


ORM und IKS systematisch integrieren

 **Die Schweizerische Gesetzgebung erklärt Internes Kontrollsystem sowie Risikomanagement für verbindlich. Bei der Integration dieser bisher oft unabhängig betriebenen Disziplinen können – systematisch umgesetzt – zahlreiche Synergien gewonnen werden.**

Mit der Verankerung von Internem Kontrollsystem (IKS) sowie Risikomanagement in der schweizerischen Gesetzgebung (Obligationenrecht ab Mitte 2007 und Versicherungsaufsichtsgesetz seit 1.1.2006) werden zwei wichtige Corporate-Governance-Komponenten als verbindlich erklärt. Damit reagiert auch die Schweiz auf das neue Umfeld für Versicherer: Die Finanzskandale und die Börsenbaisse vor wenigen Jahren haben weltweit Ratingagenturen, Gesetzgeber und Regulatoren auf den Plan gerufen. Das Bedürfnis der Stakeholder nach Internen Kontrollsystemen und nach Risikomanagement hat international stark zugenommen. Beispiele solcher Entwicklungen sind (nicht abschliessend):

- Neue Anforderungen an Interne Kontrollsysteme (z.B. Sarbanes-Oxley Act, SOX, in den USA, Loi sur la sécurité financière in Frankreich, 4., 7. und 8. EU-Richtlinie sowie Obligationenrecht/Versicherungsaufsichtsgesetz in der Schweiz)
- Neue Solvenzanforderungen (Swiss Solvency Test in der Schweiz und Solvency II in der EU)
- Enterprise Risk Management (Standard & Poors)

ORM und IKS: früher unabhängig...

Risikomanagement-Konzepte, insbesondere Operationelles Risikomanagement (ORM)



Marcel Stalder
Certified Public Accountant
Partner
Industry Leader Insurance
Audit Services
marcel.stalder@ch.ey.com



Stephanie Furger
lic. oec. HSG
Senior Manager
Advisory Services
stephanie.furger@ch.ey.com

und Internes Kontrollsystem, wurden, wo implementiert, lange Zeit als unabhängige Disziplinen behandelt:

- ORM hat sich aus dem Risikomanagement heraus entwickelt, für das oft der Chief Risk Officer verantwortlich ist und das in vielen Gesellschaften von einem Risk Management Committee überwacht wird.
- IKS hat sich als Teil der Unternehmensführung und -überwachung aus Managementkonzepten heraus entwickelt – mit verschiedenen Verantwortlichkeiten: Der Bereich Financial Reporting untersteht dem Chief Financial Officer und wird vom Audit Committee überwacht, der Bereich Operations untersteht dem Chief Operations Officer und der

Bereich Compliance dem Chief Compliance Officer. Im Zuge der Finanzskandale hat der Gesetzgeber in vielen Ländern nur den IKS-Bereich Financial Reporting als verbindlich erklärt (z.B. SOX in den USA und entsprechende Neuregelung der Revision im OR in der Schweiz).

Risikomanagement-Konzepte, insbesondere Operationelles Risikomanagement (ORM) und Internes Kontrollsystem (IKS), wurden lange Zeit als unabhängige Disziplinen behandelt.

Dadurch haben viele Firmen IKS als Ganzes in die Verantwortung des CFO und somit des Audit Committee gestellt.

Die parallele Entwicklung dieser zwei sich ergänzenden Disziplinen hat zu Redundan-

zen geführt. Trotz unterschiedlicher Herkunft und Verantwortlichkeit haben ORM und IKS zahlreiche Überschneidungen. Denn beide Disziplinen basieren auf der Prozessstruktur des Unternehmens und unterstützen das Management bei der Unternehmenssteuerung. Zahlreiche Unternehmen sehen sich deshalb mit folgenden Problemen konfrontiert:

- Manager klagen über die zunehmende Dokumentationspflicht. Nicht selten müssen sie gleich mehrmals pro Jahr mit verschiedenen Ansprechpartnern (z.B. IKS, ORM, Qualitätsmanagement) ihre Prozesse, Risiken und Kontrollen dokumentieren.
- In vielen Unternehmen hat sich eine Kontrollkultur entwickelt, die nicht mehr mit risikobasiertem Management vereinbar ist.
- Häufig werden extensive Ausgaben für Kontrollverbesserungen ohne Kosten-/Nutzen-Erwägungen in Betracht gezogen.

