

Friederike Krüsemann
Henning Heuter

RISIKOKULTUR IN FINANZINSTITUTEN

WIE IM GESAMTEN INSTITUT RISIKOORIENTIERTES HANDELN GESTÄRKT WERDEN KANN

EINLEITUNG

In Finanzinstituten werden finanzielle Risiken wie Kredit- und Marktrisiken mittels mathematisch-statistischer Modelle kalkuliert, historische Daten liefern eine solide Analysebasis. Doch hat es sich gezeigt, dass große Risiken auch in einer anderen Risikoart lauern: In den Nicht-finanziellen Risiken. Ob IT-Ausfälle, Cyber-Angriffe, Compliance-Verstöße oder schlicht menschliches Versagen. Operationelle Risiken oder Reputationsrisiken können existenzgefährdende Ausmaße annehmen und erfordern eine strategische Herangehensweise, um die Resilienz und das Überleben eines Finanzinstituts zu sichern.

Mit diesem Fachbeitrag starten wir eine fünfteilige Fokus-Reihe, die nicht-finanzielle Risiken aus verschiedenen Blickwinkeln beleuchtet:

- 1. Risk Culture in Finanzinstituten**
Der menschliche Faktor: Warum perfekte Strukturen nicht nützen, wenn die Risikokultur diese nicht trägt.
- 2. Qualität vor Quantität im IKS – risikoorientierte Ausgestaltung des internen Kontrollsystems**
Kontrollen sind wichtig, aber in welchem Ausmaß? Und wie findet man ein System, welches die perfekte Balance für das eigene Institut aufzeigt?
- 3. Reifegradmodelle im IKS – Ausführliches Fallbeispiel**
Lösungsansatzes für die Herausforderungen aus Fachbeitrag 2
- 4. Reputationsrisiko in Finanzinstituten – Chancen, Herausforderungen, Bewertung**
Die schwer zu greifenden Folgen und Auslöser für Vertrauensverluste und wie man ein Institut davor schützt.
- 5. Verzahnung OpRisk und IKT-Risikosteuerung**
Vom silodenken zur integrierten risikosteuerung

WAS BEDEUTET RISIKOKULTUR?

Den Auftakt macht der menschlichste Faktor: die Risikokultur. Richtlinien, Strukturen und Methoden existieren auf dem Papier, strategisch vorgegeben und vorgelebt werden sie vom Vorstand, gelebt werden sie von den Mitarbeitern. Die Praxis zeigt: Ausgefeilte mathematische Risikomodell und lückenlose Governance-Strukturen versagen, wenn sie nicht von einer gelebten Risikokultur getragen werden. Dieser Fachbeitrag beschäftigt sich damit, wie die Risikokultur in Finanzinstituten als effektives Fundament für das Risikomanagement zu stärken.

REGULATORIK

Die Unternehmenskultur kann als Persönlichkeit eines Unternehmens gesehen werden und basiert auf einem gemeinsamen Wertesystem. Die Risikokultur als Teil davon ist die Gesamtheit der Normen, Einstellungen und Verhaltensweisen der Mitarbeiter im Umgang mit Risiken. Ein Institut kann Risiken nur dann effektiv steuern, wenn die Identifikation und der offene Umgang mit Risiken tief mit dem kollektiven Bewusstsein verwachsen sind – über alle Bereiche hinweg.

Die Risikokultur in Finanzinstituten ist in der Regulatorik verankert. Im Folgenden wird ein kurzer Überblick über die wichtigsten Anforderungen gegeben.

EBA/GL/2021/05 Abschnitt 9 – Leitlinien zur internen Governance

Die EBA betont, dass die Risikokultur die Entscheidungen der Geschäftsleitung beeinflusst und somit Auswirkung auf die eingegangenen Risiken hat. Sie verlangt das Vorliegen einer Risikokultur, die auf das Risikobewusstsein und -verhalten des Instituts ausgerichtet ist und von allen Mitarbeitern – nicht nur von Risikospezialisten – als Schlüsselement gesehen wird. Folgende Elemente soll die Risikokultur umfassen:

