

Lukas Görnert
10/2026

VOM SILODENKEN ZUR INTEGRIERTEN RISIKOSTEUERUNG: VERZAHNUNG VON OPRISK & IT-GOVERNANCE

Einführung

DORA hat das IKT-Risikomanagement vieler Institute deutlich aufgewertet. Dennoch entstehen in der Praxis häufig zwei parallele Steuerungswelten: IT-Governance, Informationssicherheit und IT-Compliance arbeiten mit technischen Risikobewertungen, Schwachstellen, Service-Leveln und Vorfällen. Das Risikocontrolling steuert dagegen über Risikotaxonomien, Risk Self Assessments, Szenarioanalysen, Verlustdaten und Risikoberichte.

Beide Seiten befassen sich vielfach mit denselben Risiken – aber mit unterschiedlichen Begriffen, Bewertungsmaßstäben und Berichtswegen. Die Folge sind Doppelarbeiten, widersprüchliche Einschätzungen und ein fragmentiertes Risikobild. Die zentrale Herausforderung besteht daher nicht darin, ein weiteres DORA-Framework aufzubauen, sondern IKT-Risiken in die bestehende Steuerung operationeller Risiken zu integrieren.

Regulatorische Rahmenbedingungen

DORA verlangt ausdrücklich kein isoliertes IKT-Risikomanagement. Nach Art. 6 Abs. 1 DORA¹ muss der IKT-Risikomanagementrahmen Bestandteil des gesamten Risikomanagementsystems sein. Nach Art. 6 Abs. 8 Buchst. a–c DORA muss diese Strategie die Geschäftsstrategie unterstützen, die IKT-Risikotoleranz mit der allgemeinen Risikobereitschaft verbinden und messbare Leistungs- und Risikoindikatoren enthalten. IKT-

¹ [Vorordnung \(EU\) 2022/2554 - DORA](#)

Risikoappetit, KPIs und KRIs dürfen daher nicht losgelöst von Risikostrategie und Gesamtbanksteuerung definiert werden. Die Delegierte Verordnung (DelVo (EU) 2024/1774²) zum IKT-Risikomanagement konkretisiert diese Steuerungskette zusätzlich. Nach Art. 3 müssen Institute dokumentierte Verfahren vorhalten, die

- ≡ die genehmigte IKT-Risikotoleranz zugrunde legen,
- ≡ Schwachstellen und Bedrohungen anhand qualitativer oder quantitativer Indikatoren bewerten,
- ≡ Maßnahmen zur Rückführung von Risiken innerhalb der Toleranz festlegen,
- ≡ die Annahme überschreitender Residualrisiken regeln und
- ≡ Veränderungen des IKT-Risikoprofils fortlaufend überwachen.

Art. 2 Abs. 2 Buchst. c und g verlangen zusätzlich Indikatoren zur Überwachung der Umsetzung zu bestimmen sowie eine Einordnung der Verantwortlichkeiten in das 3LOD-Modell. Damit verbindet die DelVo Risikoappetit, Risikobewertung, Kennzahlen, Maßnahmensteuerung, Risikoakzeptanz und Reporting zu einem durchgängigen Regelkreis.

Auch IKT-Drittparteirisiken dürfen nicht in einem separaten Auslagerungs- oder Einkaufsprozess verbleiben. Art. 28 Abs. 1 DORA bezeichnet sie ausdrücklich als integralen Bestandteil des IKT-Risikos. Der RTS nach Delegierter Verordnung [\(EU\) 2024/1773](#) fordert in Art. 3 Abs. 5 und 6 die Zusammenarbeit mit den Kontrollfunktionen und die Konsistenz mit IKT-Risikomanagement, Informationssicherheit, BCM und Incident Management. Art. 4 Buchst. c verlangt die Einbindung von Geschäftsbereichen, internen Kontrollfunktionen und weiteren relevanten Einheiten. Nach Art. 9 Abs. 2 und 3 sind Dienstleister über KPIs, Kontrollindikatoren, Prüfungen und Berichte zu überwachen; die Ergebnisse müssen wiederum in die Risikobewertung des Instituts einfließen.

