IKSPraktiker
COMPLIANCE • RECHT • REVISION

Mittwoch, 31. August 2022

Mehrwert eines datenbasierten Risikodialogs für ein gelebtes IKS

Ein Erfahrungsbericht über das Vorgehen in der kontinuierlichen Verbesserung des Internen Kontrollsystems und die Bedeutung von Kommunikation auf Basis von Daten

Christina-Maria Martin, Senior Referentin IKS, Organisation, KfW IPEX-Bank
Alexa Schulz, Senior Managerin, Cofinpro AG

I. Die KfW IPEX-Bank und ihre Aufstellung im Internen Kontrollsystem

Die KfW IPEX-Bank verantwortet innerhalb der KfW-Bankengruppe die Export- und Projektfinanzierung. Mit der Strukturierung mittel- und langfristiger Finanzierungen für deutsche und europäische Exporte, Infrastrukturinvestitionen und Rohstoffsicherung sowie Umwelt- und Klimaschutzprojekte auf der ganzen Welt unterstützt sie heimische Unternehmen der industriellen Schlüsselsektoren auf den globalen Märkten.

Als Spezialbank verfügt die KfW IPEX-Bank über eine umfassende Branchen-, Strukturierungs- und Länderkompetenz. Sie übernimmt in Finanzierungskonsortien führende Rollen und bindet andere Banken, institutionelle Investoren und Versicherungen aktiv ein. Sie wird als rechtlich selbstständiges Konzernunternehmen geführt und ist neben ihrem Hauptsitz in Frankfurt am Main mit derzeit elf Standorten in den wichtigsten Wirtschafts- und Finanzzentren der Welt vertreten.

Die KfW IPEX-Bank stellte im Bereich der Export- und Projektfinanzierung im Jahr 2021 Kredite in Höhe von 13,6 Mrd. EUR bereit und verantwortete ein Kreditvolumen von 68,5 Mrd. EUR. Sie beschäftigte 876 Mitarbeitende (Stand 31.12.2021). Mit Blick auf das Geschäftsmodell ist der Herausforderung an ein Internes Kontrollsystem, den spezifischen Risiken in den hochgradig individuellen Prozessen der internationalen Projekt- und Exportfinanzierung angemessen und wirksam Rechnung zu tragen. Den Fokus legt die KfW IPEX-Bank dabei auf ein durchgängiges Risikoverständnis und die aktive Einbindung aller Mitarbeitenden im erfolgreich realisierten **Three-Lines-of-Defense-Modell**. Damit fördert sie die bereichsübergreifende Kooperation in der Ausgestaltung ihrer internen Kontrollverfahren.

Abbildung 1: Aufstellung der KfW IPEX-Bank nach dem Three-Lines-of-Defense-Modell

Für die Ausgestaltung und Operationalisierung ihres Internen Kontrollsystems hat die KfW IPEX-Bank eine **zentrale IKS-Evidenzstelle** eingerichtet, die parallel die Verantwortung für die Abbildung der Risiko- und Kontrollinformationen in der prozessorientierten schriftlich fixierten Ordnung trägt. Die zentrale IKS-Evidenzstelle ist in der Abteilung Organisation & IT verankert. Für die Ausgestaltung ihres Anweisungswesens hat sich die KfW IPEX-Bank für eine Kombination aus zentraler Methoden- und Dokumentationsverantwortung und dezentraler Fachverantwortung entschieden. Speziell in der Bewertung und Steuerung prozessinhärenter Risiken durch ein risikoadäquates Prozess- und Kontrolldesign greift sie auf einen Expertenkreis von rund 100 Prozessverantwortlichen zu. Damit trägt sie als Spezialbank der Komplexität und Individualität ihrer hochvolumigen und risikobehafteten Einzelgeschäftsvorgänge entsprechend Rechnung.

Aufbau und Ausgestaltung des Internen Kontrollsystems orientieren sich an den **COSO-Prinzipien** unter Berücksichtigung konzernweit geltender Leitplanken. Die Transparenz über prozessinhärente Risiken und darauf abgestellte Kontrollvorgaben schafft die KfW IPEX-Bank über eine **verbindliche Abbildung prozessintegrierter Kontrollen** in ihrer nach Front-to-End-Prinzipien ausgerichteten Prozesslandkarte. Diese liefert auf Prozessebene **maschinell auswertbare Risiko- und Kontrollinformationen**, die allen Mitarbeitenden zugänglich sind. Zur Prozessdokumentation nutzt die KfW IPEX-Bank die Software *Adonis*. Ergänzend führt die zentrale IKS-Evidenzstelle ein Risikokontrollinventar, das die Beziehung von Risiken und Kontrollen auf Prozessebene visualisiert.

II. Ziele und Vorgehen in der Entwicklung eines gelebten Internen Kontrollsystems

Nach der erfolgreichen Implementierung einer **IKS-Governance als Handlungs- und Steuerungsrahmen** sowie der Definition und Einführung des Three-Lines-of-Defense-Modells hat die KfW IPEX-Bank im 4. Quartal 2020 mit externer Unterstützung das Projekt „IKS-Risikoeinwertung von Prozessen“ aufgesetzt. Der Projektauftrag beinhaltete die Entwicklung und bankweite Einführung einer **IKS-Relevanzanalyse** zur Erhebung und Beurteilung der prozessinhärenten Risiken und Kontrollen. Die mit dieser Methode gewonnenen Risiko- und Kontrollinformationen bilden die Basis zur Vernetzung der Risikoperspektiven in den drei Verteidigungslinien und der Entwicklung eines gemeinsamen und wahrnehmbaren Risikoverständnisses.

