

Lukas Görnert
10/2026

EBA KONKRETISIERT ANFORDERUNGEN AN DAS MANAGEMENT OPERATIONELLER RISIKEN

Einführung

Mit der CRR III wurde die Ermittlung der Eigenmittelanforderungen für operationelle Risiken grundlegend vereinfacht: Die bisherigen Ansätze wurden durch einen einheitlichen, nicht modellbasierten Ansatz auf Basis der Business Indicator Component ersetzt. Diese Vereinfachung der Säule-1-Kapitalberechnung bedeutet jedoch keine Absenkung der Anforderungen an das Management operationeller Risiken. Art. 323 CRR verlangt weiterhin ein angemessenes und dokumentiertes System zur Identifikation, Bewertung und Steuerung operationeller Risiken sowie eine unabhängige OpRisk-Funktion, regelmäßiges Reporting, Validierung und Prüfung. Mit dem am 26. August 2026 veröffentlichten Konsultationspapier EBA/CP/2026/18¹ konkretisiert die EBA diese bislang abstrakten Anforderungen. Ziel ist ein harmonisierter Mindeststandard für das operationelle Risikomanagement europäischer Institute. Hintergrund ist insbesondere, dass die mit früheren fortgeschrittenen Ansätzen verbundenen Anforderungen an Governance, Daten, Szenarioanalysen und unabhängige Überprüfung mit dem Wegfall interner Modelle nicht an Bedeutung verlieren sollen. Vielmehr sollen diese Elemente – unter Berücksichtigung von Größe und Komplexität – Bestandteil eines wirksamen OpRisk-Managements aller Institute sein.

¹ [EBA/CP/2026/18](#). Die Konsultation ist bis zum 31.12.2026 geöffnet.

Ein integriertes OpRisk-Framework als Lösungsansatz

Die EBA strukturiert das künftige OpRisk-Framework im Wesentlichen entlang dreier miteinander verbundener Komponenten: Governance, einem fortlaufenden Operational Risk Management Process sowie einem Operational Risk Assessment System. Operationelle Risiken sollen damit nicht isoliert oder lediglich über eingetretene Schäden betrachtet werden. Gefordert wird vielmehr eine integrierte und zukunftsgerichtete Sicht auf das Risikoprofil, die in die regulären Steuerungs- und Entscheidungsprozesse des Instituts eingebettet ist. Für Institute bietet sich daher an, bestehende Verfahren – insbesondere RCSA, Schadensdatensammlung, Szenarioanalyse, IKS, IKT-Risikomanagement, BCM und Drittparteienmanagement – nicht als voneinander getrennte Prozesse weiterzuentwickeln. Ziel sollte vielmehr ein gemeinsames OpRisk-Zielbild sein, in dem Risiken, Kontrollen, Ereignisse, Indikatoren und Szenarien über eine konsistente Taxonomie und Datenbasis miteinander verbunden werden.

Governance und Risikoappetit

Die Verantwortung des Leitungsorgans wird deutlich konkretisiert. Das OpRisk-Management Framework und der Risikoappetit sind zu genehmigen und regelmäßig zu überwachen. Die Leitungsorgane sollen den Risikoappetit in quantitative Limite übersetzen und sicherstellen, dass die tatsächlichen Risikopositionen innerhalb dieser Grenzen bleiben. Gleichzeitig verlangt die EBA eine unabhängige Funktion für das Management operationeller Risiken in der zweiten Verteidigungslinie mit ausreichender Autorität, Ressourcen und fachlicher Expertise. Damit gewinnt insbesondere die Verbindung zwischen Risiko-Appetit, Limiten, Key Risk Indikatoren (KRIs) und Eskalationsmechanismen an Bedeutung. Ein rein qualitativ formulierter OpRisk-Risikoappetit dürfte insbesondere bei größeren Instituten künftig nicht mehr ausreichen.

Forward-looking Risk Assessment

Das Risk-Self-Assessment soll über die Betrachtung bereits realisierter Schäden deutlich hinausgehen. Die EBA nennt ausdrücklich Risk-Control-Self-Assessments (RCSA), Prozessmapping, Schadens- und Beinaheschadensdaten, Root-Cause-Analysen², Key-Risk-Indikatoren (inbs. Frühwarnindikatoren), Szenarioanalysen sowie Stresstests. Ergänzend sollen interne und externe Entwicklungen sowie Emerging Risks³ berücksichtigt werden, etwa Risiken aus neuen Technologien, künstlicher Intelligenz, ESG-Faktoren oder geopolitischen Entwicklungen. Das klassische RCSA wird damit nicht ersetzt, aber in ein umfassenderes Assessment-System eingebettet. Entscheidend wird künftig weniger die isolierte Durchführung einzelner 2nd-Line-Funktionen sein als deren nachvollziehbares Zusammenspiel. Ergebnisse sollen unter anderem zur Überwachung des

² Root-Cause-Analyse ist ein systematischer Ansatz, um nicht nur die Symptome eines Problems zu bekämpfen, sondern dessen tatsächliche Ursache zu finden. Sobald die Ursache behoben wird, tritt das Problem dauerhaft nicht wieder auf.

³ Emerging Risks sind neue oder neu aufkommende Risiken, deren Schadenspotenzial, Eintrittshäufigkeit oder genauer Charakter noch weitgehend unbekannt oder unsicher sind.