Mit der 9. MaRisk³-Novelle werden die bestehenden Anforderungen an das Risikomanagement insbesondere um eine explizite Berücksichtigung von IKT-Risiken ergänzt oder stärker mit den DORA-Anforderungen verzahnt:

- ≡ AT 2.2 Tz. 1: IKT-Risiken sind Bestandteil der operationellen Risiken und explizit in die Risikoinventur einzubeziehen.

² [DelVo 2024/1774](#)

³ [Bafin - Rundschreiben 06/2026 \(BA\) MaRisk](#)

Der IKT-Risikoappetit
muss messbar werden

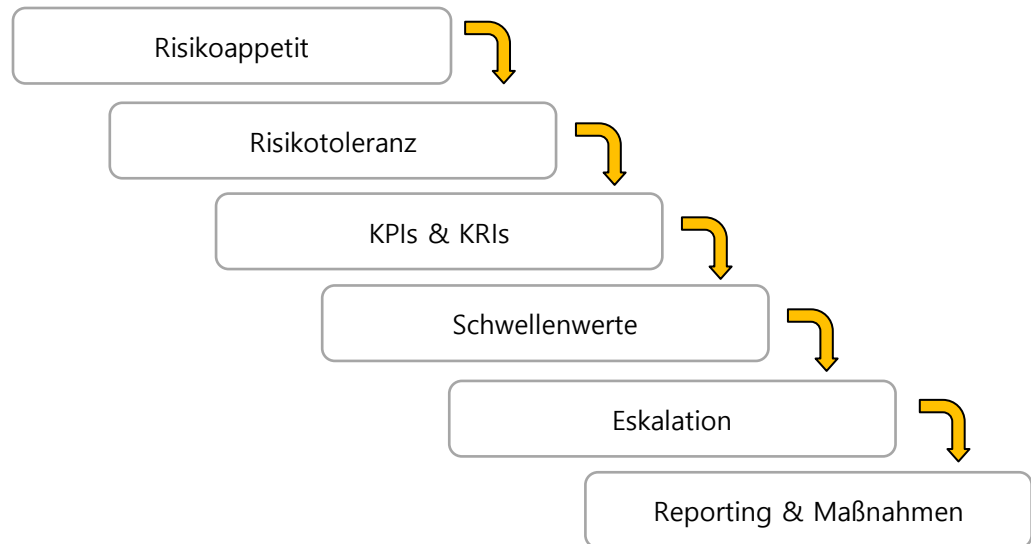
- ≡ AT 4.2 Tz. 2: Für alle wesentlichen Risiken ist ein Risikoappetit festzulegen; zugleich ist eine konsistente IKT- beziehungsweise DOR-Strategie erforderlich.
- ≡ AT 4.3.2 Tz. 1 und 2: Risiken sind zu identifizieren, zu beurteilen, zu steuern, zu überwachen und zu kommunizieren. Die Prozesse sind in die Gesamtbanksteuerung einzubinden und durch geeignete Frühwarnindikatoren zu unterstützen.
- ≡ BTR 4 Tz. 2, 4 und 5: Wesentliche operationelle Risiken sind mindestens jährlich zu identifizieren und zu bewerten. Dabei sind sowohl historische Erkenntnisse als auch potenzielle Ereignisse zu berücksichtigen und erforderliche Steuerungsmaßnahmen abzuleiten.
- ≡ BT 2.1 und BT 2.2 nimmt Bezug auf das Reporting an die Leitungsorgane.

Viele Strategien bleiben beim Risikoappetit zu abstrakt. Aussagen wie „Das Institut verfolgt einen konservativen IKT-Risikoappetit“ oder „Ausfälle kritischer Systeme sollen vermieden werden“ geben zwar eine Richtung vor, ermöglichen aber keine wirksame Steuerung.