... sollen heute harmonisiert werden

Durch diese Herausforderungen, kombiniert mit einem stetig zunehmenden Kosten- und Performance-Druck, wird effizientes Risikomanagement zunehmend zum Wettbewerbsfaktor. Die neusten Entwicklungen zielen deshalb auf die Integration und Harmonisierung von IKS, ORM und weiteren Initiativen, wie beispielsweise dem Qualitätsmanagement (EFQM, ISO etc.), ab.

Dabei soll auf bestehenden Praktiken aufgebaut werden und gleichzeitig operationelle Effizienz, Wirksamkeit und Konsistenz unterstützt werden. Wichtige Zielsetzungen dieser Harmonisierung und Integration sind:

- Keine grossen Überschneidungen oder

Lücken der verschiedenen Kontroll- und Risikomanagement-Funktionen: Alle wesentlichen Risiken, Kontrollen und Aufgaben müssen einheitlich identifiziert und adressiert sein.

- Verteilung der Aufgaben auf die am besten geeigneten Personen und Abteilungen: Alle identifizierten Risiken müssen je einem «Risk Taker», «Risk Controller» und einem «Risk Owner» zugewiesen und durch entsprechende Aufgaben gehandhabt werden.
- Verankerung des Systems im Business, denn Risikomanagement kann diese Verantwortung nicht allein übernehmen («Risk Taker»-Funktion).
- Flexibilität des Systems, um neu auftauchende Risiken, organisatorische Verän-

derungen oder lokale Bedürfnisse einbinden zu können.

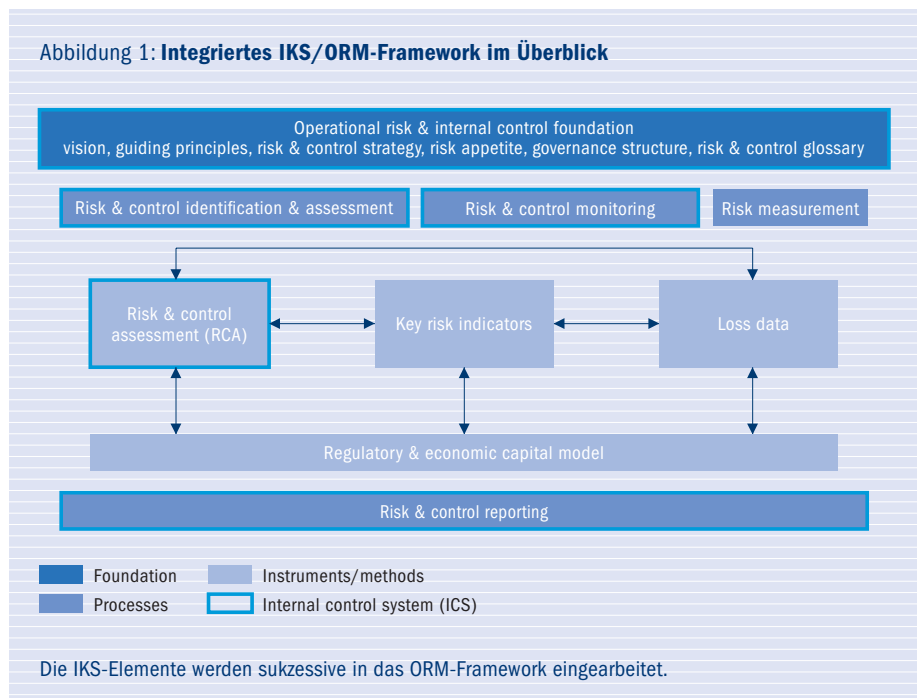
- Revisionsfähigkeit des Systems und damit Nachvollziehbarkeit der Aktivitäten; daraus leitet sich als logische Konsequenz die Dokumentation ab.

Ein bewährter Ansatz zum integrierten Management von ORM und IKS wird im Folgenden beschrieben.

Integrierter IKS/ORM-Ansatz

Der Startpunkt für die Integration von IKS, ORM und weiteren Kontrollfunktionen bildet das ORM-Framework, in das die IKS-Elemente sukzessive eingearbeitet werden (siehe Abbildung 1).

