iboWebCON

Das Interne Kontrollsystem und das Drei-Linien-Modell des DIIR

Wie passt das zusammen?

Online, 15.September 2021

Joachim Sell

Zur Person

Name:	Joachim Sell
Firma:	SellfControl – Unternehmensberatung Joachim Sell
Funktion:	Unternehmer. Inhaber.

Projekte, Aufgaben und Lösungen:

- Prozessmanagement – mehr als 30 Jahre
- Interne Risiko- und Kontrollsysteme – mehr als 17 Jahre
- Internal Audit / Revision – mehr als 15 Jahre

Meine Leidenschaft:

Als Spezialist für interne Kontrollsysteme unterstütze ich Sie bei der Bewertung, Anpassung und Implementierung von ganzheitlichen Managementsystemen. Meine Prüfungserfahrung als Revisor und Auditor nutze ich, um Risiken zu erkennen und mit innovativen Lösungsansätzen zum Kontrollmanagement ordnungsmäßige, sichere und wirtschaftliche Abläufe sicher zu stellen. Als Prüfer, Berater und als Dozent.

SellfControl
Revision · Beratung · Seminare

iboWebCON

Agenda

- Das Drei-Linien-Modell des DIIR – Die Grundsätze
- Das Drei-Linien-Modell des DIIR – Die Rollen
- Das Interne Kontrollsystem im Detail – Der Prozess
- Das Interne Kontrollsystem im Detail – Das Risiko
- Das Interne Kontrollsystem im Detail – Die Kontrolle
- Das Interne Kontrollsystem in der Gesamtansicht
- Die Risiko-Kontroll-Matrix
- Zusammenfassung / Fazit
- Fragen

Das Drei-Linien-Modell des DIIR – Die Grundsätze

6 Grundsätze (Auszug)

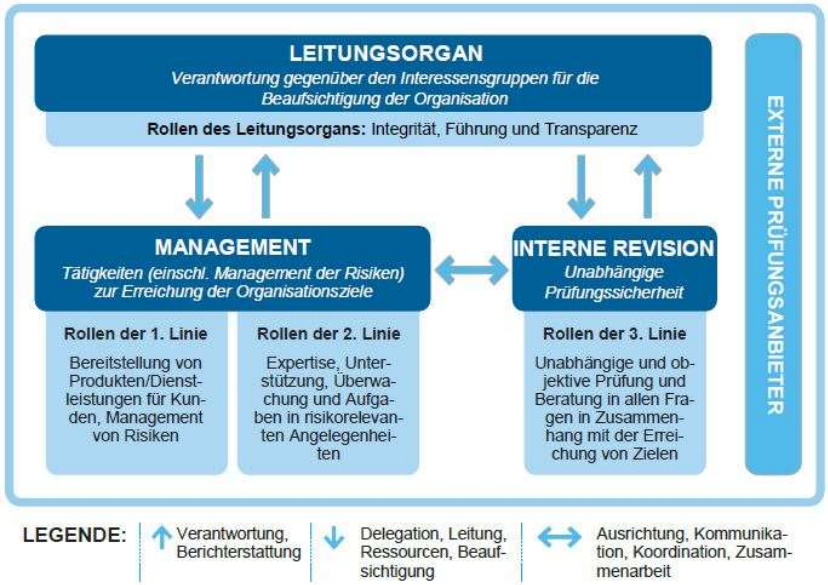
Das Drei-Linien-Modell hilft Organisationen, Strukturen und Prozesse zu identifizieren, die die Zielerreichung am besten unterstützen und eine starke Governance und ein starkes Risikomanagement ermöglichen. Das Modell ist für alle Organisation anwendbar…

- **Grundsatz 1: Governance**

  Die Governance einer Organisation erfordert angemessene Strukturen und Prozesse für die Verantwortung eines Leitungsorgans…, Tätigkeiten des Managaments…, Prüfungssicherheit und Beratung…