1. Ziele im Projekt „IKS-Risikoeinwertung von Prozessen“

An erster Stelle stand der Bedarf nach Transparenz über alle prozessinhärenten Risiken und prozessintegrierten Kontrollen. Daraus entwickelte sich schnell der Wunsch, mit Kenntnis über die Risiko- und Kontrollstruktur in einen fachbereichsübergreifenden Risikodialog zu treten. Als Voraussetzung für den bankweiten Austausch wurde die Dokumentation und Auswertbarkeit der Risiko- und Kontrollinformationen auf Basis einheitlicher Standards realisiert.

- **Transparenz** über Risiko- und Kontrollstruktur auf Prozessebene und **Nachvollziehbarkeit** auch gegenüber Dritten
  - Welche Risiken führen zur IKS-Relevanz?
  - Welche Kontrollen decken die Risiken ab?
- Schaffen einer angemessenen und vertrauensfördernden **Kontrollkultur** auf Basis eines durchgängigen **Risikoverständnis**
  - Sind Kontrollen prozessspezifisch und angemessen in Umfang und Ausgestaltung?
  - Sind Kontrollen nachvollziehbar?
- Standardisierte **Dokumentation** aller prozessbezogenen Risiken und Kontrollen
- **Generierung von Reports** aus Adonis heraus z.B.
  - Ableitung einer Risiko-Kontroll-Matrix
  - Kontrollübersicht im Kontext von Prüffeldern der Revision

Abbildung 2: Ziele im Projekt „IKS-Risikoeinwertung von Prozessen“

2. Pilotierung der IKS-Relevanzanalyse als Grundstein für den Risikodialog

Im iterativen Prozess wurde projekthaft eine Excel-basierte Vorlage „IKS-Relevanzanalyse“ zur strukturierten Erhebung und Bewertung prozessinhärenter Risiken entwickelt und pilotiert. Diese Methode sollte Fachbereichen in ihrer Rolle als erste Verteidigungslinie ermöglichen, eigenständig eine **„bottom-up“-Beurteilung der prozessspezifischen Risiken und Kontrollen** durchzuführen. Auf Basis der ermittelten Prozesskritikalität validierten

MaRisk 8.0-E – Umsetzung der EBA/GL/2020/06

Überblick und kritische Würdigung der MaRisk 8.0 mit Schwerpunkt EBA GL

08.11.2022 Lesen

Umsetzung eines wirksamen IKS im Bereich der Banksteuerung

Messbare, relevante Schlüsselkontrollen im Risikocontrolling-Prozess

02.09.2022 Lesen

Kreditvergabe- und Überwachungsprozesse bei Schiffsfinanzierungen

Überarbeitete aufsichtliche Anforderungen an Kreditvergabe- und Überwachungsprozesse bei Schiffsfinanzierungen

06.10.2022 Lesen

Prozessverantwortliche den risikoabhängigen Bedarf an Kontrollen und nahmen eine erste Überarbeitung in der Beschreibung von Kontrollvorgaben auf Basis einheitlicher Parameter vor.

Die erhobenen Daten wurden durch die zentrale Evidenzstelle in der prozessorientierten schriftlich fixierten Ordnung dokumentiert und ausgewertet. Dadurch wurden Risken und Kontrollen nachvollziehbar in Beziehung gesetzt. Durch Visualisierung der Risiko- und Kontrollinformationen schaffte die KfW IPEX-Bank mit der IKS-Relevanzanalyse die Grundlage für einen bankweiten Risikodialog.

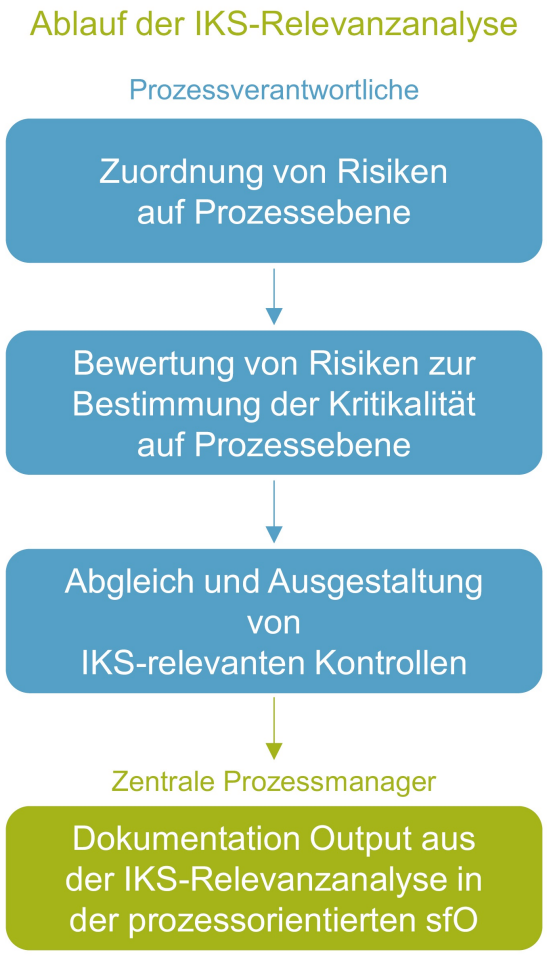


Abbildung 3: Ablauf der IKS-Relevanzanalyse zur Bottom-up-Beurteilung prozessinhärenter Risiken und Kontrollen