Ein belastbarer IKT-Risikoappetit muss deshalb in messbare Toleranzen übersetzt werden. Dazu gehören beispielsweise:

- ≡ Maximal tolerierbare Ausfallzeiten (MTA) kritischer Geschäftsservices,
- ≡ Tolerierte Anzahl an SLA-Verletzung beim Bezug von IKT-Dienstleistungen,
- ≡ Zulässige Überschreitung von Wiederanlaufzielen,
- ≡ Grenzen für Konzentrationen bei IKT-Drittparteien,
- ≡ Eskalationsschwellen für schwerwiegende oder wiederkehrende Vorfälle,
- ≡ Vorgaben zur Akzeptanz wesentlicher Restrisiken.

Die Schwellenwerte dürfen nicht isoliert durch die IT festgelegt werden. Sie müssen aus dem Geschäftsmodell, der Kritikalität der unterstützten Funktionen, den Business-Impact-Analysen, den Wiederanlaufzielen und dem übergreifenden Risikoappetit des Instituts abgeleitet werden. Die notwendige Steuerungskette lautet:



Fehlt eines dieser Elemente, bleibt eine Kennzahl häufig rein informativ. Ein roter Ampelstatus ohne definierte Konsequenz ist noch keine aufsichtlich adäquate Risikosteuerung.

KPIs & KRIs müssen dieselbe Risikologik abbilden

KPIs zeigen primär, ob Prozesse, Kontrollen und Services wie vorgesehen funktionieren. Beispiele sind Systemverfügbarkeit, Patch-Compliance, erfolgreiche Datensicherungen oder fristgerecht durchgeführte Notfalltests.

KRIs zeigen dagegen, ob sich die Risikoexposition erhöht oder eine Toleranzgrenze erreicht wird. Hierzu zählen etwa eine steigende Zahl überfälliger Schwachstellen, wiederholte Provider-Ausfälle, zunehmende SLA-Verletzungen, zunehmende Sicherheitsvorfälle, fehlgeschlagene Wiederanlauf-tests oder eine hohe Abhängigkeit von einzelnen Dienstleistern.

Entscheidend ist nicht die Anzahl der Kennzahlen. Jede Kennzahl sollte eindeutig einem Risiko, einem Kontrollziel, einer Toleranzgrenze, einem Verantwortlichen und einer Eskalationsregel zugeordnet sein. Dadurch entsteht eine Verbindung zwischen technischer Leistungsmessung und bankspezifischer Risikosteuerung.

Adressatengerechtes Reporting statt technischer Datenfriedhof

IKT-Risikoberichte enthalten häufig umfangreiche technische Informationen, lassen aber offen, welche Auswirkungen diese auf Geschäftsprozesse, Kunden, regulatorische Verpflichtungen oder die Risikotragfähigkeit haben. Für das Leitungsorgan sind vor allem folgende Fragen relevant:

- ≡ Welche kritischen oder wichtigen Funktionen sind betroffen?
- ≡ Liegt das Risiko innerhalb des genehmigten Risikoappetits?
- ≡ Wie hat sich die Exposition gegenüber der Vorperiode verändert?
- ≡ Welche Ursachen, Ereignisse, Abhängigkeiten und Kontrollschwächen bestehen?
- ≡ Welche Entscheidung oder Maßnahme ist erforderlich?

Statt lediglich über eine erhöhte Anzahl an Cyberbedrohungen zu berichten, sollte beispielsweise dargestellt werden, welche Geschäftsservices betroffen sind, wie realistisch ein erfolgreicher Angriff ist, welche Kontrollen wirken und ob das verbleibende Risiko noch innerhalb der genehmigten Toleranz liegt. Ein wirksames Reporting verdichtet daher technische Sachverhalte zu einer geschäftlichen Risikoperspektive. Wenige aussagekräftige Risikoentwicklungen, Toleranzüberschreitungen und konkrete Entscheidungsbedarfe sind für das Management regelmäßig wertvoller als ein umfangreicher Kennzahlenkatalog.