- **Grundsatz 2: Rollen des Leitungsorgans**
  - Das Leitungsorgan stellt angemessene Strukturen und Prozesse sicher.
  - Anpassung der Organisationsziele und -aktivitäten an die Ziele der Interessengruppen
  - Delegiert Verantwortung und stellt dem Management Ressourcen zur Verfügung, ..( )… und gleichzeitig sicherzustellen, dass rechtliche, regulatorische und ethische Erwartungen erfüllt werden.
- **Grundsatz 3: Management und Rollen der ersten und zweiten Linie**
  - Die Rollen der ersten Linie sind hauptsächlich mit der Lieferung von Produkten und/oder Dienstleistungen an Kunden der Organisation verbunden, einschließlich Unterstützungsfunktionen.
  - Die Rollen der zweiten Linie liefern Unterstützung beim Management von Risiken.
  - Die Rollen der ersten und zweiten Linie können miteinander verwoben oder separiert sein.
  - Manche Rollen der zweiten Linie können Spezialisten zugeordnet sein, die ergänzende Expertise, Unterstützung, Überwachung und Anforderungen für jene mit Rollen der ersten Linie liefern.
  - …die Verantwortung für das Management der Risiken ist Teil der Aufgaben der ersten und zweiten Linie und des Managements.
- **Grundsatz4: Rollen der dritten Linie**
  - Die Interne Revision bietet unabhängige und objektive Prüfungssicherheit und Beratung in Bezug auf die Angemessenheit und Wirksamkeit der Governance und des Risikomanagements.
  - Sie berichtet ihre Erkenntnisse dem Management und dem Leitungsorgan, um kontinuierliche Verbesserun-gen zu fördern. Dabei kann sie die von anderen internen und externen Anbietern erbrachten Prüfungsleistungen berücksichtigen.
- **Grundsatz 5: Unabhängigkeit der dritten Linie**
  - Die Unabhängigkeit der Internen Revision von den Verantwortlichkeiten des Managements ist von kriti-scher Bedeutung für ihre Objektivität, Autorität und Glaubwürdigkeit.
- **Grundsatz 6: Wertschöpfung und Schutz von Werten**
  - Alle Rollen, die zusammenarbeiten, tragen gemeinsam zur Wertschöpfung und zum Schutz von Werten bei, wenn sie miteinander und mit den vorrangigen Interessen der Interessengruppen in Einklang gebracht werden.

Das IIA Drei- Linien-Modell



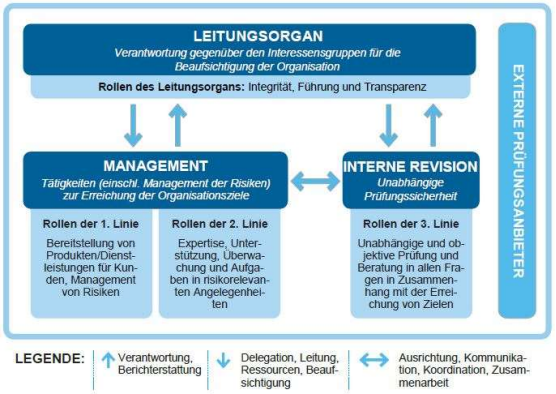
https://www.diir.de/fileadmin/fachwissen/downloads/Three-Lines-Model-Updated-German.PDF

Das Drei-Linien-Modell des DIIR – Die Rollen

Das Leitungsorgan

- Akzeptiert die Rechenschaftspflicht gegenüber den Interessengruppen für die Aufsicht über die Organisation.
- Arbeitet mit den Interessengruppen zusammen, um ihre Interessen zu überwachen und transparent über die Erreichung der Ziele zu kommunizieren.
- Pflegt eine Kultur, die ethisches Verhalten und Rechenschaftspflicht fördert.
- Richtet Strukturen und Prozesse für die Governance ein, einschließlich von Unterausschüssen, falls erforderlich.
- Delegiert Verantwortung und stellt dem Management Ressourcen zur Verfügung, um die Ziele der Organisation zu erreichen.
- Bestimmt die Risikobereitschaft der Organisation und übt die Aufsicht über das Risikomanagement (einschließlich der internen Kontrollen) aus.
- Beaufsichtigt die Einhaltung rechtlicher, regulatorischer und ethischer Erwartungen.
- Errichtet und beaufsichtigt eine unabhängige, objektive und kompetente interne Revisionsfunktion

