Friederike Krüsemann
Henning Heuter

QUALITÄT VOR QUANTITÄT IM IKS

WIE DAS INTERNE KONTROLLSYSTEM RISIKOORIENTIERT AUSGESTALTET WERDEN KANN

EINLEITUNG

Dieser Fachbeitrag ist Teil der Fokus-Reihe Non Financial Risk (NFR) und beschäftigt sich mit der Qualität im Internen Kontrollsystem (IKS), nachdem der letzte Beitrag die Risikokultur in den Blickwinkel genommen hat.

In der Praxis von Banken und Finanzdienstleistern lässt sich häufig ein Phänomen beobachten, das als „Kontroll-Inflation“ bezeichnet werden kann: Als Reaktion auf regulatorische Feststellungen oder historische Einzelfälle werden kontinuierlich neue IKS-Kontrollen etabliert. Das Ergebnis ist ein bürokratisches, träges IKS, das erhebliche Ressourcen bindet, ohne die Risikolage des Instituts zu verbessern. Wenn Kontrollaufwände in keinem angemessenen Verhältnis zu den potenziellen finanziellen Schäden stehen, verfehlt das IKS seinen Zweck.

Eine risikoorientierte und zielgerichtete Ausgestaltung des IKS ist daher nicht nur eine regulatorische Anforderung (z. B. gemäß MaRisk), sondern ein Gebot der wirtschaftlichen Vernunft. Doch wie gelingt der Wandel von der Kontroll-Quantität zur Kontroll-Qualität?

NATIONALE REGULATORISCHE ANFORDERUNGEN AN DAS IKS

Im Folgenden wird eine Auswahl der wichtigsten regulatorischen Anforderungen an das IKS dargestellt.

Anforderungen nach § 25a KWG und MaRisk (4.3)

Finanzinstitute sind nach dem KWG und den MaRisk dazu verpflichtet, ein umfassendes und angemessenes Risikomanagement einzurichten. Das inkludiert ein internes Kontrollverfahren, welches Regelungen zur Aufbau- und Ablauforganisation, zum internen Kontrollsystem, zur Risikocontrolling- sowie Compliance-Funktion und zur Internen Revision umfassen muss. Wichtig ist, dass die Interne Revision losgelöst von allen weiteren Kontrollfunktionen und Geschäftsbereichen etabliert ist. Weiterhin muss das Risikomanagement wesentliche Risiken frühzeitig identifizieren,

beurteilen, steuern und überwachen. Ein weiterer Punkt betrifft die Notwendigkeit der angemessenen Kommunikation der Risiken.

Aufbau- und Ablauforganisation

Für Tätigkeiten, die miteinander unvereinbar sind, muss sichergestellt werden, dass sie durch unterschiedliche Mitarbeiter durchgeführt werden. Zusätzlich müssen angemessene Übergangsfristen bei einem internen Wechsel, der zu Interessenkonflikten führen könnte, vorgesehen sein. Eine klare Definition und Abstimmung von Prozessen, Aufgaben, Kompetenzen oder Kommunikationswegen ist Voraussetzung. Außerdem muss sichergestellt werden, dass Berechtigungen und Kompetenzen nach dem Need-to-know-Prinzip vergeben werden. Dies muss regelmäßig überprüft werden.

Risikosteuerungs- und -controllingprozesse

Die MaRisk verlangen angemessene Prozesse zur Identifizierung, Beurteilung, Steuerung, Überwachung und Kommunikation der wesentlichen Risiken, welche in die Gesamtbanksteuerung eingebunden sind. Zur Identifizierung sollen geeignete Indikatoren genutzt werden. Die gesammelten Informationen müssen mindestens vierteljährlich schriftlich und im kritischen Fall unverzüglich an die Geschäftsleitung übermittelt werden, damit rechtzeitig Maßnahmen eingeleitet werden können.

Zur wirksamen Begrenzung von Risiken und Risikokonzentrationen können quantitative Instrumente wie Limitsysteme sowie ergänzende qualitative Analysen in die übergeordnete Gesamtbanksteuerung integriert werden. Voraussetzung hierfür ist die lückenlose Vorhaltung aller steuerungsrelevanten Daten.

