Risk Management & IKS-Konferenz 2024

Auditorium Willy G.S. Hirzel Zürich, 14. November 2024

Risk Management & IKS Essay-Kollektion 2024

29 essenzielle Risikomanagement & IKS – Themen für Sie aufbereitet

Christian Hafner, swissaxis AG – www.swissaxis.ch

swissaxis

Impressum

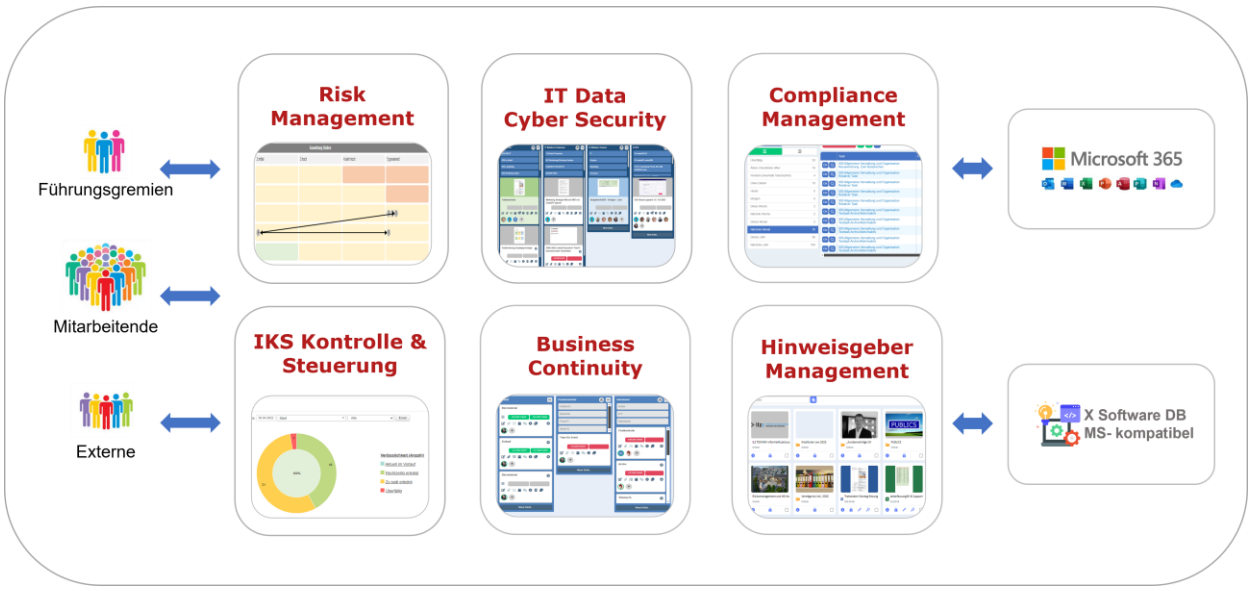
© 2024 Christian Hafner, swissaxis AG, CH-8606 Uster-Nänikon – www.swissaxis.ch

Umschlaggestaltung, Illustration: swissaxis AG
Lektorat, Korrektorat: Christian Hafner, Simone Hadorn
Übersetzung: Originalsprache Deutsch
Herausgeber: swissaxis AG
weitere Mitwirkende: Dr. Theo Altorfer, Susanne Sieber

Lösungen von swissaxis:
www.iks.ch (IKS Umsetzung)
www.swissrm.ch (Risk Management)
www.govv.ch (High End Cloud Dokumente)

Vorwort

Früher genügte es, mittels IKS die finanzrelevanten Prozesse sicherzustellen und damit die Abschlussprüfer zufriedenzustellen. Heute wird eine umfassende Good Governance erwartet. Das bedeutet eine Verknüpfung von Prozessen, Anwendungen, Verhaltensweisen und Tools zu einem umfassendes Chancen- und Risikomanagement.



Es braucht also eine ganzheitliche Herangehensweise an das Chancen- und Risikomanagements. Genau dafür steht swissaxis als Partner von KMU und Organisationen der öffentlichen Hand. Und als Vordenker in diesen Themen publizieren wir weiterhin aktiv unsere Essays, die wir für Sie wieder kompakt zusammengestellt haben. Damit haben Sie neben den Konferenzinhalten eine weitere Quelle für Ihre Inspiration.

Die Konferenzveranstalter

Dr. Theo Altorfer Susanne Sieber Christian Hafner

Inhalt

3 Vorwort

5 Wie Geschäftsprozesse dokumentieren und die Risiken managen?

10 Laufende Identifizierung der Risiken mit KI

13 Das IKS kann mehr als Kontrolle

16 Chancen erfolgreich wahrnehmen dank Risk Management

20 Good Governance: Von der Pflicht zur Kür

23 RM + IKS: Rivalen, Geschwister, Partner?

26 Homeoffice und Risk Management

28 Die grössten Risiken für Gemeinden und Städte

33 Das Risiko «Menschliche Schwäche»

Wie Geschäftsprozesse dokumentieren und die Risiken managen?

Mit Checklisten und IKS effektiv und effizient den Risikoeintritt vermeiden.

Gemäss einer KPMG-Studie sahen die Befragten folgende Nutzen im Einsatz eines IKS für das Management von Geschäftsprozessen.

- Aufdeckung von Prozessschwächen (65%)
- Schaffung von Transparenz in den Prozessen (63%)
- Einhaltung von internen Regelungen (63%)
- Harmonisierung von Prozessen (59%)

Prozesse ermöglichen die Wiederholung von Erfolgen, verhindern wiederkehrende Fehler und eliminieren menschliches Versagen – in den eigenen Abläufen und denen der Kunden.

Deshalb liegt es auf der Hand, Prozesse zu dokumentieren. Die Frage ist aber wie detailliert. Je detaillierter die Dokumentation, desto grösser der Aufwand für deren Nachführung und Kontrolle.

Ein sinnvoller Ansatz ist es, die Tiefe der Prozessdokumentation aus Risikosicht zu beurteilen – je risikoreicher desto detaillierter. Deshalb in jedem Prozess die neuralgischen Prozessschritte identifizieren und diese dokumentieren – mit einer Checkliste.

Workflow vs. Prozess

Kürzlich an einem Meeting präsentiert uns ein Kunde einen Workflow. Das Diagramm für den betroffenen administrativen Prozess war bis ins kleinste Detail durchdacht. X Stunden Denk- und Zeichenarbeit waren hineingeflossen.

Eine perfekte Basis für die Umsetzung als automatisierte ereignisgesteuerte Prozesskette mit allen Wenn-Dann-Ja-Nein-Verzweigungen.

Aber wäre das wirklich zielführend? Sind alle Prozessschritte vorhersehbar, und muss jeder Prozessschritt ereignisgesteuert sein?

In der Administration (vs. Produktion) kann nur ein kleiner Teil in strukturierten Prozessen vorgedacht werden. Die meisten administrativen Prozesse sind unstrukturiert oder nur in Teilen strukturierbar, denn sie sind nicht oder kaum vorhersehbar. Derartige Prozesse oder Fälle können deshalb nicht Ereignis- sondern müssen Sachbearbeiter-gesteuert werden.

Anstatt Prozesse wäre deshalb die Bezeichnung Aufgabenketten treffender. Wieso?

.

Viele assoziieren mit dem Wort Prozess einen Ablauf wie bei einem Fliessband. Dinge werden, ja müssen, hintereinander erledigt werden. Zuerst das Rad dann die Radmutter, etc. In administrativen Abläufen ist das aber anders. Dort kann, um beim Bild zu bleiben, oft wahlweise zuerst die Radmutter und dann das Rad, oder umgekehrt, montiert werden.

Checklisten und ein IKS sind entscheidend, um Geschäftsprozesse zu dokumentieren und Risiken effizient zu managen, indem sie Transparenz schaffen, Prozessschwächen aufdecken und die Einhaltung interner Regelungen sicherstellen.

Deshalb sprechen wir von Aufgaben, die zwar in Aufgabenketten beschrieben sind, aber nicht unbedingt hintereinander erledigt werden müssen.

Checklisten anstatt Flowcharts

Auch bei administrativen, Sachbearbeiter-gesteuerten Aufgabenketten gilt es, Fehler zu vermeiden.

Sachbearbeiter nehmen aber erfahrungsgemäss die Prozess-Flowcharts nicht zur Hand und erzielen trotzdem gute Ergebnisse. Wieso?

