Operational Risk-Resilience/Management Standards

Cite

Basel Committee on Banking Supervision, Consultative Reports; Principles for Operational Resilience; Revisions to the Principles for the Sound Management of Operational Risk

Recommended Distribution:

Operational-Risk Management, Business-Continuity Management, Risk Management, Corporate Secretary, Capital Planning, Policy, Legal, Government Relations

Websites:

https://www.bis.org/bcbs/publ/d508.pdf

https://www.bis.org/bcbs/publ/d509.pdf

Impact Assessment

- Regulators are returning attention to operational risks beyond the legal and reputational ones borne out of the 2008 crisis that were the focus of global and national regulators. This approach led to a largely retrospective construct for operational-risk management and capital that may have made banks more vulnerable to prospective risks such as the pandemic.
- The forward-looking framework conflicts with the retroactive calculation of operational risk-based capital required by recent Basel standards.
- Much in the consultations focuses on governance, reinforcing existing duties for boards and senior management and sometimes also creating new ones. In several cases, these new duties for boards may overlap with those of senior management.
- The new standards could increase bank resilience to climate change by virtue of more stringent directives to take catastrophic natural disasters into account.
- A more emphatic overall ethics and culture component is added to operational-risk management along with additional governance requirements. These may overlap or even conflict with existing corporate-culture codes. Incentive realignment specific to operational-risk management may also be required.
- The two consultations are often repetitive, likely creating a burdensome risk-management framework unless rationalized when finalized.

Overview

Although the Basel Committee believes that its post-crisis capital and liquidity framework significantly enhanced bank resilience evident in a robust industry response to the pandemic, this crisis and other developments are said to highlight the need for additional regulatory and supervisory work to improve operational resilience. Given the changing nature of operational risk, the Basel Committee has now decided against a prescriptive approach at least with regard to resilience. However, the separate consultation on operational-risk management is, despite the fact that it often addresses the same operational risks, more prescriptive and detailed, often laying out technical requirements for boards, senior management, and even junior risk managers. This standard also overlaps with the resilience standards not only with regard to business-continuity planning, but also for overall operational-risk management governance, analysis, controls, and reporting. Perhaps as a result, Basel contemplates combining these standards although it does not say how this might be done. Neither document makes clear how it is intended to relate to Basel's new operational risk-based capital framework,[1] although the resilience statement suggests that its approach is updated in response to it. Because these standards are forward-looking and the capital rule is retrospective, it is unclear how data would be integrated or the extent to which capital would buffer new risk.

Impact

These consultations draw on Basel's prior operational-risk management standards,[2] corporate governance,[3] and other statements related to continuity and outsourcing.[4] The operational-risk management principles also implement recommendations from a 2014 review of practices following the 2011 Basel standards, doing so with regard to the pandemic at least with regard to the resilience standards. Although both documents are said to establish only principles, the operational-risk management document is considerably more prescriptive. It is thus unclear how the goals Basel sets for a flexible framework that adapts easily to emerging risks applies to the management framework, which could lead banks to focus more on compliance than planning as has often been the case with other, detailed risk-management edicts.

As noted, both standards describe themselves as forward-looking even though the Basel operational risk-based capital framework is standardized and largely retrospective. While risk management and capital planning are different functions, capital divorced from emerging risk may prove an uncertain buffer. Asymmetries between these rules – for example with regard to what is considered robust mitigation – could also create conflicting incentives for banks to skirt mitigations that work well for planning but are not recognized in capital regulation.