Alle gesetzten Methoden und Verfahren müssen regelmäßig auf ihre Eignung überprüft werden.

Anforderungen aus dem AktG (§91 und §93)

Laut Aktiengesetz muss der Vorstand geeignete und wirksame Maßnahmen treffen, um gefährdende Entwicklungen frühzeitig zu erkennen. Darunter fallen Überwachungs-, Kontroll- und Risikomanagementsysteme. Laut dem Gesetz zur Stärkung der Finanzmarktintegrität gelten Systeme als wirksam, wenn sie zur Aufdeckung, Steuerung und Bewältigung wesentlicher Risiken geeignet sind.

Ist ein Unternehmen nicht an der Börse notiert, liegt die Einrichtung solcher Systeme im Ermessen des Vorstands. §93 des AktG regelt allerdings die Sorgfaltspflicht für Vorstandsmitglieder, woraus resultiert, dass lediglich die genaue Umsetzung solcher Systeme zu hinterfragen ist. Dass es grundsätzlich Systeme, die Gefahren erkennen, geben muss, steht außer Frage.

ANFORDERUNGEN AUS BCBS239 UND RDARR

Die **Grundsätze für die effektive Aggregation von Risikodaten und die Risikoberichterstattung (BSBC239)** wurde vom Basler Ausschuss für Bankenaufsicht veröffentlicht und ist seit 2016 verpflichtend. Das RDARR Framework (Effective risk data aggregation and risk reporting) bezieht sich auf BCBS239 und beschreibt die konkrete operative Umsetzung des Regelwerks.

Beide Regularien gelten für die EZB-beaufsichtigten Banken, bieten aber ebenso gute Hilfestellung für die gelungene Umsetzung bei allen anderen Instituten.

Das Ziel von RDARR und BCBS239 ist es, mithilfe einer hohen Datenqualität und aller damit einhergehenden Prozesse das Risikomanagement zu stärken und so die strategische Steuerung zu erleichtern. Zu diesem Zweck werden 7 Erwartungspunkte formuliert:

© 2026 1 PLUS i GmbH

Erwartung	Erklärung
Verantwortung des Managements	Das Management ist für die Überwachung der strategischen Ziele, der Risikostrategie und der internen Governance zuständig, zusätzlich muss es die Verantwortlichkeiten und das notwendige Know-how sicherstellen.
Anwendungsbereich	Zur Identifizierung, Steuerung, Überwachung und Meldung von Risiken soll ein Data Governance Framework festgelegt werden. Dieses wird angewandt, sobald Risikomodelle, Risikoindikatoren und die übergeordneten Berichte betroffen sind.
Effektives Daten-Governance-Framework	Im Institut müssen Rollen und Verantwortlichkeiten klar definiert sein. Dies umfasst mindestens die Dateneigentümer, die zentrale Data-Governance-Funktion und die Interne Revision.
Integrierte Daten-Architektur	Das Vorhandensein eines Data Dictionary mit Definitionen, Dateneigentümern, Validierungsregeln und Informationen zur Datenherkunft stellt eine hohe Datenqualität sicher.
Gruppenweites Datenqualitätsmanagement und Standards	Die Etablierung von Richtlinien und Prozessen gewährleistet effektive und vollständige Datenqualitätskontrollen, die zur Behebung wesentlicher Probleme führen und zu der Möglichkeit, Datenqualitätsrisiken im ICAAP und ILAAP zu berücksichtigen.
Aktualität des internen Risiko-Reportings	Es muss gewährleistet sein, dass zeitnah auf Änderungen in der Risikolage reagiert werden kann. Dementsprechend muss die Berichtshäufigkeit an die potenziellen Änderungen von Risikozahlen angepasst sein.
Effektive Implementierung	Sollten durch interne oder externe Prüfungen Schwächen aufgedeckt werden, muss eine zeitnahe Beseitigung sichergestellt werden.

WAS IST DAS IKS?