Als Prozessverantwortliche entscheiden sie aufgrund ihrer Erfahrung, was die nächsten Schritte sind. Sie benutzen eine Checkliste. Die Checkliste kann schriftlich oder nur mental vorhanden sein.

Menschen benutzen Checklisten als eine Art kognitives Netz. Sie kanalisieren unser Denken – die Aufmerksamkeit und Gründlichkeit. Zudem lassen sie Raum für die eigene Urteilsfähigkeit und um auf unerwartete Schwierigkeiten zu reagieren.

Ein kluger Ansatz zur Dokumentation von administrativen Prozessen ist deshalb die Checklisten zu formalisieren.

Denken Sie an Ärzte, Piloten, Ingenieure, und Feuerwehren. Alle benutzen Checklisten.

Wenn Checklisten nützlich sind, um Fehler bei der Arbeit mit Menschenleben zu verhindern, dann sind sie vermutlich auch ein gutes Arbeitsinstrument bei Nicht-Leben-oder-Tod-Jobs.

Vorgehen in der Praxis

Um sicherzustellen, dass wichtige Schritte in Geschäftsprozessen nicht übersehen und Risiken minimiert werden, fordern Sie Ihre Sachbearbeiter dazu auf, Checklisten zu erstellen und die neuralgischen Stellen mit hohem Risiko zu kennzeichnen.

So gehen Sie am besten vor:

1. Kommunikation der Bedeutung:
Beginnen Sie damit, die Bedeutung von Checklisten und die Gründe für ihre Implementierung zu kommunizieren. Erklären Sie den Mitarbeitern, wie Checklisten dazu beitragen können, Fehler zu reduzieren, die Effizienz zu steigern und Risiken zu minimieren. Stellen Sie sicher, dass sie verstehen, dass ihr Beitrag zur Erstellung dieser Checklisten wichtig ist.

2. Identifizierung der relevanten Prozesse:
Arbeiten Sie mit den Sachbearbeitern zusammen, um die Prozesse zu identifizieren, für die Checklisten erstellt werden sollen. Bitten Sie sie, ihre Verantwortungsbereiche zu überprüfen und diejenigen Prozesse auszuwählen, die besonders kritisch oder risikoreich sind.

3. Analyse der Prozessschritte:
Gemeinsam mit den Sachbearbeitern analysieren Sie jeden ausgewählten Prozess im Detail. Identifizieren Sie die einzelnen Schritte und entscheiden Sie, welche davon besonders wichtig oder risikobehaftet sind. Diese Schritte sind diejenigen, die in der Checkliste besonders betont werden sollten.

4. Erstellung der Checkliste:
Bitten Sie die Sachbearbeiter, basierend auf der Analyse, Checklisten für die identifizierten Prozesse zu erstellen. Geben Sie klare Anweisungen, was in die Checkliste aufgenommen werden soll, wie z.B. spezifische Aufgaben, zu überprüfende Informationen, Kontrollpunkte oder Fristen.

5. Kennzeichnung der neuralgischen Stellen:
Fordern Sie die Sachbearbeiter auf, die neuralgischen Stellen mit hohem Risiko in ihren Prozessen zu kennzeichnen. Dies könnten kritische Entscheidungspunkte, potenzielle Fehlerquellen oder Bereiche mit rechtlichen oder finanziellen Auswirkungen sein.

6. Überprüfung und Feedback:
Sobald die Checklisten erstellt wurden, überprüfen Sie diese gemeinsam mit den Sachbearbeitern auf Vollständigkeit, Klarheit und Wirksamkeit. Geben Sie Feedback und nehmen Sie gegebenenfalls Anpassungen vor, um sicherzustellen, dass die Checklisten ihren Zweck erfüllen.

7. Schulung und Implementierung:
Stellen Sie sicher, dass alle betroffenen Mitarbeiter angemessen geschult werden, um die Checklisten zu verwenden. Implementieren Sie dann die Checklisten in die entsprechenden Prozesse und stellen Sie sicher, dass ihre Verwendung regelmässig überwacht wird.

Umsetzung im Risk Management

Prozessrisiken gehören hauptsächlich zur Kategorie* «Vermeidbare Risiken». Also Risiken, die aus der Organisation heraus entstehen und keinen strategischen Nutzen bringen. Sie sollten vermieden oder kosteneffizient beseitigt werden.

Für das Management dieser Risiken empfiehlt sich der Einsatz des internen Kontrollsystems (IKS). Im IKS können die identifizierten neuralgischen Checks als Kontrollaufgaben abgebildet werden. Je nach Risiko sollte entschieden werden, ob eine prozessinvolvierte Person die Kontrolle durchführen soll oder eine vom Prozess unabhängige Person. Ebenfalls ist festzulegen, ob die Kontrolle vorgelagert oder nachgelagert und als Voll- oder Stichprobenkontrolle durchgeführt werden soll.

Und schliesslich muss geregelt werden, ob und wie ein allfälliger Kontrollnachweis dokumentiert werden muss.

**Die beiden weiteren Risikokategorien sind strategische und externe Risiken.*
*– **Strategische Risiken** sind Risiken, die eingegangen werden, um einen höheren strategischen Nutzen zu erzielen. Es sollten Schritte unternommen werden, um ihre Wahrscheinlichkeit und Auswirkungen kosteneffizient zu verringern.*
*– **Externe Risiken** sind unkontrollierbare Risiken. Sie erfordern besondere Prozesse, die Manager dazu ermutigen, diese Risiken offen zu diskutieren und kosteneffiziente Wege zu finden, um ihre Wahrscheinlichkeit zu verringern oder ihre Folgen abzumildern.*

Quellen:
KPMG-Studie zitiert in «Mit internen Kontrollsystemen erfolgreich wirtschaften», Springer Professional 19.9.2108

FAZIT

Jeder Prozess kann als Workflow dargestellt werden. Aber nicht jeder Workflow kann als Prozess strukturiert werden. Hüten Sie sich davor, Prozesse zu (über-)designen in denen Sachbearbeiter entscheiden dürfen, was die nächsten Schritte sind und wenn, sie an der Bearbeitung des Falls beteiligen. Die Checklisten der Sachbearbeiter sind ein effektives und effizientes Mittel, um Risiken zu erkennen. Das IKS schliesslich ist der geeignete Ort, um die Risiken in den neuralgischen Prozessschritten zu managen.

Laufende Identifizierung der Risiken mit KI

Rollendes, dynamisches Identifizieren von Risiken mittels künstlicher Intelligenz (KI)

Die effektive Identifizierung von Risiken in Unternehmen, Not-for-Profit- und kommunalen oder kantonalen Organisationen ist von entscheidender Bedeutung für deren langfristigen Erfolg und Stabilität.

Traditionelle Ansätze des Risikomanagements stossen jedoch oft an ihre Grenzen, insbesondere angesichts der ständigen Veränderungen in der globalen Wirtschaft, der politischen Landschaft und der technologischen Entwicklungen.

Hier setzt die Nutzung von künstlicher Intelligenz (KI) für die kontinuierliche Identifizierung von Risiken an. Ein Ansatz, der als «rollendes, dynamisches Identifizieren von Risiken» bezeichnet werden kann.

Die Herausforderung der Risikoidentifizierung

Die Identifizierung von Risiken ist eine komplexe Aufgabe, die eine umfassende Analyse verschiedener Informationsquellen erfordert.

Dazu gehören nicht nur interne Daten wie Reglemente, Verträge und Geschäftszahlen, sondern auch externe Informationen wie politische Entwicklungen, rechtliche Veränderungen und Marktbedingungen.

> *KI-gestützte, kontinuierliche Risikoidentifizierung hilft Unternehmen, sich an ständig wechselnde globale, politische und technologische Entwicklungen anzupassen.*

Die Herausforderung besteht darin, all diese Daten zu sammeln, zu verarbeiten und zu analysieren, um potenzielle Risiken frühzeitig zu erkennen und angemessen darauf reagieren zu können.

Der Einsatz von KI für das Risikomanagement

KI bietet eine vielversprechende Lösung für die Herausforderungen der Risikoidentifizierung, insbesondere in Bezug auf die Verarbeitung und Analyse grosser Datenmengen in Echtzeit.

Durch den Einsatz von maschinellem Lernen und anderen KI-Techniken können Unternehmen und Organisationen komplexe Muster und Zusammenhänge in den Daten erkennen, die für die Identifizierung von Risiken relevant sind.

Ein entscheidender Vorteil von KI ist die Fähigkeit, Modelle kontinuierlich zu trainieren und anzupassen, um sich verändernde Bedingungen und neue Informationen zu berücksichtigen.