It is unclear how the U.S. would proceed if Basel finalizes these risk-management standards. U.S. capital rules have yet to adhere to Basel's approach, retaining the advanced measurement approach (AMA) which, as of recent revisions,

---

1 See **OPSRISK20**, *Financial Services Management*, January 8, 2018.

2 See **OPSRISK9**, *Financial Services Management*, July 28, 2004.

3 See **CORPGOV19**, *Financial Services Management*, March 31, 2010.

4 See **OUTSOURCING3**, *Financial Services Management*, March 3, 2005.

now only applies to U.S. GSIBs and one large custody bank.[5] The AMA has numerous challenges but is meant to be forward-looking, an approach also embodied in U.S. stress-testing regimes now wrapped into the stress capital buffer (SCB).[6] If the U.S. retailed this approach despite its differences with Basel but modified operational-risk management standards in line with Basel's, it could well retain forward-looking policies with aligned capital and risk-management incentives, but considerable governance, scenario-analysis, and other duplicative requirements could result. Incompatibilities between the capital and management standards, especially with regard to permissible risk mitigation (e.g., insurance) would also likely create continuing inconsistencies and, perhaps, misaligned incentives. The U.S. regime would also be inconsistent with global rules, perhaps making very large U.S. banks more resilient but also less competitive in sectors where operational-risk capital and management are particularly critical (e.g., custody, asset management).

What's Next

These consultations were issued on August 6. Comment is due by November 6. Basel offers no finalization timeframe.

Analysis

These standards are to be implemented with regard to an institution's size, complexity, and business model and to national factors.

A. Operational Resilience

1. Definition

Operational resilience is here defined as a bank's ability to deliver critical operations through disruption, enabling it to identify and protect itself from threats and potential failures and respond, recover, and learn from disruptive events to minimize impact on the delivery of critical operations. Risk appetite is defined as in Basel's corporate-governance standards and critical operations are defined as in 2006 Joint Forum standards.[7]

2. Principles

Taken together with a bank's risk appetite and critical functions, these principles would be:

- Governance: The board of directors takes high-level, active responsibility for ensuring operational resilience under a range of severe, but plausible, scenarios (e.g., pandemics, catastrophic natural disasters, cyber-attack). Senior

[5] See *Client Report* **SIFI29**, October 31, 2018.

[6] See **CAPITAL225**, *Financial Services Management*, March 11, 2020.

[7] See **OPSRISK12**, *Financial Services Management*, September 7, 2006.

management is to provide timely reports to the board on business-function resilience, especially when operational stress strikes the bank.

- Operational-Risk Management: Identification should spot internal and external threats and vulnerabilities in people, processes, and systems on an ongoing basis, managing risks as identified, and managing resulting risks in accord with the operational-risk appetite. Coordination with business-continuity planning, third-party dependency management, recovery and resolution planning, and other risk-management frameworks may yield a more consistent approach to operational resilience across the enterprise. Operational-risk mitigants should be regularly assessed, adapted in the face of new challenges, and repaired promptly as needed.
- Business-Continuity Planning and Testing: These plans should test reliance under the same severe, but plausible scenarios referenced above. As one might expect, plans are to be forward-looking and capture internal and external threats, inter-dependencies, and vulnerabilities identified via business-impact analyses, recovery strategies, testing, training, and communication and crisis-management programs. Plans are to be detailed and include points of accountability across business functions and the bank as a whole, with internationally-active banks told to harmonize business-continuity plans with resolution plans and ensure effective resilience across borders with regard to critical infrastructure.
- Mapping Interconnections and Inter-Dependencies: The principles spell out broad standards for how this should be done.
- Third-Party Dependency Management: Those to third parties and intra-group affiliates are to be managed in the same fashion as direct vulnerabilities. Advance verification of third-party/intra-group risk-management practices should occur prior to operational integration, with all arrangements formalized in written agreements addressing operational resilience under normal and stress conditions. Internal-resilience and exit strategies should ensure the bank is prepared for third-party/intra-group operational failure and ensure substitutability for critical operations.
- Incident Management: This should be continuously improved as developments and experience warrant, capturing an incident's life-cycle covering factors such as classifying an incident's likely strategic impact based on pre-defined indicators along with steps necessary to return to business as usual. All incidents, including those at third parties or elsewhere in the group, are to be managed, reported, and disclosed according to the prior plan.
- Resilient IT and Cyber-Security: Specific principles in this sector largely repeat those in prior FSB documents and other standards in this arena.[8]

3. Request for Comment

Questions are posed on:

- how best to measure operational resilience given the early development stage of methodologies in this area;
- COVID-specific lessons that should be reflected in final principles; and
- the benefit of combining this set of principles with those on operational-risk management.