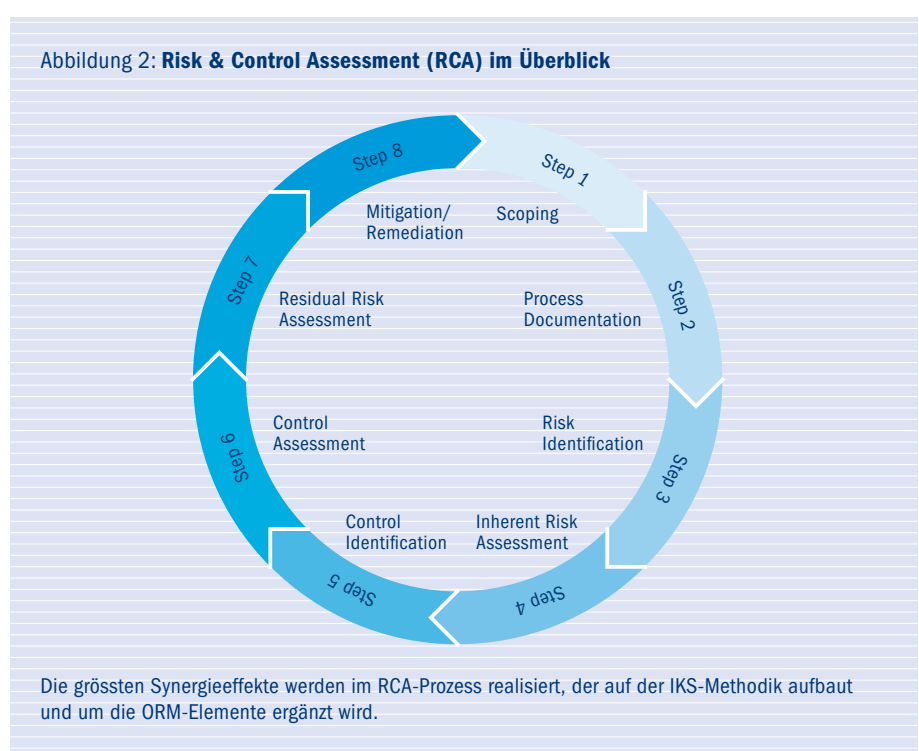
Abbildung 1: Integriertes IKS/ORM-Framework im Überblick



Die Basis des Frameworks bildet die Operational Risk & Internal Control Foundation: Hier sollen die bestehenden Komponenten wie Vision, Guiding Principles, Risk & Control Strategy, Risk Appetite, Governance Structure und Risk & Control Glossary um die Komponenten von IKS ergänzt werden. Loss Data (Vergangenheitsbezug) als Teil des Risk Measurement wird unverändert übernommen, da keine neuen Anforderungen seitens IKS gestellt werden. Key Risk Indicators (Zukunftsbezug) als Teil des Risk & Control Monitoring müssen aus rein regulatorischer Sicht in der Schweiz nicht zwingend implementiert werden. Risk & Control Assessments (Gegenwartsbezug) stehen im Zentrum der Verknüpfung der beiden Ansätze. Hier wurden früher die grössten Parallelitäten aufgebaut; entsprechend können hier auch die grössten Synergien realisiert werden. Auf diese Komponenten wird deshalb im nächsten Abschnitt noch vertieft eingegangen. Für Regulatory and Economic Capital Models bestehen im Bereich ORM in der Schweiz aus regulatorischer Sicht noch keine Anforderungen für Versicherungsunternehmen. Für Firmen, die den Solvency-II-Anforderungen genügen werden müssen, wird diese Komponente aber relevant sein. Das Risk & Control Reporting muss um die Informationsbedürfnisse aus allen Bereichen von IKS (Financial Reporting, Operations und Compliance) ausgebaut und ins ORM eingebettet werden.

Risk & Control Assessment

Beim Risk & Control Assessment (RCA) können die grössten Synergien gewonnen werden. Die IKS-Methodik bildet dabei die Basis und die ORM-Elemente werden eingebaut. Der RCA-Prozess kann in acht Schritte gegliedert werden (siehe Abbildung 2):



1. Scoping: Im Scoping werden die Prozesse und Abläufe der Unternehmung mit der Jahresrechnung (Bereich Financial Reporting), den Unternehmens- und Leistungszielen (Bereich Operations) sowie mit den Compliance-Anforderungen (Bereich Compliance) verknüpft. Daraus resultiert die Identifikation derjenigen Unternehmensprozesse, welche die Zielerreichung der Unternehmung in den genannten Bereichen massgeblich beeinflussen. Diese Kernprozesse bilden die

- Basis für den Aufbau des integrierten IKS/ORM-Systems (siehe Abbildung 3).
2. Process Documentation: Die im Schritt 1 «Scoping» als relevant identifizierten

Weil effizientes Risikomanagement zunehmend zum Wettbewerbsfaktor wird, zielen die neusten Entwicklungen auf die Integration und Harmonisierung von IKS, ORM und weiteren Initiativen ab.