3. Von der Pilotierung zur bankweiten Praxis – einen IKS-Regelkreis zum Leben erwecken

Nach dem initialen Aufsatz einer MaRisk-konformen IKS-Governance auf Ebene der zweiten Verteidigungslinie und der pilothaften Bottom-up-Erhebung der Risiko- und Kontrollstruktur durch die erste Verteidigungslinie stand die Frage im Vordergrund, wie sich auf dieser Grundlage ein in der Breite gelebter IKS-Regelkreis entwickeln lässt. Die IKS-Relevanzanalyse sollte nach dem Rollout keine Eintagsfliege bleiben. Auf folgende Fragen galt es, eine Antwort zu finden:

- Wie werden Fachbereiche effizient eingebunden und ihrer Rolle als „Manager der operationellen Risiken“ in der Praxis gerecht?
- Wie werden die gewonnenen Risiko- und Kontrollinformationen in der Breite nutzbar und zur Verzahnung der Risikoperspektiven in den drei Verteidigungslinien genutzt?
- Wie sieht ein IKS-Regelkreislauf aus, der nachhaltig zur Steigerung des IKS-Reifegrads beiträgt?

4. Prämissen für den bankweiten Rollout der IKS-Relevanzanalyse

Die KfW IPEX-Bank hat sich bei der Weiterentwicklung ihres Internen Kontrollsystems auf Basis der IKS-Relevanzanalyse in der Praxis bewusst für ein ressourcenschonendes und dialogorientiertes Vorgehen entschieden. Folgende Prämissen haben Ausgestaltung und Begleitung des Rollouts der „IKS-Relevanzanalyse“ bestimmt:

- Risiko-Awareness und Risikokultur sind keine Worthülsen; sie werden gelebt und sind beobachtbar.
- Risikokultur basiert auf gegenseitigem Verstehen und Lernbereitschaft; sie erfordert und fördert einen übergreifenden und regelmäßigen Austausch zwischen allen Beteiligten.
- Ein effizienter Austausch bedingt Zugang zu Risiko- und Kontrollinformationen für alle Beteiligten.

- Die IKS-Relevanzanalyse ist für alle Fachbereiche einfach handhabbar; ihre Durchführung kann neben dem Tagesgeschäft eigenverantwortlich geleistet werden.
- Für die IKS-Relevanzanalyse gelten verbindliche Vorgaben für eine prüfungssichere Ausgestaltung und Dokumentation der Kontrollvorgaben im Rahmen der schriftlich fixierten Ordnung.

a) Mut zur Lücke in der Konzeption der IKS-Relevanzanalyse

Die IKS-Relevanzanalyse wurde innerhalb von acht Wochen entwickelt und erfolgreich pilotiert. Aufgrund des Geschäftsmodells mit seinen hochkomplexen Geschäftsvorgängen hat in der initialen Bewertung der Prozessrisiken und Kontrollallokation die Aufwandsperspektive in Abhängigkeit von der Quantität der Kontrollen bewusst noch keine Rolle gespielt. Mit dem Mut zur Lücke wurde der Fokus in der Risikobeurteilung auf die „Top 10“ der in den letzten Jahren identifizierten Risikoursachen gelegt. Die Überprüfung der Kontrollvorgaben auf Basis definierter Parameter für ein einheitliches Kontrolldesign lag von Anfang an in der Fachverantwortung der einzelnen Bereiche.

b) Face-to-Face-Kommunikation und individuelle Begleitung der Fachbereiche

Um schnell ins Lernen zu kommen, hat die KfW IPEX-Bank den bankweiten Rollout der IKS-Relevanzanalyse in zehn Wochen realisiert. Dazu wurden mit Einbindung aller Fachbereiche rund 400 Prozesse auf prozessinhärente Risiken bewertet und in diesem Zusammenhang rund 250 Kontrollen auf ihre Angemessenheit hin validiert.

Zur Einbindung der ca. 100 Prozessverantwortlichen und rund 60 Führungskräfte hat sich die KfW IPEX-Bank für **Informationsreihen im Remote-Format** entschieden. Neben der Hilfe zur Selbsthilfe hatten alle Prozessverantwortlichen die Möglichkeit zur bilateralen Unterstützung in der Anwendung der „IKS-Relevanzanalyse“ zur Bewertung der eigenen Prozesse.

Dabei hat die zentrale IKS-Evidenzstelle bewusst nur methodisch unterstützt. Die Fachbereiche als erste Verteidigungslinie haben die fachliche Verantwortung getragen. Sie haben so ein **initiales und unverfälschtes Bild über ihre Einschätzung der prozessinhärenten Risiken** geschaffen für den späteren Abgleich mit den Risikoperspektiven der zweiten und dritten Verteidigungslinie.

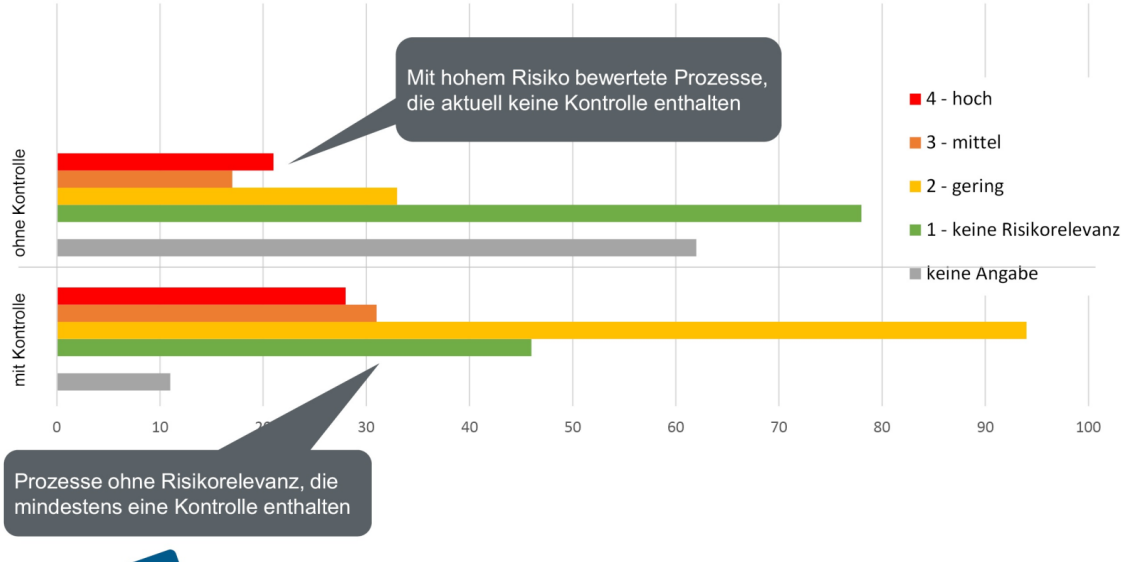
c) Dokumentation und Visualisierung von Risiko- und Kontrollinformationen