[8] See *Client Reports* in the **INFOSEC/CYBER** series.

B. Operational-Risk Management

These standards are meant to reinforce the resilience principles described above and expand on them.

1. Definition

As in the capital rules, operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk but excludes strategic and reputational risk.

2. Risk Management Construct

Banks are to rely on three operational-risk defence lines:

- business-unit management. Staff is to identify and verify material operational-risk exposures, establish controls, report resource shortfalls, and report risks within designated tolerances and outside these parameters. Business-unit support functions in larger banks should also be subject to these operational-risk controls;
- independent corporate risk management, which should have an independent view of business-unit exposures and controls and provide units with operational-risk management tools. The degree of independence depends on bank size/complexity, but larger institutions should have risk management segregated from business units. Quality assurance may be a 1.5 line of defense based on organizational structure; and
- independent verification and validation that informs board activities. This should be conducted by inside or outside audit personnel which should review all legal units and opine on overall risk-management conduct, controls, correction, and exposure.

Basel has found that the independence of the second line of defense is sometimes compromised and that other functional and accountability confusions challenge the effectiveness of this approach as used by many banks. The consultation thus re-emphasizes this three-line model and emphasizes it should be used for all operational risks, including IT. An array of policies and procedures to reinforce each line are detailed in the consultation. Basel also emphasizes how rapidly operational risk may change and thus the importance of senior management ongoing understanding of exposures, willingness to ensure sufficient resources for mitigation or absorption, and effective governance.

C. Operational-Risk Management Principles

These are:

- Governance: The board is to lead a strong risk-management culture implemented by senior management to include incentives for positive behavior accompanied by effective ethics and risk-management training. The board should also establish a

code or policy to address conduct risk for both staff and the board overseen by a "senior ethics committee" or similar body.

- Operational Risk Framework: The board and senior management should understand operational-risk exposures, understanding that it is inherent in all business activities and thus ensuring that the operational-risk management framework is fully integrated into other risk-management constructs using the three lines of defense described above. This framework is also to be embedded in strategic planning. A detailed list of requisite documentation is also provided.
- Board of Directors: In addition to the governance principle noted above, the consultation includes two separate principles adding additional board duties (e.g., the need to oversee material operational risks and the effectiveness of control protocols). Detailed procedures here may overlap with those described for senior management in the earlier principle, although the bulk of these additional principles focuses on setting thresholds, ensuring accountability, and judging effectiveness.
- Senior Management: This principle details how senior management should enforce and implement board edicts, demonstrating to the board how the three defense lines work in practice for material businesses and risks. Appropriate managerial committees, reports, and responses are also detailed.
- Risk-Management Environment: This issue is separately addressed for senior-management policies and procedures. The principles also address event management, scenario analysis, and the control, monitoring, and assurance framework along with the metrics senior management should deploy in this arena. A separate principle also addresses change management, instructing senior management to ensure it is appropriately funded and effectively articulates actions by each line of defense as risks change and across product lifecycles. Another principle details how senior management is to monitor the bank's operational-risk profile and material exposures.
- Control and Mitigation: Going beyond all the specifics noted above, this principle details how controls should be constructed, monitored, and improved. Technology risks should be managed as operational risk.
- IT Risk: In addition to specifying the framework for technology risk noted above, the principles also go into detail on specific considerations with regard to IT and security.
- Business-Continuity Planning: Banks are to prepare forward-looking business-continuity plans, with the discussion here repeating much in the operational-resilience consultation described above.
- Disclosures: Disclosures are needed to ensure transparency and improved industry practice. Formal disclosures policies should be established, reviewed, and deployed as needed.
- Supervisors: These are told to ensure that all the principles are effectively implemented, with the consultation detailing ways to do so and how to enhance information sharing among domestic and international supervisory agencies.