Dies ermöglicht ein «rollendes, dynamisches Identifizieren von Risiken», bei dem das Risikomanagement nicht als einmalige Aufgabe betrachtet wird, sondern als kontinuierlicher Prozess, der sich an die sich ändernde Umgebung anpasst.

Implementierung

Die erfolgreiche Implementierung eines KI-gestützten Risikomanagements erfordert eine sorgfältige Planung und Integration verschiedener Datenquellen und KI-Technologien.

Unternehmen und Organisationen sollten sicherstellen, dass ihre Datenqualität hoch ist und dass sie über die erforderlichen Ressourcen und Fachkenntnisse verfügen, um KI-Modelle effektiv zu trainieren und zu implementieren.

Es gibt verschiedene KI-Technologien und Plattformen, die für das Risikomanagement genutzt werden können, darunter «Generative AI Models» wie Gemini 1.5 Pro von Google oder Maschinenlernprogramme wie TensorFlow und PyTorch oder.

Darüber hinaus können spezialisierte Dienstleister massgeschneiderte Lösungen anbieten, die den spezifischen Anforderungen eines Unternehmens oder einer Organisation entsprechen.

Datenschutz und Datensicherheit

Die Integration von KI in das Risikomanagement bringt zahlreiche Vorteile mit sich, birgt jedoch auch potenzielle Risiken im Hinblick auf Datenschutz und Datensicherheit. Unternehmen und Organisationen müssen sicherstellen, dass die Informationen, die sie an KI-Systeme weitergeben, angemessen geschützt sind und nicht unautorisiert offengelegt oder missbraucht werden.

Eine Möglichkeit, den Datenschutz zu gewährleisten, besteht darin, robuste Sicherheitsmassnahmen zu implementieren, einschliesslich der Verschlüsselung von Daten während der Übertragung und Speicherung sowie der Zugriffssteuerung und Authenti- fizierung von Benutzern. Darüber hinaus sollten Unternehmen sicherstellen, dass sie sich an geltende Datenschutzgesetze und -richtlinien halten und sicherstellen, dass ihre KI-Anbieter ebenfalls strenge Datenschutzstandards einhalten.
Ein weiterer wichtiger Aspekt ist die Transparenz und Kontrolle über die Verwendung von Daten durch KI-Systeme. Unternehmen sollten klare Richtlinien und Vereinbarungen festlegen, die den Umfang und die Zwecke der Datenverwendung durch die KI definieren.

Dies umfasst
•Datenschutzvereinbarungen
•Datenschutzrichtlinien
•Mechanismen zur Überwachung und Überprüfung der Datenverarbeitung.

Durch die Umsetzung dieser Massnahmen können Unternehmen und Organisationen die Vorteile von KI-gestütztem Risikomanagement voll aus-schöpfen, während sie gleichzeitig sicherstellen, dass die Vertraulichkeit, Integrität und Verfügbarkeit ihrer Daten gewährleistet sind.

FAZIT

Die Integration von KI in das Risikomanagement bietet die Möglichkeit, Risiken frühzeitig zu erkennen, fundierte Entscheidungen zu treffen und die Resilienz und Widerstandsfähigkeit von Unternehmen und Organisationen zu stärken. Durch ein rollendes, dynamisches Identifizieren von Risiken können sie sich besser auf die Herausforderungen der Zukunft vorbereiten und langfristigen Erfolg sichern. Datenschutz und Datensicherheit muss aber ein integraler Bestandteil jeder KI-Implementierung sein, um das Vertrauen der Stakeholder zu erhalten und langfristigen Erfolg zu sichern.

Das IKS kann mehr als Kontrolle

Seine volle Wirkung entfaltet das IKS, wenn es als Steuerungssystem gelebt wird.

Mitarbeiterinnen und Mitarbeiter wissen, dass Kontrollen nützlich sind. Sie kontrollieren ihre Arbeitsschritte selbst – intuitiv oder mit Checkliste – damit ihr Arbeitsergebnis stimmt.

Auf dieser Kultur muss ein IKS aufsetzen. Ein IKS, welches auch von den Mitarbeiterinnen und Mitarbeitern gestaltet und getragen wird, ist die beste Risiko-Sicherung.

Anstelle von Bedenken wie: «Ist man nicht mehr zufrieden mit meiner Arbeit? Soll ich nun überwacht werden?» tritt Überzeugung von Mitarbeitern, auch für das Risikomanagement und IKS Mit-Verantwortung zu übernehmen.

Gleichzeitig lohnt sich eine Rückbesinnung auf die Anfänge des IKS.

Vom IKS zurück zum ICS

Der Begriff des IKS wurde ursprünglich wortwörtlich aus dem Amerikanischen übersetzt. Dabei ging die Bedeutung des «C» leider verloren.

Das Wort «Controls» bedeutet nicht Überwachung und Kontrolle. Sondern sich um etwas kümmern, für etwas die Verantwortung übernehmen.

> *Das IKS entfaltet seine volle Wirkung als Steuerungssystem, wenn es von Mitarbeitern gestaltet und getragen wird, und fördert so eine Kultur der gemeinsamen Verantwortung statt bloßer Überwachung.*

Besser wäre es also, gar nicht von Kontrollen zu sprechen, sondern das IKS, oder ICS als das zu bezeichnen, was es im Idealfall wirklich ist – ein Steuerungs- und Führungsinstrument.

swissIKS®

IKS – natürlich digitalisiert.
www.iks.ch

Microsoft Partner Network

BDO SCHWEIZ Kooperation

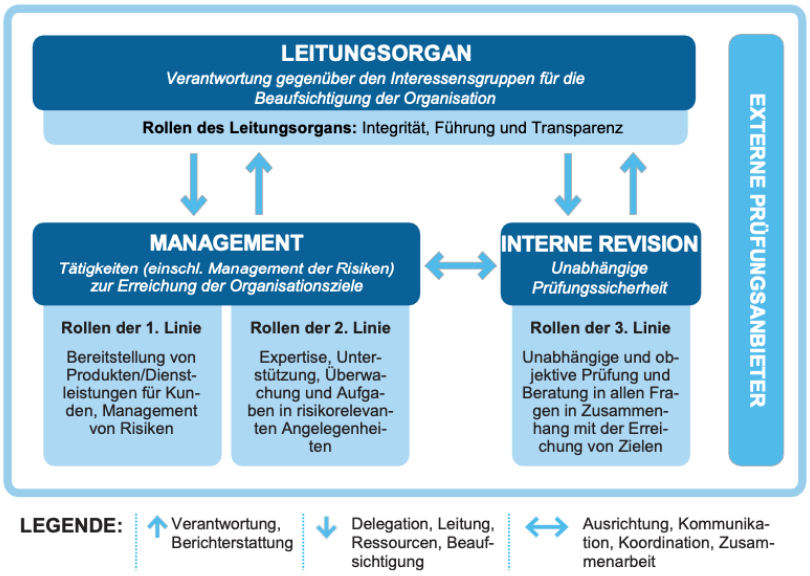
Fokus eines ICS als Steuerungs-system

Ein ICS betont die aktive Gestaltung und Lenkung von Unternehmensprozessen.
Es dient primär zur strategischen Steuerung und Entwicklung des Unternehmens; sekundär zur Verhinderung von Verstössen.
Es unterstreicht die Wichtigkeit und Notwendigkeit, Mitarbeiter als wertvolle Partner in diesem Prozess zu sehen, anstatt sie lediglich zu kontrollieren.

Das übergeordnete Ziel bei der Einführung oder Erneuerung eines IKS / ICS muss es sein, eine Unternehmenskultur zu schaffen, in der die Einhaltung von (Compliance-) Richtlinien in tägliches Handeln integriert ist und von allen als wertvolle Unterstützung für ihre Arbeit empfunden wird.

Der Anfang, der Start

In vielen Unternehmen liegt die Verantwortung für das IKS im Finanzbereich. Nicht zuletzt deshalb, weil die Wirtschaftsprüfer jährlich die Existenz des IKS bestätigen müssen. Deshalb beginnt ein IKS-Projekt häufig dort. Von hier aus kann es zu einem ICS-Steuerungssystem weiterentwickelt werden.



Glücklicherweise gibt es einen Positionsbezug der wichtigsten Berufsorganisation im Thema Überwachung der finanziellen Führung – dem Institute of Internal Auditors (IIA) – dazu. Das IIA hat das IKS nämlich bereits vor drei Jahren zu einem Teil des (unternehmensweiten) Riskmanagements erklärt.