Das interne Kontrollsystem (IKS) ist kein isoliertes Prüfwerkzeug, sondern umfasst die Gesamtheit aller systematisch aufeinander abgestimmten Kontrollen und Kontrollprozesse innerhalb eines Instituts. Es fungiert als das unsichtbare Sicherheitsnetz des Unternehmens, das tief in die täglichen Betriebsabläufe integriert ist.

Ein funktionsfähiges und lebendiges IKS ist für jedes Institut unerlässlich. Es dient als zentrales Steuerungselement, um regulatorische Vorgaben und gesetzliche Rahmenbedingungen verlässlich einzuhalten. Das primäre Ziel ist dabei klar definiert: Die frühzeitige Identifikation und effektive Minimierung betrieblicher Risiken, um finanzielle Schäden, Reputationsverluste und Verstöße gegen die Regulatorik konsequent zu vermeiden.

Über den reinen Schutzgedanken hinaus sichert ein starkes IKS jedoch auch die Genauigkeit der Finanzberichterstattung sowie die Effizienz der Geschäftsprozesse. Die Vermeidung von schlechten Entscheidungen, insbesondere auf Managementebene durch fehlerhafte Risikoreports, ist eines der Hauptziele. Das IKS schafft somit das notwendige Vertrauen, das in einem dynamischen Marktumfeld einen wichtigen Stabilitätsfaktor darstellt und die Erfüllung der Anforderungen der Aufsichtsbehörden unterstützt.

© 2026 1 PLUS i GmbH

IKS: CHANCEN UND HERAUSFORDERUNGEN

Die Ausgestaltung eines IKS sollte gut abgewogen werden. Die größte Herausforderung in der Praxis liegt darin, die richtige Balance zwischen zu vielen und zu wenigen Kontrollen zu finden. Viel hilft hier eben nicht viel. Wird das System mit Kontrollen überfrachtet, droht der berüchtigte „Papiertiger“: Ein bürokratisches Monster, das auf dem Papier lückenlos wirkt, in der Realität jedoch die Prozesse lähmt und von den Mitarbeitern nicht mehr getragen werden kann.

Besonders deutlich wird dies bei der Frage, wie viel Vier-Augen-Prinzip (4AP) im Alltag überhaupt realistisch ist. Wenn viele Kleinstschritte getätigt werden müssen, verkommt die Kontrolle zur reinen Formsache – es wird blind unterschrieben und der eigentliche Sicherheitsgewinn geht verloren. Kontrollen müssen im Arbeitsalltag gelebt werden können, sonst verliert das Institut die essenzielle Risikoorientierung aus den Augen. Man konzentriert sich vor lauter Kontroll-Aktivismus auf die Masse statt auf die tatsächlich bedrohlichen Risiken.

Aus diesen Herausforderungen erwachsen jedoch auch Chancen, wenn das Prinzip „Qualität vor Quantität“ konsequent angewendet wird:

- **Effizienz und Akzeptanz:** Ein schlankes, risikoorientiertes IKS entlastet die operativen Einheiten. Wenn Mitarbeiter verstehen, warum eine Kontrolle wichtig ist und diese zeiteffizient umsetzbar ist, verbessert sich die Risikokultur im Unternehmen.
- **Verlässliche Basis für Managemententscheidungen:** Ein qualitativ hochwertiges IKS liefert präzise, aussagekräftige Berichte. Das Management erhält so ein klares Bild der tatsächlichen Risikolage und kann strategische Entscheidungen auf fundierter Basis treffen.
- **Resilienz statt Scheinsicherheit:** Indem Scheinkontrollen eliminiert und Schlüsselkontrollen gestärkt werden, wandelt sich das IKS von einer lästigen Pflichtaufgabe zu einem strategischen Tool, das das Institut widerstandsfähiger gegen echte Bedrohungen macht.

IKS: KONTROLLE ODER MAßNAHME?

Um die Qualität eines IKS zu steigern, muss zunächst begriffliche Klarheit herrschen. In der Praxis werden „IKS-Maßnahmen“ und „IKS-Kontrollen“ oft in einen Topf geworfen. Das führt dazu, dass die IKS-Dokumentation künstlich aufgebläht wird, weil jeder Arbeitsschritt als Kontrolle deklariert wird. Für ein schlankes und wirksames IKS ist die Differenzierung somit fundamental.