Das IIA Drei- Linien-Modell



Rollen der ersten Linie

- Leitet und lenkt die Tätigkeiten (einschließlich des Managements von Risiken) und den Einsatz von Ressourcen, um die Ziele der Organisation zu erreichen.
- Unterhält einen ständigen Dialog mit dem Leitungsorgan und berichtet über geplante, tatsächliche und erwartete Ergebnisse im Zusammenhang mit den Zielen der Organisation sowie über Risiken.
- Errichtet und unterhält geeignete Strukturen und Prozesse für das Management des Betriebs und der Risiken (einschließlich interner Kontrollen).

Rollen der zweiten Linie

- Bietet ergänzende Fachkenntnisse, Unterstützung, Überwachung und Aufgaben im Zusammen-hang mit dem Risikomanagement, einschließlich
  - Entwicklung, Implementierung und kontinuierliche Verbesserung von Risikomanagementpraktiken (einschließlich interner Kontrollen) auf Prozess-, System- und Entitäts-ebene.
  - Erreichung von Risikomanagement-Zielen, wie z. B. Einhaltung von Gesetzen, Regulierungen und akzeptablem ethischem Verhalten, interne Kontrollen, Informations- und Technologiesicherheit, Nachhaltigkeit und Qualitätssicherung.
- Bereitstellung von Analysen und Berichten über die Angemessenheit und Wirksamkeit des Risikomanagements (einschließlich interner Kontrollen).

Rollen der dritten Linie

Interne Revision

- Bewahrt die primäre Rechenschaftspflicht gegenüber dem Leitungsorgan und die Unabhängigkeit von den Verantwortlichkeiten des Managements.
- Vermittelt dem Management und dem Leitungsorgan unabhängige und objektive Prüfungssicherheit und Beratung hinsichtlich der Angemessenheit und Wirksamkeit der Governance und des Risikomanagements (einschließlich interner Kontrollen), um die Erreichung der Organisationsziele zu unterstützen und kontinuierliche Verbesserungen zu fördern.
- Meldet dem Leitungsorgan Beeinträchtigungen der Unabhängigkeit und Objektivität und setzt bei Bedarf Schutzvorkehrungen um.

Externe Prüfungsdienstleister

- Bieten zusätzliche Prüfungssicherheit zur
  - Erfüllung gesetzlicher und regulatorischer Erwartungen, die dem Schutz der Interessen der Interessengruppen dienen.
  - Erfüllung von Wünschen des Managements und des Leitungsorgans zur Ergänzung interner Quellen von Prüfungssicherheit.

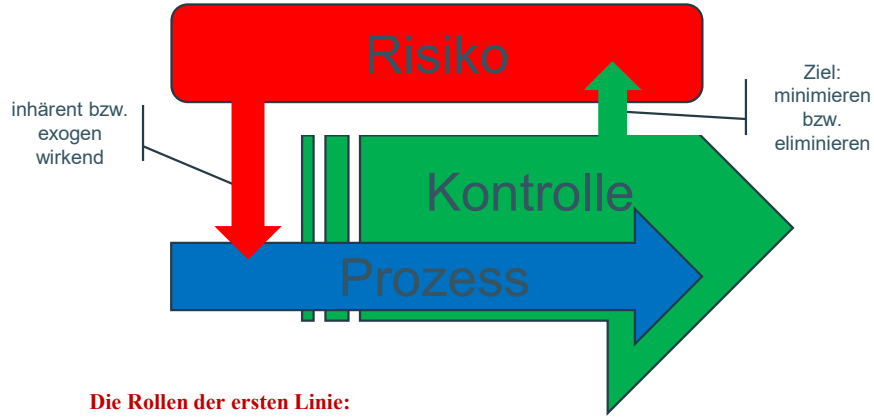
https://www.diir.de/fileadmin/fachwissen/downloads/Three-Lines-Model-Updated-German.PDF