- **Leitungskultur (Tone from the top):** Das Leitungsorgan sollte den institutsweiten Standard setzen. Es kommuniziert die Werte und Erwartungen und fordert die Mitarbeiter auf, diese einzuhalten und zu leben.
- **Verantwortlichkeiten:** Jeder Mitarbeiter muss in der Lage sein, seine Aufgaben wahrzunehmen und die Tragweite von Entscheidungen aus Risikosicht nachvollziehen können.
- **Wirksame Kommunikation und kritischer Dialog:** Vor allem in Entscheidungsprozessen sollen verschiedenste Sichtweisen unterstützt werden, grundsätzlich soll ein offenes und konstruktives Umfeld gefördert werden.
- **Anreize:** Es dürfen keine Fehlanreize, die das Eingehen unverhältnismäßig hoher Risiken fördert, gesetzt werden.

MaRisk AT 3 – Gesamtverantwortung der Geschäftsleitung

Die Anforderungen an die Risikokultur in den MaRisk sind hauptsächlich im Modul AT 3 definiert. Die Identifikation und der bewusste Umgang mit Risiken sollen durch die Art und Weise der Tätigkeitsausübung aller Mitarbeiter gefördert werden. Zusätzlich soll sichergestellt werden, dass Entscheidungsprozesse zu aus Risikosicht ausgewogenen Ergebnissen führen. Dies soll erreicht werden durch:

- klare Bekenntnis der Geschäftsleitung zu risikoangemessenem Verhalten
- strikte Beachtung des durch die Geschäftsleitung festgelegten Risikoappetits
- Rechenschaftspflicht der Mitarbeiter für persönliches Risikoverhalten
- Ermöglichung und Förderung des transparenten und offenen institutsinternen Dialogs
- Einrichten von Überwachungsverfahren zur Einhaltung der Risikokultur

EBA/GL/2022/03 – Leitlinien zu gemeinsamen Verfahren und Methoden für den aufsichtlichen Überprüfungs- und Bewertungsprozess (Supervisory Review and Evaluation Process, SREP) sowie für die aufsichtlichen Stresstests

Es soll beurteilt werden, ob die Finanzinstitute über eine ihrem Geschäftsmodell und der Risikobereitschaft angemessene Risikokultur verfügen. Als Bewertungskriterien sollen folgende Elemente herangezogen werden:

- Liegt eine ausreichende Kenntnis der eigenen Struktur vor?
- Sind die eingerichteten Strukturen transparent und angemessen komplex? Können die Strukturen für kriminelle Aktivitäten missbraucht werden?
- Basiert die Risikokultur auf einer ganzheitlichen Risikobeurteilung und dem definierten Risikoappetit?
- Wird ein Umfeld konstruktiver Kritik gefördert?
- Gibt es die Möglichkeit, Missstände anonym zu berichten?
- Gibt es angemessene Regelungen zu Interessenkonflikten?
- Besteht Chancengleichheit zwischen den Geschlechtern und wird Diskriminierung vorgebeugt?
- Wird die Risikokultur über alle Institutsebenen hinweg gelebt?
- Beinhaltet der Verhaltenskodex Grundsätze/Beispiele für (nicht) akzeptables Verhalten?

RISIKO- GOVERNANCE

Kultur, Schnittstelle, Governance: Vom Silo-Denken zur integrierten Steuerung

In vielen Instituten herrscht traditionell ein ausgeprägtes Silo-Denken. Das Risikomanagement (2nd Line of Defense) wird als regulatorische Kontrollinstanz wahrgenommen, während sich der Vertrieb (1st Line of Defense) primär auf Ertragsziele fokussiert. Diese organisatorische und vor allem kulturelle Trennung birgt erhebliche operationelle und strategische Risiken.

Dementsprechend muss es das Ziel sein, eine integrierte Steuerung zu entwickeln.

- **Risiko als gemeinsame Verantwortung:** Eine moderne Governance bricht diese gedanklichen Trennungen auf. Risikoorientierung darf nicht an der Schnittstelle zum Markt enden; sie muss integraler Bestandteil jeder geschäftspolitischen Entscheidung sein.
- **Das Three Lines of Defense-Modell als Partnerschaft:** Die 2nd Line of Defense agiert nicht mehr rein kontrollierend, sondern als strategischer Sparringspartner für das Business. Das gemeinsame Ziel ist die Optimierung des Risiko-Rendite-Profiles, nicht das Verhindern von Geschäft.