Jetzt muss die Praxis nur noch der Lehre folgen und die organisatorische Trennung zwischen IKS und Risikomanagement auflösen, womit das **IKS als Teil des Riskmanagements** endlich von strategischer Bedeutung wird.

Quellen: «Compliant dank IKS» Vortrag von Daniela Sandmann, Geschäftsführerin, A-ROSA Reederei GmbH und Partnerin ACC Treuhand AG anlässlich der Risk Management & IKS-Konferenz vom 16. November 2023
-Erkenntnis 1 aus der IKS-Konferenz vom 24. November 2021
-Erkenntnis 2 aus der Risikomanagement & IKS-Konferenz vom 16. November 2022
-Deutsches Institut für Interne Revision, IIA Positionspapier: Das Drei-Linien-Modell, Juli 2020

FAZIT

Trotz offensichtlichem Nutzen wie Qualitätssicherung, Kundenzufriedenheit und Risikominimierung sind Kontrollen bei Mitarbeitenden und auch bei Vorgesetzten unbeliebt, wenn sie sie als Überwachung auf Fehlverhalten empfinden.

Sobald die Mitarbeiter aber als wertvolle Partner am Prozess beteiligt sind, verstehen sie den Nutzen ihres (Kontroll-)Beitrag zur Steuerung und Entwicklung des Unternehmens.

Diese Entwicklung wird unterstützt, wenn das Finanz-IKS zu einem Unternehmens-IKS-ICS aufgewertet wird, und es ins Enterprise Risk Management integriert wird.

Verunsicherung kann minimiert werden, wenn ein IKS bereichsweise eingeführt wird. So kann vermittelt werden, dass die erarbeiteten Kontrollen die Verlässlichkeit des Arbeitsbeitrags erhöhen und Risikoevents anzeigen

Chancen erfolgreich wahrnehmen dank Risk Management

Erfolgsversprechende Geschäftschancen schützen mittels relevantem Risikomanagement

Jede Organisation, die Chancen erfolgreich wahrnehmen möchte, trifft unweigerlich auf Herausforderungen und Krisen, die es zu meistern gilt.

Alle Entscheidungen und Aktivitäten sind deshalb mit Risiken verbunden, und das Risikomanagement (RM) dient dazu, die Chancen z.B. aus der strategischen Geschäftsplanung selbstbewusst ergreifen zu können.

In der Praxis hat sich ein 5-Schritte-Prozess bewährt, um keine Chance zu verpassen, resp. die mit jeder Chance einhergehenden Risiken zu managen.

- Festlegen von Umfang und Kontext der Risikobeurteilung
- Festlegen Risikokategorien und -kriterien
- Risikoidentifikation
- Risikoanalyse und -bewertung
- Risikobehandlung

> *Der erste Schritt im Risikomanagement ist die Festlegung von Umfang, Grenzen und Kontext der Risikobeurteilung, um eine effiziente Nutzung von Zeit und Ressourcen zu gewährleisten.*

Schritt 1: Festlegen von Umfang und Kontext der Risikobeurteilung

Der erste Schritt besteht darin, den Umfang, die Grenzen und den Kontext festzulegen. Dies gewährleistet eine bessere Nutzung von Zeit, Aufwand und Ressourcen der Organisation.

Ein sinnvoller Ansatz ist die strategische Geschäftsplanung, die Unternehmensbereiche und die (grössere) Projekte auf Chancen und Risiken zu untersuchen.

Der Erarbeitungsprozess – in Anlehnung an die ISO-Norm 31000:2018 für das Risikomanagement – gliedert sich wie folgt:

Schritt 2: Festlegung der Risikokategorien und -kriterien

Risikokriterien sind eine Reihe von Regeln oder Aussagen, die eine einheitliche Entscheidungsfindung ermöglichen. Die Verwendung von Risikokriterien unterstützt eine bessere Entscheidungsfindung.
Ein zielführender Ansatz ist es, die Risikokriterien in Risikokategorien zu bündeln. Es empfiehlt sich die Einteilung in drei Kategorien von Risiken, die jeweils einen anderen Risikomanagementansatz erfordern.

– **Vermeidbare Risiken** entstehen aus der Organisation heraus und bringen keinen strategischen Nutzen. Sie sollten vermieden oder kosteneffizient beseitigt werden.

– **Strategische Risiken** sind Risiken, die eingegangen werden, um einen höheren strategischen Nutzen zu erzielen. Es sollten Schritte unternommen werden, um ihre Wahrscheinlichkeit und Auswirkungen kosteneffizient zu verringern.

– **Externe Risiken** sind unkontrollierbare Risiken. Sie erfordern besondere Prozesse, die Manager dazu ermutigen, diese Risiken offen zu diskutieren und kosteneffiziente Wege zu finden, um ihre Wahrscheinlichkeit zu verringern oder ihre Folgen abzumildern.

Schritt 3: Risikoidentifikation

Aus Schritt 1 und 2 ergibt sich der Rahmen für die Identifizierung und Zuteilung der zu den Chancen gehörenden Risiken. Das Resultat kann übersichtlich in einer Matrix der Risikokategorien und der Risikoherkunft dargestellt werden.

Risikoherkunft / Risiko-Kategorien	Strategie-ziele	Unter-nehmens-bereiche	Pro-jekte
Vermeid-bare Risiken			
Stra-tegische Risiken			
Externe Risiken			

Schritt 4: Risikoanalyse und -bewertung

Ein Risiko zu analysieren, bedeutet das Risiko zu verstehen und ist die Grundlage für die Bewertung.

Eine eigentliche Bewertung ist nur für die strategischen und externen Risiken notwendig, denn die vermeidbaren Risiken können/sollen vermieden oder kosteneffizient beseitigt werden.

Die Vermeidung der Risiken kann mittels internem Kontrollsystem (IKS) erfolgen.

Vorgehen: In einem Bottom-up-Ansatz die Prozesse nach vermeidbaren Risiken durchkämmen und die «Schlüssel-Checks» zur Vermeidung/Beseitigung der Prozessrisiken als Kontrollen in ein dynamisches IKS einpflegen.

Für jedes zu bewertende Risiko muss entschieden werden,

- wer bewertet (interne, externe Experten und wie viele) und
- wie oft soll bewertet werden.

Die Bewertung selbst erfolgt nach einem einheitliche Raster für Eintretenswahrscheinlichkeit, Schadenhöhe und Einfluss auf die Reputation.

Je grösser die Anzahl der Bewerter und je öfter bewertet wird, desto notwendiger wird eine Dynamisierung des RM-Prozesses.

Das Resultat der Bewertung(en) erhält der sog. Risk Owner und sein Stellvertreter.

Schritt 5: Risikobehandlung

Die Behandlung strategischer und externer Risiken erfordert einen umfassenden Ansatz, der sowohl präventive als auch reaktive Massnahmen umfasst.

Es ist in der Verantwortung der Risk Owner, dass zeitgerechte angemessene Massnahmen ergriffen werden.

Organisatorisch ist festzulegen, wer über die Durchführung der Massnahmen entscheidet. Meistens ist es sinnvoll, die Entscheide gemeinsam als Leitungsorgan zu fällen, da Kosten und Nutzen oft in mehreren Bereichen anfallen.

Es versteht sich von selbst, dass die Umsetzung der Massnahmen, resp. deren Ergebnis ebenfalls überwacht werden muss – am sinnvollsten als Teil desselben dynamischen RM-Prozesses wie für die Risikobewertung.

FAZIT

Es besteht ein signifikanter Zusammenhang zwischen langfristigem Erfolg und dem bewussten Umgang mit Risiken.

Die Integration von Risiko und Strategie ermöglicht es den Leitungsorganen, die besten Chancen auszuwählen und relevante Risiken zu managen.

Good Governance: Von der Pflicht zur Kür

Wer Risikomanagement nur betreibt, um die Abschlussprüfer zufriedenzustellen, verpasst die Chance für eine umfassende Good Governance.

Unternehmen stehen in der heutigen komplexen Geschäftswelt vor zahlreichen Herausforderungen, die von dynamischen Marktbedingungen bis hin zu technologischen Entwicklungen reichen.

Die Zeiten sind vorbei, als es genügte, mittels IKS die finanzrelevanten Prozesse sicherzustellen und die Abschlussprüfer zufriedenzustellen. Um erfolgreich zu agieren, ist ein umfassendes Chancen- und Risikomanagement für eine Good Governance unerlässlich.