Die im Rollout gewonnenen Risiko- und Kontrollinformationen wurden durch die zentrale IKS-Evidenzstelle auf Prozessebene in *Adonis* erfasst und ausgewertet. Vier Monate nach dem Rollout lag die Risikosicht der ersten Verteidigungslinie in Zahlen und Fakten vor und konnte mit der zweiten Verteidigungslinie in Verantwortung für die übergreifende Steuerung der operationellen Risiken erstmals diskutiert werden.

Impulse für den Risikodialog (exemplarisch):

- Teilt die zweite Verteidigungslinie im Grundsatz die Risikosicht der Fachbereiche?
- Geht die Bank in der Ableitung der Kritikalität einheitlich und angemessen vor?
- Steht die Anzahl von Kontrollen im Verhältnis zur Prozesskritikalität?
- Liegen aus der laufenden Überwachung Erkenntnisse für die Risikozuordnung vor?
- Sind die Risikodefinitionen verständlich und weitgehend interpretationsfrei anwendbar?
- Welchen Einfluss haben interne Prüfungen auf die Kontrollstruktur im Status quo?

Die frühen Erkenntnisse führen von Beginn an zu zielgerichteten Maßnahmen, die zur Aufklärung von Missverständnissen in der Interpretation und Anwendung von Risikodefinitionen beitragen. Der Deep Dive in die Daten ermöglicht allen Organisationseinheiten den Blick in ihre Risikobewertung und Kontrollstruktur.



...essname	F2E-Strecke	Organisationseinheit	Risikoeinwertung	Zugeordnete Risiken	Kontrolle(n)
Beispiel 1	Kreditprozess	xyz	keine Risikorelevanz	keine	ja
Beispiel 2	Kreditprozess	xyz	keine Angabe	Compliance	ja
Beispiel 3	Kreditprozess	xyz	gering	Compliance, Rechtsrisiko, Reputationsrisiko	nein
Beispiel 4	Kreditprozess	abc	mittel	Compliance	nein
Beispiel 5	Kreditprozess	abc	hoch	Rechtsrisiko, Modellrisiko,	ja

Abbildung 4: Beispiel für die Visualisierung von Daten für den Risikodialog (exemplarisch)

d) Etablierung dialogorientierter Austauschformate im Three-Lines-of-Defense-Modell

Neben den regulären Gremien zur Steuerung der finanziellen und operativen Risiken der Bank hat die KfW IPEX-Bank weitere Gremien eingerichtet. Diese dienen gezielt der Förderung des übergreifenden Austauschs zu Erkenntnissen mit Relevanz für die Ausgestaltung der IKS-Governance und des IKS-Regelkreises. Im Dialog erfolgt der verbindliche Regelaustausch u. a. zu:

- regulatorischen Entwicklungen
- Anpassungen im Anweisungswesen mit Relevanz für das Interne Kontrollsystem
- Anpassungen in der organisatorischen Aufstellung und Wechsel in Zuständigkeiten
- Maßnahmen zur Stärkung der Risikokultur
- Erkenntnisse aus internen und/oder externen Prüfungen
- Folgeinformation aus Fachveranstaltungen (z. B. Verbände, Schulungen, Konferenzen)
- Vernetzung in der Risikosteuerung (ISMS, BKM, OpRisk und IKS-Management)

III. Kommunikation in Zahlen, Daten und Fakten

Nach 15 Monaten lässt sich festhalten, dass der Invest in Kommunikation auf Basis von Daten einen maßgeblichen Einfluss auf die konstruktive und effiziente Weiterentwicklung des Internen Kontrollsystems ausgeübt hat. Der intensive Risikodialog hat **von Anfang an eine gemeinsame Lernkurve und hohe Awareness** im Three-Lines-of-Defense-Modell ermöglicht – bei überschaubarem Aufwand! Die an das Kommunikationskonzept geknüpften Ziele wurden weitgehend erreicht.