Eine Maßnahme (oft auch als Richtlinie, Arbeitsanweisung oder Prozessschritt definiert) beschreibt die grundsätzliche Ausgestaltung eines Arbeitsablaufs. Sie gibt vor, *wie* eine Aufgabe ordnungsgemäß zu erledigen ist, um Risiken von vornherein zu minimieren oder prozessuale Standards zu sichern.

- Beispiel: Die Vorgabe, dass Stammdaten von Kunden im System zunächst vollständig erfasst werden müssen und anschließend der Personalausweis angeschaut, mit den angegebenen Daten abgeglichen und schließlich eingescannt und abgelegt wird, ist eine Maßnahme. Sie ist Teil der operativen Arbeiten.

Eine Kontrolle hingegen setzt genau dort an, wo die Maßnahme aufhört. Sie ist ein eigenständiger, nachgelagerter oder begleitender Prüfschritt, der explizit darauf ausgelegt ist, die Einhaltung der Maßnahmen zu überwachen oder Fehler im Prozess aufzudecken. Eine Kontrolle stellt sicher, dass das Soll-Ergebnis tatsächlich erreicht wurde.

- Beispiel: Der automatisierte Systemabgleich, ob alle Pflichtfelder der Kundendaten befüllt sind und ein Dokument (Personalausweis) hinterlegt ist, ist die eigentliche Kontrolle.

Wer Maßnahmen und Kontrollen verwechselt, schafft Scheinsicherheit. Wenn ein Prozess aus zehn Schritten besteht und jeder Schritt blind als „Kontrolle“ deklariert wird, verliert das System an Fokus. Erst die gezielte Verknüpfung einer operativen Maßnahme mit einer darauf abgestimmten,

risikoorientierten Schlüsselkontrolle sichert die Qualität des IKS, ohne die Quantität unnötig in die Höhe zu treiben.

IKS-KONTROLLEN: LÖSUNGS-ANSÄTZE

Aber wie kann man konkret den Übergang von Quantität zur Qualität schaffen? Im Folgenden werden fünf Ansätze skizziert, wie IKS-Kontrollen risikoorientiert ausgestaltet werden können:

Konsequente Verknüpfung von Risiko vor Kontrolle und nach Kontrolle

Der häufigste Grund für überdimensionierte Kontrollen ist eine unzureichende Verknüpfung zwischen der Risikoanalyse und dem Kontroll-Design. Kontrollen dürfen niemals im luftleeren Raum entstehen, sondern müssen direkt aus einer fundierten Bewertung der inhärenten Risiken (Risiko vor Kontrollen) abgeleitet werden.

Wesentlichkeitsgrenzen definieren: Institute müssen klare, quantifizierte Toleranzschwellen festlegen. Liegt der maximale potenzielle Schaden eines Risikos (vor Kontrolle) unter der Wesentlichkeitsgrenze, ist eine engmaschige, manuelle Kontrolle wirtschaftlich nicht zu rechtfertigen.

Fokus auf das Risiko nach Kontrolle (Restrisiko): Ziel einer Kontrolle ist es, das inhärente Risiko auf ein akzeptables Restrisiko-Niveau zu senken. Ist das Risiko ohnehin gering, reicht oft eine Basisüberwachung oder die bewusste Akzeptanz des Risikos aus.

Zusammengefasst bedeutet das, dass vor der Etablierung von Kontrollen das Risiko vor Kontrolle bewertet werden muss. Die Höhe dieses Risikos bzw. Schadens wird mit den Wesentlichkeitsgrenzen abgeglichen, woraus bestimmte Kriterien für eine Kontrollgestaltung folgen.