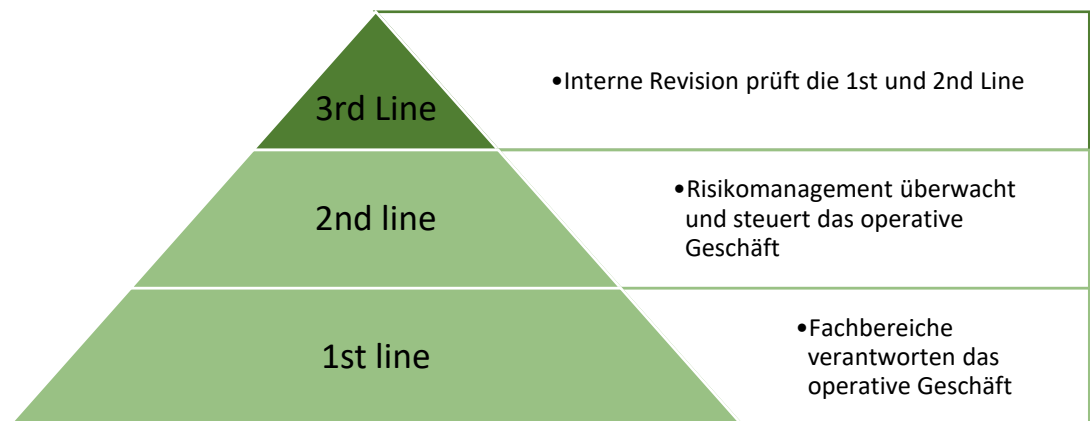


Abbildung 1: Three Lines of Defense (TLod)

RISIKOKULTUR IN DER PRAXIS

Die Ausprägung einer Risikokultur zeigt sich am ehesten im Arbeitsalltag einzelner Mitarbeiter. Erfahrungsgemäß ist die Risikokultur in der Governance fest verankert, das sagt allerdings wenig

darüber aus, ob die Werte tatsächlich so gelebt werden. Die Beispiele der Schadensmeldungen und der risikostrategischen Vorgaben zeigen exemplarisch, welche Stolpersteine im Alltag lauern können.

Das Melden von Schäden und Beinahe-Schäden

Die Erfassung von tatsächlichen OpRisk-Schäden ist regulatorische Pflicht. Das (zusätzliche) systematische Erfassen von Beinahe-Schäden ist für ein präventives Risikomanagement ebenso von großer Bedeutung. Wenn ein Systemausfall oder ein Prozessfehler im letzten Moment ohne finanziellen Schaden abgefangen wurde, ist dies natürlich ein Grund zur Erleichterung, aber ebenso ein wertvoller Frühwarn-indikator.

Damit es möglich ist, aus (Beinahe-)Schäden zu lernen, ist eine Meldung unerlässlich, doch genau daran hapert es oft. Zunächst muss erst einmal erkannt werden, dass es sich um einen (Beinahe-)Schaden handelt. Bei tatsächlichen Schäden lässt sich diese Hürde noch recht einfach umgehen, indem bspw. eine Meldung Voraussetzung für die Buchung ist. Bei Beinahe-Schäden ist dies wesentlich komplizierter, da nichts Konkretes passiert ist, was weiterer Handlungen bedarf. Dennoch ist es wichtig, den Mitarbeitern Strategien zum Erkennen von Beinahe-Schäden an die Hand zu geben. Folgendes kann auf einen Beinahe-Schaden hinweisen:

- Ein Eingreifen beim Vier-Augen-Prinzip wird nötig.
- Die IT-Abteilung blockiert schwerwiegende Phishing-Mails.
- Ein Bearbeitungsfehler fällt zufällig auf, bspw. durch Ungereimtheiten oder Kundennachfragen.
- Ein System verleitet durch das Design dazu, oftmals falsch zu klicken oder die Felder falsch auszufüllen.
- Ein System stürzt öfter ab und die Daten wurden nur zufällig vorher gespeichert.