3. Risk Identification: Die grössten Risiken Prozesse werden nun basierend auf allfällig bereits bestehenden Prozessunterlagen dokumentiert.

- für die Zielerreichung in den Bereichen Financial Reporting, Operations und Compliance werden nun auf Prozessstufe identifiziert und dokumentiert. Auf Basis des unternehmensweit definierten Risikokatalogs werden sie in die vier Kategorien Menschen, Prozesse, Systeme und externe Einflüsse eingeteilt.
- Inherent Risk Assessment: Die identifizierten Risiken werden bezüglich Eintrittswahrscheinlichkeit und Schadensausmass bewertet.
 - Control Identification: Existierende Kon-

trollen, die zur Adressierung der identifizierten Risiken implementiert wurden, werden identifiziert und dokumentiert.

- Control Assessment: Die identifizierten Kontrollen werden bezüglich ihrer Effektivität nach Design und Performance bewertet.
- Residual Risk Assessment: Durch die Kombination von Inherent Risk Assessment (Schritt 4) und Control Assessment (Schritt 6) wird das Restrisiko definiert.
- Mitigation/Remediation: Das Restrisiko wird ins Verhältnis zur Risikotoleranz

des Unternehmens gesetzt. Befindet sich das Restrisiko über der Toleranzgrenze, müssen Mitigation Actions zur weiteren Reduktion des bestehenden Risikos definiert werden.

Das beschriebene integrierte Modell kann zusammenfassend wie in Abbildung 4 (siehe Seite 12) dargestellt werden.