Eine gemeinsame Risikosprache schaffen

Die IT-Governance betrachtet Risiken typischerweise ausgehend von Anwendungen, Assets, Schwachstellen, Schutzbedarfen und technischen Kontrollen. Das Risikocontrolling denkt stärker in Risikoereignissen, Eintrittshäufigkeiten, Schadensauswirkungen und aggregierten Risikopositionen. Beide Perspektiven sind notwendig. Sie müssen jedoch über eine gemeinsame Szenario Logik verbunden werden. Eine identifizierte technische Schwachstelle allein ist noch kein operationelles Risikoszenario. Ein integriertes Szenario könnte beispielsweise lauten:

Aufgrund eines fehlerhaften Releases beim extern betriebenen Kernbankservice kommt es zu einem mehrstündigen Systemausfall. Zahlungsverkehrsprozesse können nicht fristgerecht ausgeführt werden. Manuelle Ersatzverfahren reichen aufgrund des Transaktionsvolumens nicht aus. Daraus entstehen Kundenbeeinträchtigungen, Nachbearbeitungskosten, mögliche regulatorische Folgen und Reputationsschäden.

Das Szenario verbindet eine technische beziehungsweise dienstleisterbezogene Ursache mit einem konkreten Ereignis, dem betroffenen Geschäftsservice, vorhandenen

IKT-Risiken systematisch
in das Risk Self Assess-
ment einbinden

Kontrollen und den finanziellen sowie nichtfinanziellen Auswirkungen. Erst dadurch wird aus einem technischen Problem ein bewertbares operationelles Risiko.

IKT-Risiken sollten weder isoliert neben dem Operational-Risk-Management gesteuert noch pauschal in einer allgemeinen OpRisk-Kategorie zusammengefasst und mit einem allgemein gültigen Risikopuffer versehen werden. Erforderlich sind eine gemeinsame Datengrundlage und eine abgestimmte Bewertungslogik.

Ausgangspunkt des Risk Self Assessments sollten kritische Geschäftsservices und End-to-End-Prozesse sein. Anschließend ist zu analysieren, von welchen Anwendungen, Infrastrukturen, Daten, Personen und internen oder externen Dienstleistern diese abhängen. Dadurch können unter anderem folgende Szenarien systematisch berücksichtigt werden:

- ≡ Ausfälle interner oder ausgelagerter IKT-Services
- ≡ Cyberangriffe und Datenmanipulation,
- ≡ Fehler bei Änderungen und Software-Releases,
- ≡ Unzureichende Berechtigungssteuerung,
- ≡ Datenqualitäts- und Schnittstellenfehler,
- ≡ Unwirksame Notfall- und Wiederanlaufverfahren,
- ≡ Dienstleister-, Konzentrations- und Subdienstleisterrisiken,
- ≡ Fehlende oder nicht praktikable Exit-Möglichkeiten.

Dabei muss nicht für jedes einzelne IKT-Asset⁴ ein separates OpRisk-Szenario angelegt werden. Entscheidend ist, dass die mögliche Auswirkung auf Geschäftsprozesse und kritische Funktionen herausgearbeitet wird.

Die Verbindung zwischen IKT- und OpRisk-Management erfolgt dabei über den betroffenen Geschäftsprozess bzw. die kritisch wichtigen Funktionen: Erkenntnisse zu IKT-Bedrohungen, Schwachstellen, Abhängigkeiten und Kontrollen bilden den Input für die Ableitung und Bewertung entsprechender operationeller Risikoszenarien.