Das Wichtigste ist es, die Mitarbeiter einzubinden und auf ihre Kooperation zu setzen. Sollte ein Beinahe-Schaden gemeldet werden, muss dieser Hinweis ernst genommen und Handlungen, die auch bei tatsächlichen Schäden Anwendung finden, folgen. So wird den Mitarbeitern gezeigt, dass ihre Zusammenarbeit mit dem Risikomanagement geschätzt wird und tatsächlich Wirkung entfaltet. Dies stärkt die Risikokultur im Unternehmen und sorgt für eine lebendige Umsetzung im Arbeitsalltag.

Das Einhalten risikostrategischer Vorgaben

In Finanzinstituten sollte im Rahmen der Risikokultur und des Risikoappetits festgelegt werden, welche Branchen oder Kunden von Geschäften ausgeschlossen werden (bspw. Tabakbranche oder lokale Kunden, mit denen Geschäfte bereits einmal nicht erfolgreich waren). Da besonders im Vertrieb mit Zielen im Zusammenhang mit variablen Vergütungen gearbeitet wird, ist es notwendig, die Mitarbeiter ausreichend zu sensibilisieren, dass die Einhaltung der Vorgaben über dem Erreichen der persönlichen Ziele steht.

Um das gewährleisten zu können, müssen die Mitarbeiter einerseits die risikostrategischen Vorgaben kennen und verinnerlichen, andererseits müssen die Anreize so gesetzt werden, dass sie nicht im Widerspruch zur Risikokultur stehen. Ein offenes Umfeld, in dem transparent über potenzielle Abschlüsse oder Nicht-Erreichen von Zielen gesprochen werden kann, ist essenziell.

PERSPEKTIV- WECHSEL

Aufgrund der hohen Arbeitsbelastung, stetig steigenden Ansprüchen und wenig bis keinen sichtbaren direkten Einfluss auf die Tätigkeiten ist es nicht verwunderlich, wenn die Risikokultur im Arbeitsalltag nicht immer mitgedacht wird. Dennoch sollte sich ein Institut bemühen, diesem Phänomen entgegenzuarbeiten. Zu diesem Zweck werden im Folgenden Maßnahmen vorgestellt, die einen Perspektivwechsel bei den Mitarbeitern begünstigen.

Awareness-Maßnahmen und psychologische Sicherheit

Damit Mitarbeiter Fehler und (Beinahe-)Schäden überhaupt transparent machen, braucht es eine sichere Umgebung. Wenn das Melden eines Fehlers mit Sanktionen oder Reputationsverlust im Team verbunden ist, werden Risiken vertuscht oder auf andere geschoben, bis sie systemkritisch werden oder anderweitig auffallen. Im Institut muss demnach ein Umdenken zu einer positiven Fehlerkultur stattfinden: Das Melden eines Fehlers oder (Beinahe-)Schadens ist keine Schwäche, sondern trägt aktiv zum Schutz des Instituts bei.

Risikokultur direkt im Onboarding verankern

Der erste Eindruck zählt und beeinflusst die Arbeitsweise. Neue Mitarbeiter sollten das Risikomanagement nicht erst Monate nach Eintritt durch verpflichtende Schulungen, die oft nur als Formalie wahrgenommen werden, kennenlernen. Risikobewusstes Handeln gehört ab Tag eins in das Onboarding-Programm, da es eine unerlässliche Pflicht in Finanzinstituten ist. Hierbei geht es nicht um Gesetze, sondern um das Vermitteln der gelebten Werte: "Wir sind ein risikobewusstes Institut, und du bist Teil davon."

Das Intranet als lebendige Kommunikationsplattform nutzen

Risikomanagement muss greifbarer und spannender für Mitarbeiter werden. Dazu bietet sich das Intranet als interne Aufklärungschance mit vielen kreativen Möglichkeiten an. Die Nutzung von modernem Storytelling spricht viele Menschen an und kann bspw. für anonymisierte Fallstudien, interessante Grafiken zu aktuellen Bedrohungslagen oder kurze Videos im Reel-Style genutzt werden.