Die Good Governance ist dann erreicht, wenn bestimmte Prozesse, Anwendungen, Verhaltensweisen und Tools vollständig in der Führungsarbeit integriert sind.

1.Enterprise Risk Management (ERM): Die Grundlage für strategische Entscheidungen

Enterprise Risk Management bildet den Kern eines effektiven Chancen- und Risikomanagements.
Dieser Prozess ermöglicht es Unternehmen, Risiken auf organisatorischer Ebene zu identifizieren, zu bewerten und zu steuern. ERM schafft eine umfassende Sicht auf die Risikolandschaft und ermöglicht es Führungskräften, strategische Entscheidungen auf einer fundierten Basis zu treffen.
Durch die Integration von ERM wird die Risikokultur im gesamten Unternehmen gestärkt, und die Organisation kann flexibel auf Veränderungen reagieren.

2. Interne Kontrolle & Steuerung: Effiziente Überwachung und Lenkung von Prozessen

Die Implementierung eines internen Kontrollsystems (IKS) ist entscheidend, um Risiken zu minimieren und Compliance sicherzustellen. Eine klare Struktur von internen Kontrollen und Steuerungen gewährleistet die Einhaltung von Unternehmensrichtlinien und -prozessen.

Dieser Schritt ist essenziell, um die Wirksamkeit der unternehmerischen Tätigkeiten sicherzustellen und potenzielle Risiken frühzeitig zu erkennen. Durch die Verknüpfung von internen Kontrollen mit ERM wird eine ganzheitliche Herangehensweise an das Risikomanagement geschaffen.

3. Compliance (Risk) Management: Rechtliche Anforderungen und ethische Standards im Blick

Das Compliance (Risk) Management stellt sicher, dass Unternehmen gesetzliche Anforderungen und ethische Standards einhalten.

Durch die Integration von Compliance in das Risikomanagement können potenzielle rechtliche Risiken frühzeitig erkannt und gemindert werden. Dies schafft nicht nur rechtliche Sicherheit, sondern stärkt auch das Vertrauen der Stakeholder in die Integrität des Unternehmens.

4. Hinweisgeber-Management: Früherkennung durch interne Informationen

Ein effektives Chancen- und Risikomanagement erfordert auch einen offenen Kommunikationskanal für Mitarbeiter, Kunden und andere Stakeholder.

Das Hinweisgeber-Management ermöglicht es, frühzeitig auf mögliche Risiken oder ethische Verstösse aufmerksam zu werden. Eine Kultur der Offenheit und Transparenz ist entscheidend, um relevante Informationen zu erhalten und schnell auf potenzielle Probleme reagieren zu können.

Es reicht nicht aus, lediglich die finanzrelevanten Prozesse sicherzustellen und die Abschlussprüfer zufriedenzustellen; vielmehr ist ein umfassendes Chancen- und Risikomanagement unerlässlich für eine effektive Good Governance.

5. IT, Data, Cyber Security Management: Schutz vor digitalen Risiken

Angesichts der zunehmenden Digitalisierung ist ein umfassendes Management von IT-, Daten- und Cyber-Security-Risiken unerlässlich.

Die Integration dieser Komponenten in das Chancen- und Risikomanagement stellt sicher, dass Unternehmen gegen digitale Bedrohungen gewappnet sind. Die kontinuierliche Überwachung und Anpassung der Sicherheitsmassnahmen gewährleisten den Schutz sensibler Informationen und die Aufrechterhaltung der Geschäftskontinuität.

Business Continuity Management: Vorbereitung auf Unvorhergesehenes

Abschliessend ist das Business Continuity Management von entscheidender Bedeutung.

Es stellt sicher, dass Unternehmen auch in Krisensituationen handlungsfähig bleiben. Die Entwicklung von Notfallplänen und die regelmässige Überprüfung der Geschäftskontinuität gewährleisten, dass das Unternehmen auf unvorhergesehene Ereignisse vorbereitet ist und schnell wieder in den Normalbetrieb übergehen kann.

FAZIT

Good Governance steht für die Notwendigkeit einer ganzheitlichen Herangehensweise an das Chancen- und Risikomanagement.
Die Integration von Enterprise Risk Management, internen Kontrollen, Compliance-Management, Hinweisgeber-Management, IT- und Cybersecurity-Management sowie Business Continuity Management bildet die Basis für eine effektive Risikoreduktion und ermöglicht Unternehmen, in einem dynamischen Umfeld erfolgreich zu agieren.
Nur durch die Verknüpfung dieser Prozesse, Anwendungen, Verhaltensweisen und Tools kann ein umfassendes Chancen- und Risikomanagement gewährleistet werden.

RM + IKS: Rivalen, Geschwister, Partner?

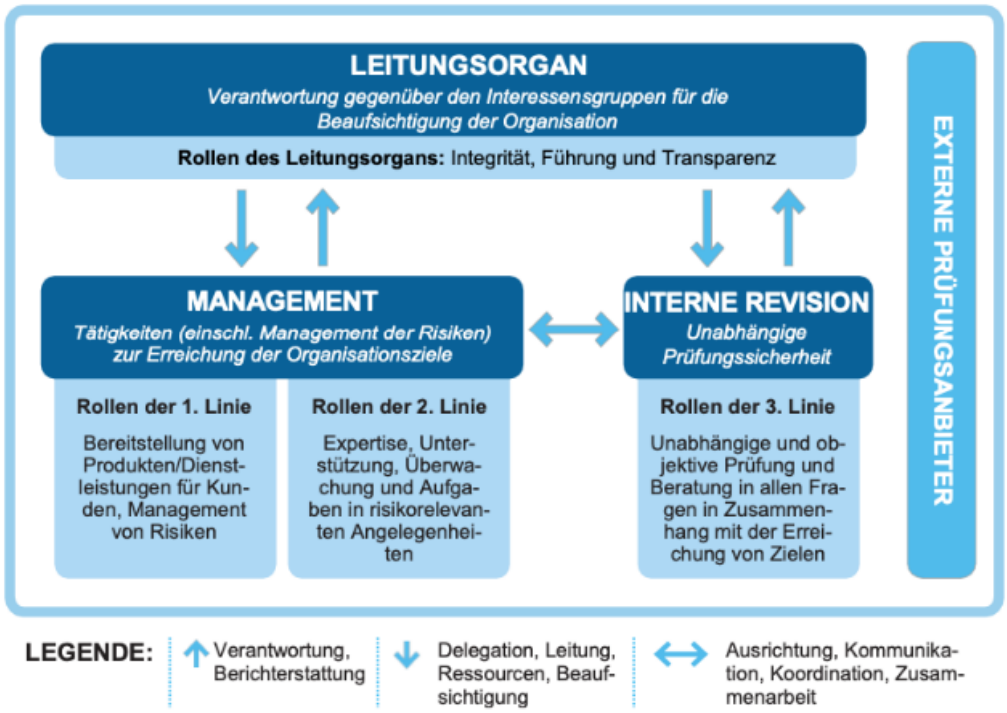
Auf welche Governance-Stufe gehören RM und IKS? Gehören sie organisatorisch zusammen?

Bis vor Kurzem wurde in Lehre und Praxis organisatorisch klar zwischen IKS und Risikomanagement unterschieden.

Folgt man den aktuellen Empfehlungen des «Institute of Internal Auditors (IIA)» und des «Swiss Code of Best Practice for Corporate Governance» braucht es einen neuen Ansatz.

Das IIA ordnet das IKS und RM nicht (mehr) klar einer der beiden ersten «Line of Defences» zu.

Gemäss IIA muss das Leitungsorgan (VR, Behörde) die Risikobereitschaft der Organisation bestimmen und die Aufsicht über das Risikomanagement (inkl. der internen Kontrollen) ausüben.



Das Management (GL, Verwaltung)

- errichtet und unterhält geeignete Strukturen und Prozesse für das Management des Betriebs und der Risiken (inkl. interner Kontrollen).

- entwickelt, implementiert und verbessert kontinuierlich die Risikomanagementpraktiken (inkl. interner Kontrollen) auf Prozess-, System- und Entitätsebene.

- stellt das Erreichen der Risikomanagement-Ziele sicher, wie z. B. Einhaltung von Gesetzen, Regulierungen und akzeptablem ethischem Verhalten, interne Kontrollen, Informations- und Technologiesicherheit, Nachhaltigkeit und Qualitätssicherung.