Geschäftsführung	Commitment zum Vorgehen und Sprechfähigkeit für Rückfragen erzielen • Information zu Zielen, Rollen und Aufgaben der IKS-Relevanzanalyse • Hinweis zu Aufwänden zur Umsetzung und Hilfestellungen
Abteilungs- und Teamleiter	Commitment zum Vorgehen und Übernahme der Umsetzungsverantwortung • Information zu Zielen, Rollen und Aufgaben der IKS-Relevanzanalyse • Hinweis zu Aufwänden zur Umsetzung und Hilfestellungen • Beschreibung des Ablaufs und Erwartung an die fachliche Begleitung im Kontext der Verantwortung für das operative Risikomanagement
Prozess-verantwortliche	Awareness und Befähigung zur Durchführung der IKS-Relevanzanalyse • Information zu Zielen und Aufgaben der IKS-Relevanzanalyse • Exemplarischer Ablauf und Klärung offener Fragen • Erläuterung der Hilfestellungen und Supportleistung durch Teamleiter
IKS-Gremien (Arbeits- und Leitungsebene)	Kenntnis von Verlauf und Ergebnissen sowie Lessons Learned im Rollout • Information zur Abdeckung der Prozess- und Kontrollstruktur • Lieferung von Ansätzen zur Diskussion von Auffälligkeiten mit Impact auf die Weiterentwicklung eines integrierten IKS

Abbildung 5: Inhalte und Adressaten im IKS-Kommunikationsfahrplan

Die **iterative Konzeption und Entwicklung der IKS-Relevanzanalyse** erfolgte projekthaft im Rahmen von Workshops. Diese waren so konzipiert, dass sie i. d. R. keine Vorbereitung der Teilnehmer erforderten. Die Akzeptanz zur Teilnahme und Mitgestaltung wurde wahrnehmbar gesteigert, die Projektarbeit hat spürbar an Schnelligkeit gewonnen.

Zur **Einbindung aller Umsetzungsverantwortlichen** in der Pilotierung und im Rollout hat die zentrale IKS-Evidenzstelle u. a. folgende Kommunikationsmaßnahmen realisiert:

- authentische Berichterstattung über Erfolge und Misserfolge in der Pilotierung
- Durchführung von 15 Informationsveranstaltungen in den drei Monaten des Rollouts
- persönliche Begleitung der Fachbereiche in individuellen Fragestellungen der Umsetzung
- Abschlusskommunikation und Danksagung an alle Beteiligten nach Pilotierung und Rollout
- Information aller Beteiligten über ihren Beitrag im Jahresbericht an die Aufsichtsorgane
- Weiterentwicklung dialogorientierter Austauschformate der IKS-Gremien
- Regelinformation aller Stakeholder über Projektstatus und gemeinsame Identifikation von potenziellen Abhängigkeiten zu bankinternen Entwicklungen

Die **laufende Reflexion der Wirksamkeit aller Maßnahmen** und die Priorisierung der nächsten Handlungsfelder erfolgte in halbjährlichen Review-Terminen mit dem Projektauftraggeber. Hier wurden u. a. auch die Wirksamkeit der Maßnahmen zur Risiko-Awareness und zum Zusammenwachsen der drei Verteidigungslinien kritisch bewertet.

Weitere Elemente im Kommunikationsfahrplan:

- IKS-Pflichtschulung für alle Mitarbeitenden
- IKS-Informationsportal im Intranet zur Vermittlung des Basiswissens

IV. Lessons Learned aus einem Jahr IKS-Relevanzanalyse

Die IKS-Evidenzstelle hat von Anfang an wertvolle Impulse erhalten, welche Maßnahmen zur Weiterentwicklung und damit zur Steigerung des IKS-Reifegrads zu priorisieren sind. Nachfolgend ein Auszug der Lessons Learned und der daraus abgeleiteten Maßnahmen für die KfW IPEX-Bank:

1. Transparenz fördert das gemeinsame Risikoverständnis

Das Ziel des fachbereichsübergreifenden Risikodialogs auf Basis „echter“ Daten ging nach sechs Monaten auf. Mit Erfassung der Risiko- und Kontrollinformationen in *Adonis* und deren Auswertung können die Risikosichten der drei Verteidigungslinien gegenübergestellt und Abweichungen hinterfragt werden. Der Revision fällt es leichter, auf Basis maschinell abrufbarer Informationen am Prozess die Angemessenheit von Kontrollen in Anlehnung an einheitliche Standards zu überprüfen. Für Prozessverantwortliche werden Feststellungen nachvollziehbarer bzw. können abweichende Meinungen zur Risikobeurteilung objektiver erörtert werden.

Weiterzuentwickeln sind **einheitlich anzuwendende Parameter zur Beurteilung von Risiken und Kontrollerfordernissen**. Die an sich interpretationsfreien Risikodefinitionen sind noch nicht durchgängig präsent, die Beurteilung von prozessinhärenten Risiken erfolgt daher in Teilen noch zu subjektiv. Die KfW IPEX-Bank plant die Entwicklung einer Matrix, auf deren Grundlage die Beurteilung der Prozesskritikalität differenzierter erfolgt und die Allokation von Kontrollen nachvollziehbarer und effizienter wird. Die Fachverantwortung der ersten Verteidigungslinie muss methodisch besser unterstützt und in Folge z. B. auch gegenüber der Internen Revision stärker gelebt werden.

2. Der Mix aus zentraler und dezentraler SFO-Verantwortung lässt sich optimieren

In Teilen fehlt die **übergreifende Front-To-End-Sicht** zur Bestimmung des „Point-of-no-Return“ innerhalb einer Prozessstrecke – also dem Punkt, an dem sich ein prozessinhärentes Risiko bei fehlenden oder unzureichenden Kontrollvorgaben nicht mehr angemessen steuern lässt. Die Prozess- und Dokumentenverantwortung innerhalb eines Fachbereichs liegt bei unterschiedlichen Personen und ist sehr dezentral gestreut. Dadurch kann es zu Redundanzen in der Dokumentation von Kontrollabläufen kommen bzw. wird die

ausschließliche Abbildung prozessintegrierter Kontrollen im Rahmen der prozessorientierten schriftlich fixierten Ordnung nicht durchgängig eingehalten. Die Überwachung und Überprüfung des Internen Kontrollsystems ist damit nicht durchgängig effizient.