Im Folgenden wird beispielhaft skizziert, wie eine solche Gestaltung aussehen könnte:

Wesentlichkeits-grenze/ Risikopoten-zial vor Kontrolle	Reife-grad 1	Reife-grad 2	Reife-grad 3	Reife-grad 4	Reife-grad 5
‹ 5.000 EUR	X				
5.000 – 15.000 EUR		X			
15.001 – 25.000 EUR			X		
25.001 – 35.000 EUR				X	
› 35.000 EUR					X

Anforderungen an die Reifegrade:

- Reifegrad 1: Stichprobenartige präventive Kontrollen des ausführenden Mitarbeiters
- Reifegrad 2 Stichprobenartige präventive Kontrollen im Vier-Augen-Prinzip, standardisierte Dokumentation notwendig
- Reifegrad 3: Vollständige präventive Kontrollen im Vier-Augen-Prinzip, standardisierte Dokumentation notwendig, wird auf aggregierter Datenbasis auf Wirksamkeit geprüft
- Reifegrad 4: Vollständige präventive Kontrollen im Vier-Augen-Prinzip, standardisierte Dokumentation notwendig, wird auf Einzeldatenbasis auf Wirksamkeit geprüft
- Reifegrad 5: Automatisierte Kontrolle muss eingeführt werden

Dieser Ansatz wird im nächsten Fachbeitrag ausführlich vorgestellt.

© 2026 1 PLUS i GmbH

Der Top-Down-Ansatz statt Bottom-Up-Wildwuchs

Viele Kontrollsysteme wachsen historisch von unten nach oben (Bottom-Up): Jeder Fachbereich sichert sich gegen jede denkbare Eventualität ab. Ein zielgerichtetes IKS erfordert hingegen einen Top-Down-Ansatz:

1. **Definition der Kernrisiken:** Welche Risiken bedrohen die Geschäftsstrategie, die regulatorische Compliance oder die finanzielle Stabilität des Instituts wirklich?
2. **Identifikation der Schlüsselkontrollen:** Schlüsselkontrollen werden für Risiken ab einem gewissen Schadenspotenzial gesetzt. Dieses Schadenspotenzial muss von jedem Institut definiert werden und sollte eine reale Gefahr, wenn das Risiko eintritt, widerspiegeln. Statt vieler Kleinstkontrollen sollte sich das Institut auf die wirksame Ausgestaltung jener Schlüsselkontrollen konzentrieren.
3. **Eliminierung von Redundanzen:** Durch eine systematische Inventur des Kontrollrahmens lassen sich Doppelarbeit und parallele Kontrollstränge in unterschiedlichen Abteilungen identifizieren und abschaffen. Werden beispielsweise Daten für ein Risikoreporting aus einem System genutzt, für welches bereits Kontrollen implementiert sind, kann an dieser Stelle auf weitere Kontrollen verzichtet werden.

Effizienzsteigerung durch die Auswahl passender Kontrollarten

Manuelle Kontrollen (Vier-Augen-Prinzip via E-Mail, Unterschriftenmappen etc.) sind fehleranfällig, binden wertvolle Personalkapazitäten und verleiten dazu, Kontrolle um der Kontrolle Willen zu betreiben. Risikoorientierung bedeutet auch, die Kontrollart dem Risiko anzupassen:

- **Präventiv vor Detektiv:** Präventive Kontrollen (z. B. systemseitige Berechtigungsprüfungen, Pflichtfelder) verhindern Fehler, bevor sie entstehen. Sie sind meist effizienter als detektive Kontrollen (z. B. Abgleichlisten), die im Nachgang aufwendig aufgearbeitet werden müssen.
- **Automatisierung forcieren:** Wo immer möglich, sollten Kontrollen in die IT-Systeme integriert werden. Automatisierte Kontrollen laufen standardisiert, verursachen nach der Implementierung kaum Grenzkosten und reduzieren den menschlichen Faktor im Kontrollprozess.
- **Aggregierte Daten kontrollieren:** Geht es um die Kontrolle von Daten, kann auf aggregierter Ebene gearbeitet werden. Sollten dort Fehler festgestellt werden, kann dieser Datenstamm granular analysiert werden. Sollte jedoch keine Auffälligkeit auftreten, können alle Einzeldaten als kontrolliert betrachtet werden.