- stellt Analysen und Berichte über die Angemessenheit und Wirksamkeit des Risikomanagements (inkl. interner Kontrollen) bereit.

Da das Obligationenrecht nur die Prüfungspflicht der Existenz des internen Kontrollsystems (IKS) festhält, jedoch keine Begriffsdefinition und Mindestanforderungen an das IKS nennt, schliesst der neue «Swiss Code of Best Practice for Corporate Governance» diese Lücke.

Der Swiss Code definiert das IKS als Trilogie von Risikomanagement, Compliance-Management und Finanzüberwachung (Ziffern 26 bis 29).

Die interne Revision soll die Wirksamkeit des IKS beurteilen (Ziffer 31), und die externe Revision soll sich von Gesetzes wegen auf die Prüfung der Existenz des IKS beschränken.

> *IKS als Trilogie von Risikomanagement, Compliance-Management und Finanzüberwachung.*

Um nun die Frage zu beantworten, auf welche Governance-Stufe das Risk Management und IKS angesiedelt werden sollen, lohnt es sich die Verantwortlichkeiten des Verwaltungsrats in Erinnerung zu rufen.

- Die Überwachung der Geschäftstätigkeit des Unternehmens und die Sicherstellung, dass es im Einklang mit den geltenden Gesetzen und Vorschriften agiert.

- Die Festlegung von Strategien und Zielen für das Unternehmen sowie die Überwachung der Umsetzung dieser Strategien.

- **Die Überwachung der Finanzen des Unternehmens, einschliesslich der Aufstellung und Überwachung von Budgets und der Genehmigung von Investitionsentscheidungen.**

- **Die Sicherstellung, dass das Unternehmen über angemessene interne Kontrollen und Risikomanagementprozesse verfügt.**

- Die Überwachung der Geschäftsleitung des Unternehmens und der Entscheidungen, die von ihr getroffen werden.

Mit der Änderung des schweizerischen Aktienrechts per 01. Januar 2023 hat sich zudem die kollektive Haftungssituation des Verwaltungsrats geändert. Er ist nun auch für Fragen der operativen Zahlungsfähigkeit des Unternehmens persönlich und undelegierbar verantwortlich. Eine Missachtung dieser Pflicht kann erhebliche kollektive Haftungsrisiken begründen.

Quellen: «Wegweisende externe Prüfung» Handelszeitung 12. April 2023
«Swiss Code of Best Practices for Corporate Governance» von economiesuisse
«DAS DREI-LINIEN-MODELL DES IIA» Juli 2020

FAZIT

Ob Sie Ihr IKS als Trilogie von Risikomanagement, Compliance-Management und Finanzüberwachung definieren, oder das RM traditionell eher als strategische Funktion und IKS mehr als ein operationelle Aufgabe zur Vermeidung von Risiken sehen, für eine angemessene gute Unternehmensführung müssen alle Risk Management-Funktionen in die Nähe des obersten Leitungsorgan rücken.

Homeoffice und Risk Management

Je mehr Homeoffice desto mehr Zeit und Sorgfalt braucht es fürs Riskmanagement – durch alle Chefs auf allen Ebenen.

Seit dem Ende der Corona-Zeit ermöglichen zahlreiche Organisationen ihren Mitarbeitern eine flexiblere Arbeitsgestaltung, die eine Kombination aus Büropräsenz und Homeoffice beinhaltet. Dabei erweist sich besonders die Variante mit drei Tagen im Unternehmen und zwei Tagen im Homeoffice als bevorzugte Wahl.

Diese neue Arbeitsrealität stellt Führungskräfte jedoch vor besondere Herausforderungen. Die herkömmliche räumliche und persönliche Nähe fehlt, und das Führen auf Distanz erfordert einen erhöhten Zeitaufwand sowie eine sorgfältige Organisation.

Kommt dazu, dass wir vermutungsweise mehr Fehler machen, wenn wir von zu Hause aus, arbeiten.

Um dies zu untersuchen, wandte sich ein Forscherteam einem ungewöhnlichen empirischen Umfeld zu: dem Profischach.

Die Forscher analysierten eine Reihe von Online-Turnieren, die während der Pandemie vom amtierenden Weltmeister Magnus Carlsen organisiert wurden und die so aufgebaut waren, dass sie traditionelle Offline-Wettkämpfe widerspiegelten.
Da die meisten Teilnehmer an mindestens einem der letzten Turniere des Weltschachbundes dabei waren, konnten die Forscher die Leistungen der einzelnen Teilnehmer online und vor Ort vergleichen, indem sie die künstliche Intelligenz eines führenden Schachcomputers benutzten, um mehr als 200.000 Züge und damit verbundene Fehler zu bewerten.

Homeoffice erfordert starke Riskmanagement-Massnahmen, da die räumliche Distanz die Fehleranfälligkeit erhöhen kann.

Die Reduzierung von Kontrollen bei Homeoffice-Tätigkeiten zugunsten einer stärkeren Eigenverantwortung der Mitarbeiter kann deshalb kontraproduktiv wirken. Ob mit oder ohne Homeoffice, die Verantwortung für das Management der operationellen Risiken liegt schliesslich weiterhin in der Verantwortung der Führungsebene.

Fragen wie die Einhaltung des Vier-Augen-Prinzips, die ordnungsgemässe Abwicklung von Beschaffungen und die Auswertung von IT-Berechtigungen sowie Logfiles sind nur einige Beispiele aus einer breiten Palette von operationellen Risiken..

Es gilt zu beachten, dass diese Risiken auch im Kontext des Homeoffice bestehen bleiben und dort möglicherweise noch schwieriger zu managen sind.

Eine sorgfältige Balance zwischen Vertrauen in die Eigenverantwortung der Mitarbeiter und der notwendigen Kontrolle zur Sicherstellung der operativen Integrität ist daher entscheidend für den nachhaltigen Erfolg von Unternehmen in dieser neuen Arbeitswelt

Praxis-Tipp:
Das interne Kontrollsystem auf Excel-Tabellen mag funktionieren, wenn alle vor Ort sind. Wenn aber zwei Fünftel der Zeit von zu Hause aus gearbeitet wird, ist ein filegestütztes IKS kaum mehr wirksam und verlässlich. Überlegen Sie sich Ihre IKS-Tabellen mit einem Web-basierten Tool abzulösen. Damit erreichen Sie

•eine lückenlose Nachvollziehbarkeit der Kontrolltätigkeit
•die Sicherstellung des nahtlosen Übergangs bei Personalwechsel
•die Stärkung der Auftrags-Verbindlichkeit und -Verlässlichkeit
•den Schutz der Datenintegrität

Zudem kreieren Sie Transparenz und Ihr IKS wird zu einem echten Steuerungs- und Leitungssystem, welches die Arbeit der Chefs erleichtert.

Die grössten Risiken für Gemeinden und Städte

Ein Guide für den schnellen Einstieg in die Erarbeitung eines Risk Managements für Gemeinden und Städte

Jede Gemeinde und Stadt, die Chancen erfolgreich wahrnehmen möchte, trifft unweigerlich auf Herausforderungen und Krisen, die es zu meistern gilt.

Alle Entscheidungen und Aktivitäten sind deshalb mit Risiken verbunden, und das Risikomanagement (RM) dient dazu, die Chancen z.B. aus den Legislaturzielen selbstbewusst ergreifen zu können.

Die Einführung eines formellen Risikomanagementprozesses gelingt, wenn

1. die oberste Führungsebene ein wirksames Risikomanagement will, damit die «richtigen» Risiken eingegangen werden.
2. der Wille zur klaren Formulierung von Verantwortlichkeiten für das Risikomanagement auf allen Ebenen vorhanden ist.
3. geeignete personelle Ressourcen zur Übernahme der Rollen und Verantwortlichkeiten zur Verfügung stehen.

Der Prozess selbst umfasst fünf Schritte:

1. **Festlegen von Umfang und Kontext der Risikobeurteilung**
2. **Festlegen Risikokategorien und -kriterien**
3. **Risikoidentifikation**
4. **Risikoanalyse und -bewertung**
5. **Risikobehandlung**

> *Risk Management ist erfolgreich, wenn die Führung unterstützt, Verantwortlichkeiten klar sind und genügend Ressourcen bereitstehen.*

swissIKS®

IKS – natürlich digitalisiert.
www.iks.ch

Microsoft Partner Network

BDO SCHWEIZ Kooperation

Schritt 1: Festlegen von Umfang und Kontext der Risikobeurteilung

Der erste Schritt des Risikomanagementprozesses besteht darin, den Umfang, die Grenzen und den Kontext festzulegen. Dies gewährleistet eine bessere Nutzung von Zeit, Aufwand und Ressourcen der Organisation.