Beispielsweise muss der Ausfall einer einzelnen Anwendung nicht als eigenständiges OpRisk-Szenario bewertet werden. Unterstützt die Anwendung jedoch den Zahlungsverkehr, kann ihr Ausfall als Ursache in ein übergeordnetes Szenario „Unterbrechung

⁴ Eine vom Institut genutzte Software- oder Hardwarekomponente innerhalb seines Netzwerk- und Informationssystems. Beispiele sind Anwendungen, Server, Endgeräte, Netzwerkkomponenten oder Datenbanken.

des Zahlungsverkehrs infolge eines IKT-Ausfalls“ einfließen. Die technische Ursache und die Wirksamkeit der IKT-Kontrollen werden aus dem IKT-Risikomanagement übernommen, während im OpRisk-Self-Assessment die Auswirkungen auf den Geschäftsprozess, etwa finanzielle Schäden, Betriebsunterbrechungen oder regulatorische Folgen, bewertet werden.

Bereits vorhandene Informationen sollten hierfür gemeinsam genutzt werden: IKT-Risikobewertungen, Business-Impact-Analysen, Schutzbedarfe, interne und externe Verlustereignisse, Vorfälle, Schwachstellen, Prüfungsfeststellungen, Notfalltests, Service-Level-Verletzungen und Dienstleisterbewertungen. Wiederholt verfehlte Wiederanlaufziele oder bekannte Schwachstellen dürfen nicht ausschließlich im IT- oder BCM-Bereich verbleiben. Sie müssen auch die Kontrollbewertung und das Residualrisiko im Risk Self Assessment beeinflussen.

Zielbild einer integrierten Steuerung

Für eine wirksame Verzahnung sind vor allem fünf Bausteine erforderlich:

1. Gemeinsame Taxonomie: IKT-, Cyber-, Informationssicherheits-, Drittparteien- und OpRisk-Kategorien werden über ein verbindliches Mapping verbunden. Eine erste Orientierung zur integrierten Risikotaxonomie hat die EBA in ihrem finalen Report (EBA/RTS/2025/03) bereits veröffentlicht.⁵
2. Abgestimmter Risikoappetit: IKT-Toleranzen werden aus dem übergreifenden Risikoappetit, der Kritikalität der Geschäftsservices und den Auswirkungstoleranzen abgeleitet.
3. Gemeinsame Kennzahlenbibliothek: KPIs und KRIs werden zentral definiert und Risiken, Kontrollen, Schwellenwerten und Verantwortlichen zugeordnet.
4. Verzahnte Bewertungs- und Berichtsprozesse: IKT-Risikobewertungen, Risk Self Assessments, Szenarioanalysen, Business-Impact-Analysen und Drittparteienbewertungen greifen aufeinander zurück.
5. Klare Governance: IT-Governance und Informationssicherheit bewerten technische Ursachen und Kontrollen. Die Fachbereiche verantworten Prozesse, Auswirkungen und Risiken. Das Risikocontrolling stellt Methodenkonsistenz, Aggregation und Überprüfung sicher. Das Leitungsorgan genehmigt Risikoappetit und Toleranzen und entscheidet über wesentliche Überschreitungen.

⁵ Vgl. [EBA/RTS/2025/03](#) S.8

Fazit

Die wirksame Steuerung von IKT-Risiken erfordert mehr als ein eigenständiges DORA-Framework. Entscheidend ist die konsequente Verzahnung von IT-Governance, Informationssicherheit, Risikocontrolling und Operational-Risk-Management. Risikoappetit, Toleranzgrenzen, KPIs, KRIs, Szenarioanalysen, Drittparteienrisiken und Management Reporting müssen auf einer gemeinsamen Methodik und Datenbasis aufbauen. Erst wenn technische Sachverhalte in geschäftliche Auswirkungen übersetzt und in Risk Self Assessments, Entscheidungsprozesse und die Gesamtbanksteuerung integriert werden, entsteht ein konsistentes Risikobild. Die regulatorischen Anforderungen aus DORA, MaRisk und der zugehörigen DelVo unterstreichen damit eine zentrale Botschaft: Nicht zusätzliche Einzelprozesse schaffen Resilienz, sondern ein durchgängiger Steuerungskreislauf mit klaren Verantwortlichkeiten, messbaren Toleranzen und wirksamen Eskalationsmechanismen.

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