Der Handlungsbedarf besteht darin, Front-To-End-Managern einen aktiveren Part in der Beurteilung der Risiko- und Kontrollstruktur zu geben. Perspektivisch ist die heterogene Struktur der Prozess- und Dokumentenverantwortlichen zu analysieren und ggf. themenbezogen zu optimieren. Dabei sind die im Geschäftsmodell begründeten Spezifika der Prozess- und Kontrollgestaltung angemessen zu berücksichtigen.

3. Verbindlichkeit in der Information unterstützt die Awareness in der Breite

Um die Risiko-Awareness unabhängig von Berufserfahrung und Zugehörigkeit zu fördern, wurde die **IKS-Schulung zur Pflichtschulung** erklärt. Dadurch wird die Bedeutung eines wirksamen Internen Kontrollsystems in die Breite getragen. Das Verständnis für Steuerungs- und Überwachungsmaßnahmen wächst mit dem Verständnis für die dahinterstehenden Risiken. Es wird bewusst, dass es eines Internen Kontrollsystems nicht nur aus regulatorischen Anforderungen heraus bedarf. Jeder kann und soll sich mit dem Thema Internes Kontrollsystem daher vertraut machen.

Ergänzend muss die **Hilfe zur Selbsthilfe in der Informationsbeschaffung** und das Know-how im fachlichen Prozess- und Kontrolldesign weiter ausgebaut werden. In Planung sind u. a. Informationsreihen, die grundlegende Kenntnisse sowie Tipps und Tricks in der Gestaltung von Prozessen aus der Front-To-End-Perspektive pragmatisch vermitteln.

4. Je differenzierter die Sicht auf die Risiken, desto besser deren Überwachung

Auch wenn es geholfen hat, zu Beginn das Compliance-Risiko als eine übergeordnete Risikoart zu betrachten: mit Auswertung der Daten hat sich gezeigt, dass dieses Risiko aus Sicht der ersten Verteidigungslinie naturgemäß in nahezu 50 % der Prozesse verortet wird. Zur effektiven Steuerung auf Basis der Echtdaten fehlt bei diesem Ansatz der zweiten Verteidigungslinie der differenziertere Blick auf den fachlichen Risikohintergrund (Wertpapier-Compliance, Datenschutz, Geldwäsche, regulatorische Compliance u. a.). Im Gegenzug hat sich der „Mut zur Lücke“ – also der Fokus auf die 10 wesentlichsten OpRisk-Ursachen in der Prozessbewertung – als richtig erwiesen und kann beibehalten werden.

Auf Basis der initialen Risikozuordnung Anfang 2021 wird das Compliance-Risiko in 2022 im Rahmen der Prozessprolongationen neu hinterfragt und konkreter ausgelegt. Dabei stehen bei Unsicherheiten in der **Auslegung der Risikodefinitionen** die Risikovertreter der zweiten Verteidigungslinie als Ansprechpartner zur Verfügung und die Datenbestände werden „ongoing“ sukzessive optimiert.

5. Persönliche Begleitung zur schnellen Steigerung des IKS-Reifegrads beibehalten

Ein Jahr nach dem ersten Durchlauf der „IKS-Relevanzanalyse“ werden die regulären Termine zur Prozessprolongation genutzt, um einen zweiten Blick auf die initiale Risikoeinwertung und Kontrollbeschreibung zu werfen. Dabei zeigt sich, dass viele Prozessverantwortliche sich ihrer Rolle als Manager der prozessinhärenten Risiken deutlich bewusster sind. Dennoch fällt es nicht immer leicht, Kontrollvorgaben im eindeutigen Bezug zum Risiko prüfungssicher zu definieren. Analog zum Rollout werden Prozessprolongationen daher mit monatlichen Informationsreihen begleitet, um die Bedeutung einer prüfungssicheren schriftlich fixierten Ordnung zu verdeutlichen. Es werden methodische Hilfestellungen gegeben und die Risikovertreter der zweiten Verteidigungslinie unterstützen in der Interpretation von Risiken auf Prozessebene.