Im Kontext einer Gemeinde ist ein sinnvoller Ansatz die Legislaturziele, die Verwaltungsbereiche und (grössere) Projekte auf Risiken zu untersuchen.

Der Erarbeitungsprozess – in Anlehnung an die ISO-Norm 31000:2018 für das Risikomanagement – gliedert sich wie folgt:

Schritt 2: Festlegung der Risikokategorien und -kriterien

Risikokriterien sind eine Reihe von Regeln oder Aussagen, die eine einheitliche Entscheidungsfindung ermöglichen. Die Verwendung von Risikokriterien unterstützt eine bessere Entscheidungsfindung.

Ein zielführender Ansatz ist es, die Risikokriterien in Risikokategorien zu bündeln.

Praxiserprobt ist die Einteilung in drei Kategorien von Risiken, die jeweils einen anderen Risikomanagementansatz erfordern.

– Vermeidbare Risiken entstehen aus dem Gemeindewesen heraus und bringen keinen strategischen Nutzen. Sie sollten vermieden oder kosteneffizient beseitigt werden.

– Strategische Risiken sind Risiken, die eingegangen werden, um einen höheren strategischen Nutzen zu erzielen. Es sollten Schritte unternommen werden, um ihre Wahrscheinlichkeit und Auswirkungen kosteneffizient zu verringern.

– Externe Risiken sind unkontrollierbare Risiken. Sie erfordern besondere Prozesse, die Manager dazu ermutigen, diese Risiken offen zu diskutieren und kosteneffiziente Wege zu finden, um ihre Wahrscheinlichkeit zu verringern oder ihre Folgen abzumildern.

Aus Schritt 1 und 2 ergibt sich der Rahmen für die Identifizierung und Zuteilung der Risiken. Das Resultat kann übersichtlich in einer Matrix dargestellt werden, wobei vertikal in Risikokategorien eingeteilt und horizontal die Risiken von ihrer Herkunft her zugeteilt werden.

Risikoher-kunft / Risiko-Kategorien	Legis-latur-ziele	Verwal-tungs-bereiche	Pro-jekte
Vermeid-bare Risiken			
Stra-tegische Risiken			
Externe Risiken			

Schritt 3: Risikoidentifikation

Für eine schnelle Erarbeitung eines Risk Managements lohnt es sich mit Vorgabedokumenten zu arbeiten. Die Vorgabedokumente illustrieren mögliche Risiken pro Risikoherkunftsbereich. Dies erleichtert den Sachexperten den Einstieg ins Thema und löst Assozationsketteneffekte aus, welche eine Risikoidentifikation effizient und effektiv vorantreiben.

Eine Liste mit möglichen Risiken für Legislaturziele, Verwaltungsbereiche und Projekte stellen wir Ihnen gerne zu (Mail an christian.hafner@swissaxis.ch)

Schritt 4: Risikoanalyse und -bewertung

Ein Risiko zu analysieren bedeutet, das Risiko zu verstehen und ist die Grundlage für die Bewertung.

Eine eigentliche Bewertung ist nur für die strategischen und externen Risiken notwendig, denn die vermeidbaren Risiken können/sollen vermieden oder kosteneffizient beseitigt werden.

Die Vermeidung der Risiken kann mittels internem Kontrollsystem (IKS) erfolgen.

Vorgehen: In einem Bottom-up-Ansatz die Prozesse nach vermeidbaren Risiken durchkämmen und die «Schlüssel-Checks» zur Vermeidung/Beseitigung der Prozessrisiken als Kontrollen in ein dynamisches IKS einpflegen.

Für jedes zu bewertende Risiko muss entschieden werden,

-wer bewertet (interne, externe Experten und wie viele) und
-wie oft soll bewertet werden.

Die Bewertung selbst erfolgt nach einem einheitliche Raster für Eintretenswahrscheinlichkeit, Schadenhöhe und Einfluss auf die Reputation.

Je grösser die Anzahl der Bewerter und je öfter bewertet wird, desto notwendiger wird eine Dynamisierung des RM-Prozesse.

Das Resultat der Bewertung(en) erhält der sog. Risk Owner und sein Stellvertreter.

Schritt 5: Risikobehandlung

Die Behandlung strategischer und externer Risiken erfordert einen umfassenden Ansatz, der sowohl präventive als auch reaktive Massnahmen umfasst.
Es ist in der Verantwortung der Risk Owner, dass zeitgerechte angemessene Massnahmen ergriffen werden.

Organisatorisch ist festzulegen, wer über die Durchführung der Massnahmen entscheidet. Meistens ist es sinnvoll, die Entscheide gemeinsam als Leitungsorgan zu fällen, da Kosten und Nutzen oft in mehreren Bereichen anfallen.

Es versteht sich von selbst, dass die Umsetzung der Massnahmen, resp. deren Ergebnis ebenfalls überwacht werden muss – am sinnvollsten als Teil desselben dynamischen RM-Prozesses wie für die Risikobewertung.

FAZIT

Es besteht ein signifikanter Zusammenhang zwischen langfristigem Erfolg und dem bewussten Umgang mit Risiken.

Die Integration von Risiko und Strategie ermöglicht es den Behörden, die besten Chancen auszuwählen und relevante Risiken zu managen.

Das Risiko «Menschliche Schwäche»

Mehr als zwei Drittel der Schäden durch Betrugsfälle in Unternehmen werden von eigenen Mitarbeitern verursacht.

Typische interne Täter sind in der Regel gut gebildet, zwischen 40 und Mitte 50 Jahre alt, in leitenden Positionen im Finanzbereich tätig und arbeiten seit mindestens zehn Jahren im Unternehmen.

Durch ihre lange Betriebszugehörigkeit geniessen sie hohes Vertrauen und kennen die Schwachstellen in den Kontrollsystemen. Obwohl sie selten zuschlagen, verursachen sie oft erhebliche Schäden.

Menschliche Schwächen

Die Täter sind selten Robin Hoods. Die Motive für interne Betrügereien reichen von

- Spielsucht über Habgier,
- luxuriösen Lebensstil und finanzielle Notlagen bis hin zu
- Geltungssucht, mangelnder Wertschätzung, Rache und persönlichem Vorteil.

Die meisten dieser menschlichen Schwächen sind im Charakter angelegt.

Deshalb hat die Personalauswahl bei der Verhinderung von Betrug eine (leider oft unterschätzte) hohe Bedeutung. Die Charaktereigenschaften insbesondere von Führungskräften sollten bei der Einstellung sorgfältig geprüft werden.

> *Langjährige Führungskräfte verursachen durch ihre Schwächen häufig schwere Reputationsschäden.*

Finanzieller Schaden vs. Reputationsschaden

Oft ist der finanzielle Schaden für ein Unternehmen verkraftbar. Wenn aber ein Unternehmen einen Schaden an seinem Ruf erleidet, kann es mit erstaunlicher Geschwindigkeit zusammenbrechen. Mit den Worten von Benjamin Franklin: «Es braucht viele gute Taten, um einen guten Ruf aufzubauen, und nur eine schlechte, um ihn zu verlieren.»

swissRM™
Risk Management - natürlich digital
www.swissrm.ch

Microsoft Partner Network
BDO SCHWEIZ Kooperation

Bei Aufdeckung eines Fehlverhaltens empfiehlt sich deshalb, als allererstes das Management des Risikos, das sich aus einer möglichen Beschädigung des Rufes des Unternehmens infolge einer negativen Wahrnehmung in der Öffentlichkeit (z.B. bei Kunden, Geschäftspartnern, Aktionären, Behörden) an die Hand zu nehmen.

Kontrollsysteme vs. Kultur

Um schwarze Schafe im Unternehmen zu verhindern, sind Massnahmen wie regelmässige Kontrollen und Audits leider unzureichend.

Nützlich sind eine vertrauensvolle Unternehmenskultur und offene Fehlerkommunikation. Die für die Prävention von internen Wirtschaftsstraftaten wichtigste Massnahme ist aber gleichzeitig die verpönteste.

Whistleblowing

Whistleblowing führt am häufigsten zur Entdeckung von «Innentätern», da diese ihre kriminellen Handlungen fortsetzen, solange sie unentdeckt bleiben.

Organisationen mit funktionierendem Meldesystem decken bis zu 80% der Missstände durch Whistleblower auf. Ganz wichtig zu wissen: 55 % der Hinweisgeber sind Mitarbeiter.