Fallstudien können entweder interne Schäden aufgreifen, erläutern, einordnen und mögliche Konsequenzen aufzeigen oder auf externe Fälle eingehen.

Konsequent in den Dialog mit allen Mitarbeitern treten

Kultur entsteht nicht durch Rundmails des Vorstands, sondern durch Gespräche mit den einzelnen Mitarbeitern. Risikomanager müssen einen Teil ihrer Arbeit konsequent weg von ihren Schreibtischen in den Fachabteilungen erledigen. Regelmäßige Fragerunden, Vorstellungen neuer Tätigkeiten oder generelle Aufklärung über Risikothemen lassen das gesamte Risikomanagement greifbarer wirken und bauen Barrieren ab. Tendenziell wenden sich Mitarbeiter bei Fragen oder kritischen Fällen eher an die Risikomanager, wenn sie diese gut kennen.

Das Anforderungsprofil im Risikomanagement anpassen

Historisch wurden Risikocontrollingabteilungen oft mit ausgeprägten Analytikern und zahlenfokussierten Strategen besetzt. Für eine starke Risk Culture reicht das nicht mehr aus. HR und Führungskräfte müssen bei der Rekrutierung für Risiko-Rollen gezielt auf Mitarbeiter setzen, die Menschenkenntnis vorweisen und Lust haben, viel zu kommunizieren. Gefragt sind eine hohe Sozialkompetenz, Kenntnisse in Mediation und im Beziehungsaufbau. Komplexe Risikosachverhalte müssen empathisch und verständlich vermittelt werden. Ein Risikomanager mit diesem Profil baut Barrieren ab und fördert die intrinsische Kooperationsbereitschaft der Fachbereiche.

RISIKOKULTUR ALS WETTBEW- ERBSVORTEIL

UNTERSTÜTZUNG DURCH 1 PLUS i

AUTOREN

Starke Risikokultur				
Hohe interne Awareness	Integration im Onboarding	Einbindung des Intranets	Kontinuierlicher Dialog	Kommunikative Kompetenz im Risikomanagement

Eine gelebte Risikokultur ist kein regulatorisches Nice-to-have, sondern das verpflichtende Sicherheitsnetz eines Finanzinstituts. Wenn es gelingt, das Silo-Denken zu überwinden, das Melden von (Beinahe-)Schäden positiv zu besetzen und das Risikomanagement durch kommunikationsstarke Mitarbeiter nahbar zu machen, wandelt sich das Risikobewusstsein von einer lästigen Pflicht zur gelebten Realität. Institute, die diesen Perspektivwechsel meistern, sind nicht nur resilienter gegenüber Krisen, sondern auch agiler und erfolgreicher am Markt.

Das zielführende Managen der (Beinahe-)Schäden sowie das Fokussieren auf Regelkonformität steigert die Institutsqualität, Kundenorientierung und setzt Kapazitäten für Optimierungen frei. Institute, die nicht ständig kleine Feuer löschen müssen, können ihren Fokus voll auf das Kerngeschäft richten. So wird nicht nur die Kunden-, sondern auch die Mitarbeiterzufriedenheit verbessert, was sich direkt in einer höheren Arbeitsleistung niederschlägt.

Ein wesentliches Ergebnis einer starken Risikokultur ist die Minimierung von Reputationsrisiken, welche schwerwiegende Folgen haben können. Das Kundenvertrauen ist die wichtigste Währung für ein Finanzinstitut. Durch die Stärkung der Risikokultur kann zeitgleich das Kundenvertrauen gestärkt werden, was zu einem nachhaltigen Anstieg des Wettbewerbsvorteils führt.

Sie möchten noch mehr im Zusammenhang mit der Risikokultur 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 Definition und Stärkung der internen Risikokultur. Wir erarbeiten u.a. Quick-Check-Lösungen für den Status quo, welche wir Ihnen in Form von Inhouse-Kundenworkshops sehr gern vorstellen. Sprechen Sie uns doch einfach an!

Ihr 1 PLUS i Team



HENNING HEUTER
henning.heuter@1plusi.de



FRIEDERIKE KRÜSEMANN
friederike.krusemann@1plusi.de