- Exports, Imports & Trade Compliance
- Harassment & Discrimination

SAI360 is giving companies a new perspective on risk management. By integrating Governance, Risk, Compliance (GRC) software and Ethics & Compliance Learning resources, SAI360 can broaden your risk horizon and increase your ability to identify, manage, and mitigate risk. See risk from every angle.
Visit www.sai360.com.

195150 0325