Hinweisgebersystem funktionieren aber nur, wenn der hinweisgebende Mitarbeiter sicher ist, dass er seine Stelle nicht verliert. Es ist deshalb entscheidend, für den Schutz von Hinweisgebern zu sorgen.

Die Bedeutung von Hinweisgebern wurde bereits 2007 von der Eidgenössischen Finanzkontrolle betont. Der Whistleblowing Report 2021 der Fachhochschule Graubünden bestätigt, dass ein funktionierendes Meldesystem entscheidend ist.

In der Schweiz waren 32,5% der Unternehmen im Jahr 2020 von illegalem und unethischem Verhalten betroffen. 27,6% der befragten Unternehmen konnten dank einer Meldestelle über 80% des finanziellen Gesamtschadens aufdecken.

Reputationsschäden sind gravierender als finanzielle Verluste, daher sind Whistleblowing und eine offene Firmenkultur entscheidend.

Petzer und Nestbeschmutzer

Jede Organisation, die ernsthaft Risikomanagement betreiben möchte, sollte eine Meldestelle und einen Prozess für Hinweisgeber implementieren. Der Prozess sollte es den Mitarbeitern ermöglichen, anonym und ohne Verletzung der Treuepflicht gegenüber dem Arbeitgeber ihr Wissen weiterzugeben.

Der Hinweisgeber darf nicht befürchten müssen, als Nestbeschmutzer stigmatisiert zu werden

Im Gegenteil, ein gut in die Unternehmenskultur eingebettetes Meldesystem unterstützt die Zivilcourage der Hinweisgeber.

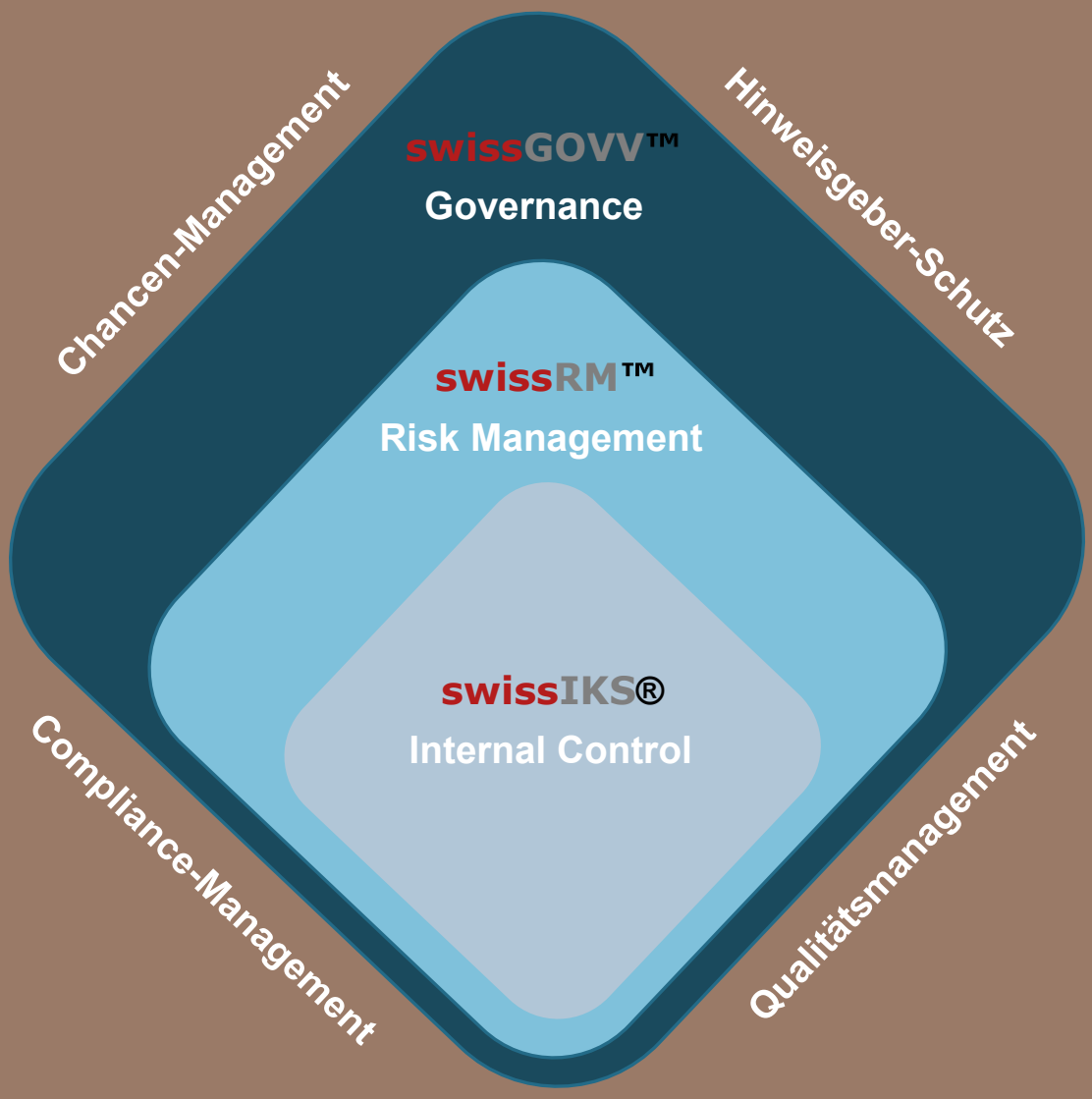
Wenn sich die Mitarbeiter allerdings nicht sicher fühlen und befürchten, als Petzer gebrandmarkt zu werden und sogar die Stelle zu verlieren, wird die Meldequote tief bleiben. Meldesysteme, die funktionieren verzeichnen pro Jahr 10 Meldungen auf 1000 Mitarbeiter, wobei nur jede zweite Meldung zur Aufdeckung eines Fehlverhaltens führt.

Quellen:
«Der Faktor Mensch: Beobachtungen aus der Sicht eines Forensic-Dienstleisters» Vortrag von Matthias Kiener, Leiter Forensic Services, Mazars SA anlässlich der Risk Management & IKS-Konferenz vom 16. November 2023
„Nicht Petzer, sondern Diener des Arbeitgebers“ NZZ am Sonntag, 20.02.2022
„Mehr Schutz für Whistleblower“ Börsen-Zeitung, 28.03.2022
„Whistleblowing mit abschreckender Wirkung“ Max-Plack-Gesellschaft, 21.02.2022
„Whistleblowing Report 2021» Fachhochschule Graubünden, Oktober 2021
„Kriminellen Mitarbeitern auf der Spur“ Springer Professional, 07.02.2023
«When Hiring CEOs, Focus on Character» HBR, Aiyesha Dey, Juli-August 2022
„Das Risiko von Fehlverhalten und Betrug in Unternehmen wächst“ Handelsblatt, 22.05.2023
«Wenn das Risikomanagement versagt – Blogbeitrag» Netzwerk Risikomanagement, 30.07.2023
«Reputation and Its Risks» von Robert G. Eccles et al., Harvard Business Review, Februar 2007

FAZIT

Die wichtigsten Massnahmen, um Betrug vorzubeugen sind Hintergrundprüfungen, klare Verhaltensregeln, interne Kontrollen und die Förderung von Transparenz. Unternehmen können durch implementierte Massnahmen dazu beitragen, eine integre und ethische Umgebung zu schaffen.

Einfache sofort wirksame organisatorische Massnahmen sind Stellvertretereinsatz und Aufgabenrotation. Ein schwarzes Schaf wird haufenweise «gute» Gründe vorbringen, warum er unersetzlich ist, und gleichzeitig das Zeichen, eine diskrete Untersuchung einzuleiten. Da menschliche Schwächen die Wurzel von Betrug sind, ist ein empathisches Interesse der Vorgesetzten am Verhalten der Mitarbeiter entscheidend, um das Risiko zu minimieren. **Aufmerksame Vorgesetzte spüren, wenn sich Mitarbeiter in Situationen manövrieren und das Schlechte in ihrem Charakter die Oberhand gewinnt.** Ohne Garantien für den Schutz von Hinweisgebern gibt es kein effizientes Frühwarnsystem, um Innentäter-Risiken rechtzeitig zu erkennen und Sanktionen, Strafzahlungen und Reputationsschäden zu vermeiden!



Risk Management und IKS – Die Essenz

swissaxis