Etablierung einer Challenge-Funktion (2nd Line of Defense)

Um die Verhältnismäßigkeit von Maßnahmen sicherzustellen, bedarf es einer unabhängigen Instanz, die als kritischer Sparringspartner für die Fachbereiche (1st Line of Defense) agiert. Diese Rolle kommt dem zentralen IKS-Management oder dem Risikocontrolling zu. Ein Ziel dieser Rolle ist es, ein einheitliches Vorgehen im gesamten Institut sicherzustellen. Da es unterschiedlichste Mitarbeiter und Ansichten gibt, gehen auch die Arbeitsweisen oder persönlichen Anforderungen teilweise weit auseinander. Dies sollte im Rahmen gehalten werden, um einer einheitlichen Linie zu folgen.

- **Abgleich Risiko vor und nach Kontrolle:** Das IKS-Management muss bei der Neueinführung jeder Kontrolle die Beantwortung folgender Frage einfordern: Welches konkrete Risiko wird hier in welchem Ausmaß reduziert und steht dieser Nutzen im Verhältnis zu den laufenden Kosten?

© 2026 1 PLUS i GmbH

- **Regelmäßige Wirksamkeits- und Effizienzprüfungen:** Kontrollen dürfen nicht für die Ewigkeit gebaut sein. Im Rahmen des jährlichen IKS-Regelkreises muss geprüft werden, ob bestehende Kontrollen überhaupt noch notwendig sind (z. B. weil sich die IT-Landschaft geändert hat) oder ob sie aufgrund veränderter Risikolagen angepasst werden sollten.

Kulturwandel: Fehler- und Risikokultur stärken

Die Tendenz zur Überkontrolle ist oft das Symptom einer defensiven Unternehmenskultur, in der Fehler absolut tabu sind und Mitarbeiter sich durch den Aufbau von Kontrollbergen absichern wollen.

- **Risikoappetit beachten (Mut zur Lücke):** Das Management muss beispielsweise über die Risikostrategie transparent kommunizieren, dass das Eingehen und Akzeptieren von Kleinstschäden ökonomisch sinnvoller ist als die (scheinbar) vollständige Eliminierung des Risikos durch teure Kontrollprozesse.
- **Verantwortung stärken:** Prozessverantwortliche (Process Owner) sollten auch die Kosten- und Effizienzverantwortung für ihre Kontrollen tragen. Wenn der Aufwand für das IKS das eigene Budget belastet, schärft dies den Blick für das Wesentliche.

ZUSAMMENFASSUNG UND FAZIT

Ein effektives IKS in Finanzinstituten zeichnet sich nicht durch die Anzahl seiner Kontrollen aus, sondern durch deren Treffsicherheit. Um eine Kontroll-Inflation zu verhindern, müssen Institute den Mut aufbringen, Risiken zu quantifizieren, Kleinstrisiken bewusst zu akzeptieren und sich auf automatisierte Schlüsselkontrollen zu fokussieren. Nur so transformiert sich das IKS von einem bürokratischen Papiertiger zu einem strategischen Steuerungsinstrument, das Risiken minimiert und gleichzeitig die operative Handlungsfähigkeit wahrt.

UNTERSTÜTZUNG DURCH 1 PLUS i

Sie möchten noch mehr im Zusammenhang mit der Qualitätssteigerung bei IKS-Kontrollen wissen oder mit uns zu diesen Themen diskutieren? Die 1 PLUS i GmbH unterstützt Sie neben der Klärung spezifischer Fragen insb. auch bei der konkreten Umsetzung, beispielsweise bei der Erarbeitung von Wesentlichkeitsgrenzen, der Identifikation von Schlüsselkontrollen, der Implementierung von verantwortlichen Rollen und Funktionen oder Abgleichtools, die für Ihr Institut entwickelt werden.

Wir bieten einen umfassenden Ansatz, in dem wir die gesamte Umsetzung begleiten, oder Quickcheck-Lösungen bzw. Workshops, die wir Ihnen in Form von Inhouse-Kundenworkshops sehr gern vorstellen. Sprechen Sie uns doch einfach an!

Ihr 1 PLUS i Team

AUTOREN

HENNING HEUTER
henning.heuter@1plusi.de

FRIEDERIKE KRÜSEMANN
friederike.krüsemann@1plusi.de

© 2026 1 PLUS i GmbH