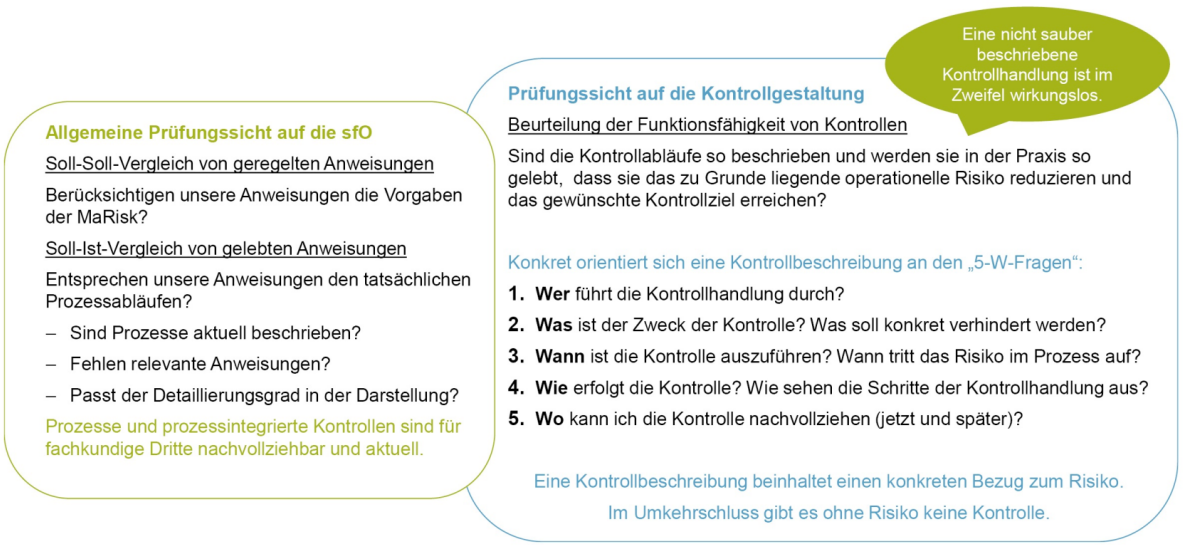


Abbildung 6: Prüfungssicheres Kontrolldesign

6. Risikoanalysen der zweiten Verteidigungslinie sind besser zu verzahnen

In die Analysen zur Steuerung operationeller Risiken wie z. B. aus der Business-Impact-Analyse oder übergreifender OpRisk-Assessments werden z. T. andere Ansprechpartner eingebunden. Die Analysen finden aktuell noch zeitlich unabhängig von der IKS-Relevanzanalyse statt. Es fehlt der aufeinander abgestimmte Austausch zwischen der zweiten Verteidigungslinie und den Prozessverantwortlichen über potenziell IKS-relevante Erkenntnisse. Aus Sicht der Prozessverantwortlichen unkritische Prozesse können so abweichend zu Ergebnissen aus anderen Risikoanalysen im Widerspruch stehen.

Ein wesentliches Handlungsfeld stellt damit die Aufnahme der Prozesse und Methoden sowie der Informationsflüsse aus den verschiedenen Analysen zur Steuerung operationeller Risiken dar. Ziel muss das gemeinsame Wissen und die Nutzung risikorelevanter Daten sein, um ein wirksames und effizientes Kontrollsystem gestalten und steuern zu können.

V. Der datenbasierte Risikodialog als Wegbereiter für die Zukunft

Der IKS-Regelkreis als mindestens einmal im Jahr zu durchlaufender Prozess wird als **iterativer Steuerungsprozess** definiert. Im Zuge der immer engeren Verzahnung auf Basis des laufenden Risikodialogs wurde er um unterjährige Auslöser ergänzt und wird jetzt als „lebender“ und damit als kontinuierlicher Verbesserungsprozess verstanden. Er ist mit eigenen Kontrollvorgaben für alle Beteiligten nachvollziehbar in *Adonis* abgebildet. Der in der schriftlich fixierten Ordnung verankerte Prozess zeigt allen Verteidigungslinien und IKS-relevanten Gremien transparent auf, an welcher Stelle sie im IKS-Regelkreis eingebunden sind und an welcher Stelle sie einen aktiven Part in der Weiterentwicklung des Internen Kontrollsystems übernehmen.

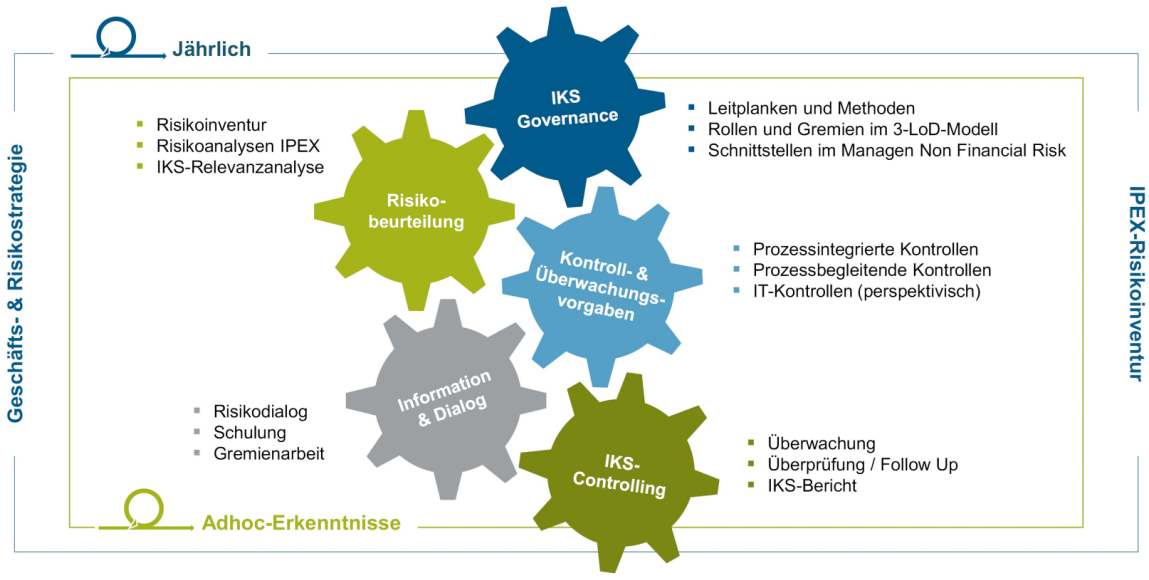


Abbildung 7: Der IKS-Regelkreis als kontinuierlicher Verbesserungsprozess

Mit der Einführung der IKS-Relevanzanalyse wurde der IKS-Regelkreis im Jahr 2021 erstmals vollständig durchlaufen. Die Bewertung der prozessinhärenten Risiken aus der Sicht der ersten Verteidigungslinie konnte direkt im IKS-Jahresbericht berücksichtigt werden. Für das Jahr 2022 steht im Fokus, die initial erhobenen **Risiko- und Kontrollinformationen zu validieren und zu konkretisieren**. Bis Ende 2022 werden weitgehend alle Kontrollen prüfungssicher – und damit für fachkundige Dritte nachvollziehbar – im Rahmen der

Prozessprolongationen beschrieben sein. Das Ziel: jedes Prozessrisiko steht im eindeutigen Zusammenhang zur Kontrollbeschreibung und damit zum Kontrollziel und -zweck. Im Umkehrschluss gibt es keine Kontrollen, denen kein eindeutiges Risiko zu Grunde liegt.