Integration in Geschäfts- und Steuerungsprozesse	Risikoappetits, zur Priorisierung von Maßnahmen, für den ICAAP und zur Stärkung der Operational Resilience verwendet werden. Die EBA stellt ausdrücklich klar, dass OpRisk-Management kein eigenständiger Compliance-Prozess sein soll. OpRisk-Aspekte sollen unter anderem in Produkt- und Prozessgovernance, Change Management, Incident Management, Entscheidungen über Drittparteien sowie Maßnahmen- und Eskalationsprozesse integriert werden. Hieraus ergibt sich für viele Institute ein wesentlicher organisatorischer Handlungsbedarf: Informationen aus bestehenden „Vorprozessen“ müssen systematisch in das übergreifende OpRisk-Profil einfließen, ohne parallele Bewertungswelten aufzubauen.
Daten, Taxonomie und Reporting	Der Entwurf stärkt auch die Anforderungen an die zugrunde liegende Datenbasis. Institute sollen eine Taxonomie nicht nur zur Klassifikation von Verlusten, sondern auch zur Einordnung von Risikoereignissen und zur Aggregation des OpRisk-Profiles über Prozesse und Organisationseinheiten hinweg verwenden. Hinzu kommen Anforderungen an Data Ownership, dokumentierte Datenquellen und Definitionen, Datenqualitätskontrollen, Audit Trails und – soweit relevant – Reconciliation-Prozesse. Das Management Reporting soll Exposures, Schäden, Incidents, Trends und Maßnahmen adressatengerecht zusammenführen. Eine besondere Rolle spielt dabei die Schwelle von 750 Mio. EUR des Business Indicators. Für Institute oberhalb dieser Schwelle sieht der Entwurf unter anderem einen erweiterten Datenumfang, quantitative OpRisk-Limits, mindestens jährliche Effektivitätsreviews des Frameworks und mindestens ein quartalsweises Reporting des Risikoprofils an das Leitungsorgan vor. Unterhalb der Schwelle gelten vereinfachte Anforderungen; der Grundsatz eines wirksamen OpRisk-Frameworks bleibt jedoch bestehen.
DORA und operationelle Resilienz	Die EBA verbindet das operationelle Risikomanagement ausdrücklich mit DORA. IKT-Risiken, Cybervorfälle, Datenprobleme und Risiken aus IKT-Drittparteien sind als wesentliche Quellen operationeller Risiken in das Gesamtframework einzubeziehen. Gleichzeitig sollen Doppelarbeiten vermieden werden: Bereits unter DORA etablierte Strategien, Prozesse, Kontrollen und Informationen können genutzt werden, sofern sie auch die Anforderungen des OpRisk-Frameworks erfüllen.
Validierung und unabhängige Prüfung	Schließlich konkretisiert das Papier die Rollen von interner Validierung und Prüfung durch die interne Revision. Die Validierung ist Bestandteil der laufenden Compliance- und Kontrollmechanismen und soll insbesondere die Angemessenheit und Leistungsfähigkeit des Operational Risk Assessment Systems sowie ausgewählter Berechnungs- und Bewertungsverfahren beurteilen. Die Interne Revision verfügt demgegenüber über

Einordnung und Handlungsbedarf

einen weitergehenden Prüfungsauftrag. Sie beurteilt unabhängig von den geprüften Aktivitäten, Prozessen und Systemen die Zuverlässigkeit und Wirksamkeit des OpRisk-Management Prozesses, des RCSAs sowie die Integrität der zugrunde liegenden Policies, Prozesse, Kontrollen und Daten.

Das Konsultationspapier erfindet das Management von operationellen Risiken nicht neu. Viele der angesprochenen Elemente sind in etablierten Instituten bereits über MaRisk, DORA, IKS, RCSA, Schadensdatenmanagement oder ICAAP vorhanden. Die wesentliche Veränderung liegt vielmehr darin, dass die EBA diese bislang teilweise verteilten Anforderungen zu einem konsistenten und aufsichtlich überprüfbaren Mindeststandard nach Art. 323 CRR zusammenführt. Institute sollten die Konsultation daher zum Anlass nehmen, weniger einzelne neue Pflichten zu implementieren als die Kohärenz ihres bestehenden Frameworks zu überprüfen. Im Mittelpunkt sollte die Frage stehen, ob Governance, Risikoappetit, RCSA, Szenarioanalyse, Schadens- und Ereignisdaten, KRIs, IKT- und Drittparteienrisiken sowie Maßnahmen und Reporting tatsächlich ein stimmiges Bild des operationellen Risikoprofils erzeugen. Ein sinnvoller erster Schritt ist deshalb ein strukturierter Readiness- bzw. GAP-Check entlang der neuen zur Konsultation stehenden Anforderungen. Darauf aufbauend können gezielt methodische, organisatorische und datenbezogene Anpassungen vorgenommen werden. Damit lässt sich regulatorische Konformität mit einem praktischen Mehrwert verbinden: einem transparenteren Risikoprofil, weniger parallelen Risikobewertungen und einer besseren Verzahnung von OpRisk-Management und Operational Resilience.

Unterstützung durch
1 PLUS i

Gerne unterstützen wir Sie bei sämtlichen Fragestellungen rund um das Thema OpRisk und IKT-Risikomanagement. Sollten Sie Interesse an weiteren Details zu den obigen Ausführungen und den damit einhergehenden Fragestellungen haben, sprechen Sie uns gerne an. (info@1plusi.de)

Autor
Lukas Görnert



Lukas.Goernert@1plusi.de