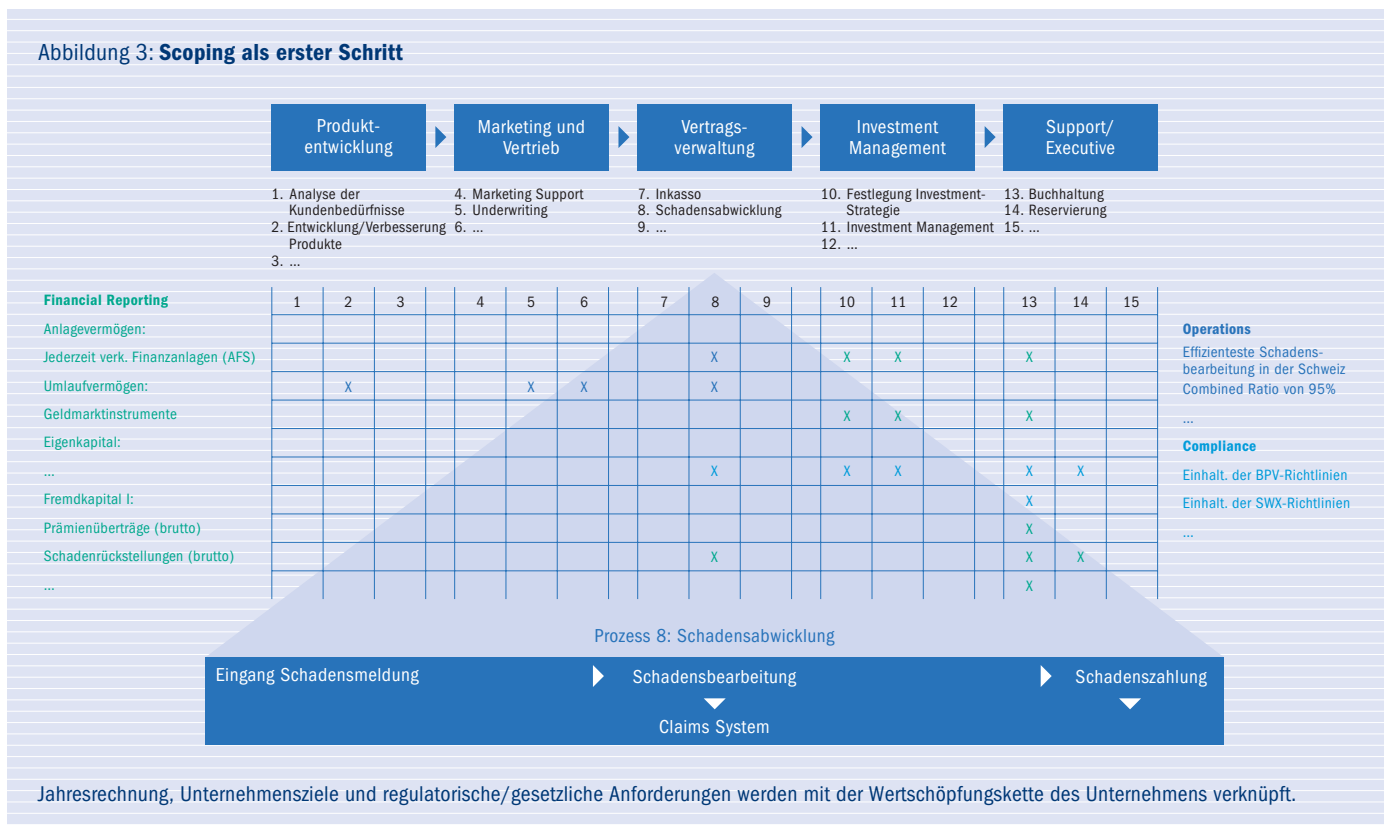
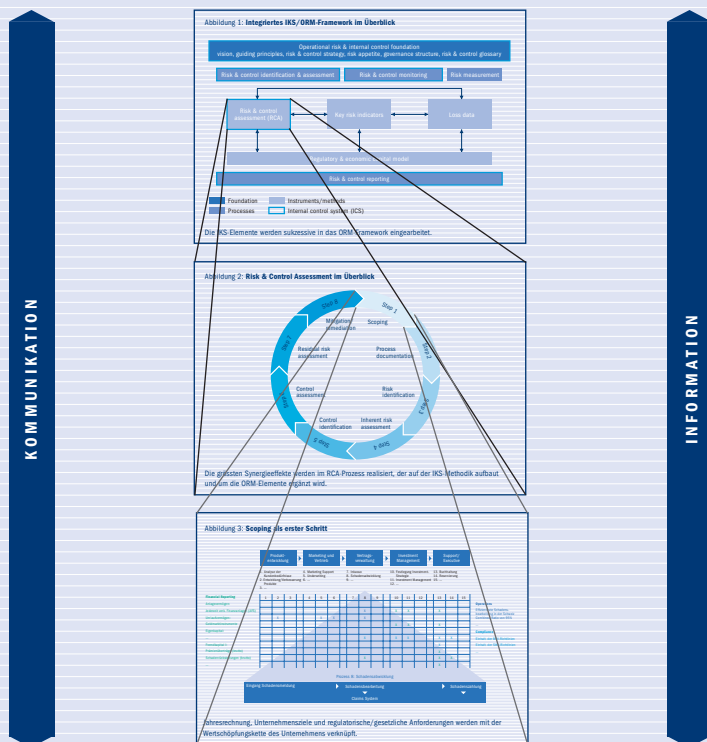


Abbildung 4: Integriertes IKS/ORM-Framework



Information und Kommunikation sind wesentliche Bestandteile beim Implementierungsprozess.

Vorteile und Herausforderungen

Der Nutzen eines integrierten IKS/ORM-Modells liegt in der systematischen Verknüpfung der verschiedenen Governance, Risk- und Kontrollorgane eines Unternehmens. Risiko- und Kontrollprozesse werden einheitlich definiert und Assessment- sowie Reportingprozesse aufeinander abgestimmt. Dadurch werden Redundanzen abgebaut, Lücken geschlossen – und die Reportings zu einer Gesamtaussage verdichtet. Was zählt, ist die Sicherheit als Ganzes und

nicht fragmentierte Betrachtungen innerhalb von verschiedenen Funktionen. Im Zentrum dieses Ansatzes steht die Generierung von Mehrwert und nicht die isolierte Adressierung von regulatorischen Anforderungen – was auch die Akzeptanz im Management sowie in der Linienorganisation erhöht.

Die Herausforderungen dieses integrierten ORM- und IKS-Ansatzes sind mehrschichtig. Er verlangt die Verschmelzung bisher unabhängiger Bereiche und Disziplinen. Das isolierte Wissen einer Disziplin

reicht beim integrierten Ansatz nicht aus. Zur erfolgreichen Implementierung bedarf es Spezialistenteams, die in allen Themen gleichermassen bewandert sind und darüber hinaus mehrjährige Branchenerfahrung mitbringen. Weil dieser Ansatz neu ist, sind zahlreiche Unternehmen auf kompetente Beratung angewiesen. ■