Erwartungsgemäß sind noch keine **Effizienzgewinne durch signifikante Straffungen in der Kontrollstruktur** zu quantifizieren. Daher liegt ein weiterer Schwerpunkt auf der Schärfung der Parameter zur Ableitung von IKS-relevanten Kontrollen auf Basis von risikospezifischen und regulatorischen Erfordernissen.

Das **Risiko-Kontroll-Inventar** ist historisch gewachsen und wird aktuell noch händisch gepflegt. Auf Basis der erhobenen und dokumentierten Daten konnten bereits Struktur und Aufbau für eine maschinelle Befüllung des Inventars mit Risiko- und Kontrollinformationen definiert werden. In Prüfung ist die integrierte Abbildung der Prüfungsfelder und -erkenntnisse der Internen Revision.

Ein weiteres Handlungsfeld stellt die bessere Transparenz über Risiken und Kontrollen in ausgelagerten Prozessen sowie in den Prozessen der im Jahr 2021 neu gegründeten Tochter KfW IPEX-Asia dar. Hier kann an die Erfahrungen aus dem Rollout der IKS-Relevanzanalyse angeknüpft werden.

Die unabhängige Überprüfung der Angemessenheit und Wirksamkeit liegt aktuell in der Verantwortung der Internen Revision. Auch hier kann auf Basis transparenter Risiko- und Kontrollinformationen ein angemessener Weg definiert werden, um die erste und/oder zweite Verteidigungslinie im Sinne eines unabhängigen **Kontrolltesting** ergänzend zur laufenden Überwachung einzubinden.

VI. Das Fazit nach 1,5 Jahren datenbasiertem Risikodialog

Im Austausch untereinander und mit anderen Banken zeigt sich, es gibt nicht den einen Weg zum Ziel, um ein zum Geschäftsmodell und zur Organisation passendes, risikoadäquates Internes Kontrollsystem auf Basis transparenter und valider Risiko- und Kontrollinformationen zu entwickeln.

Und auch wenn Papier geduldig ist, die Mitarbeiter sind es i. d. R. nicht. So haben insbesondere Prozessverantwortliche i. d. R. andere Herausforderungen, als „praxisfremde“ Risikosteuerungssysteme zu implementieren. Jede Fehlentwicklung bindet unnötige Ressourcen, jede zentrale Maßnahme wird zu Recht kritisch hinterfragt.

Die KfW IPEX-Bank hat sich daher bewusst für einen iterativen, lernenden Ansatz und mit der IKS-Relevanzanalyse eine für ihre Organisation und ihr Geschäftsmodell passende Methode entschieden. Damit konnte die eine oder andere Komplexitätsfalle vermieden werden.

Der Erfolg zeigt sich u. a. in der aktiven Rückkopplung zwischen der IKS-Evidenzstelle und allen Umsetzungsverantwortlichen sowie im Tempo, mit dem aus der Bewertung von über 400 Prozessen wertvolle Impulse zur IKS-Weiterentwicklung direkt in die Prüfung und Umsetzung gehen bzw. für eine spätere Realisierung geplant werden.

Nur im Dialog wird das Thema Internes Kontrollsystem erfolgreich aus der Theorie-Nische auf die Praxisebene gehoben. Die Bereitschaft, sich mit Risiken aus einer Risikomanagementperspektive bewusster auseinanderzusetzen, wächst bankweit. Und so erklärt sich auch das Feedback z. B. aus dem Markt: „Mit meiner langjährigen Erfahrung macht es keinen Spaß, jetzt so detailliert auf Prozess- und Kontrollbeschreibungen zu achten – aber es macht Sinn!“

Bekommt die KfW IPEX-Bank schon Bestnoten für ihr Internes Kontrollsystem? Noch nicht. Aber alle drei Verteidigungslinien kommen jeden Tag ins Gespräch über Risiken und Risikosteuerung. Es ist erlebbar, dass Risikokultur und Awareness existieren und das Thema Internes Kontrollsystem über die regulatorische Notwendigkeit hinaus als sinnhafter Beitrag für ein stabiles Geschäftsergebnis angesehen wird.

Ist die KfW IPEX-Bank schon am Ziel? Eindeutig Nein. Aber sie ist als Organisation gemeinsam auf einem guten und planbaren Weg. Mit einem Umsetzungszeitraum von ca. drei Jahren konnte bereits im zweiten Jahr der IKS-Reifegrad stark verbessert werden. Und

alle Beteiligten bringen Verständnis und Lösungsvorschläge mit, wenn es an der einen oder anderen Stelle noch hakt.

PRAXISTIPPS

- Keine Lösung von der Stange nehmen, sondern die institutsspezifischen Anforderungen verstehen und in eine risikoadäquate IKS-Governance und einen effizienten IKS-Regelkreis übersetzen.
- Iterativ vorgehen, um als Organisation schnell zu lernen und Komplexitätsfallen zu vermeiden.
- Für die Beurteilung von Risiken und Beschreibung von Kontrollvorgaben verbindliche Formate definieren, kommunizieren und methodisch begleiten.
- Über die Dokumentation und Visualisierung von Risiko- und Kontrollinformationen frühzeitig auf Basis „echter“ Daten aus der Praxis mit allen Hierarchieebenen ins Gespräch kommen.
- Den aktiven Dialog innerhalb des Three-Lines-of-Defense-Modells koordinieren und fördern.

Beitragsnummer: 20624