Das Interne Kontrollsystem im Detail – Der Prozess

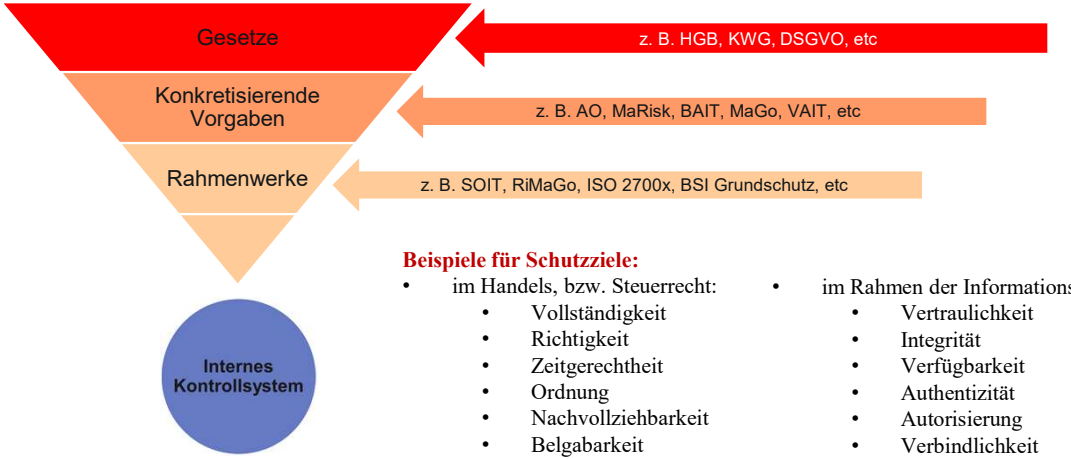
Prozess

Prozessinhalte:
- Waren
- Dienstleistungen
- Produktionsmaterial
- Informationen
- buchalterische Daten
- Etc.

Schutzobjekte:
- Anwendungen/Software
- Systeme/ Hardware
- Infrastruktur
- Hauptbuchkonten
- Personenbezogene Daten
- Etc.



Gesetzliche und aufsichtliche Anforderungen generieren Schutzziele:



Beispiele für Schutzziele:
- im Handels, bzw. Steuerrecht:
  - Vollständigkeit
  - Richtigkeit
  - Zeitgerechtheit
  - Ordnung
  - Nachvollziehbarkeit
  - Belgabarkeit
  - Unveränderlichkeit
- im Rahmen der Informationssicherheit:
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Authentizität
  - Autorisierung
  - Verbindlichkeit

Die Rollen der ersten Linie:
- …führen die eigentlichen Prozessabläufe durch
- …sind verantwortlich für den Betrieb und die Unterhaltung der Schutzobjekte
- …sie beachten die gesetzlichen und aufsichtlichen Anforderungen
- …führen Kontrollhandlungen durch

Die Rollen der zweiten Linie:
- …stellen die Aufbauorganisation für die Prozessdurchführung zur Verfügung
- …identifizieren Schutzobjekte
- …identifizieren gesetzliche und aufsichtliche Anforderungen

Die Rollen der dritten Linie:
- …prüfen die Prozessabläufe auf Wirtschaftlichkeit

Das IIA Drei- Linien-Modell

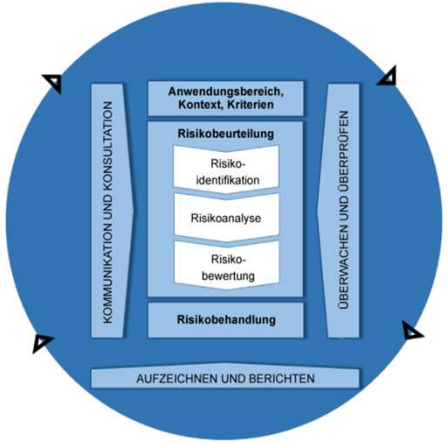
Das Interne Kontrollsystem im Detail – Das Risiko

Risiko

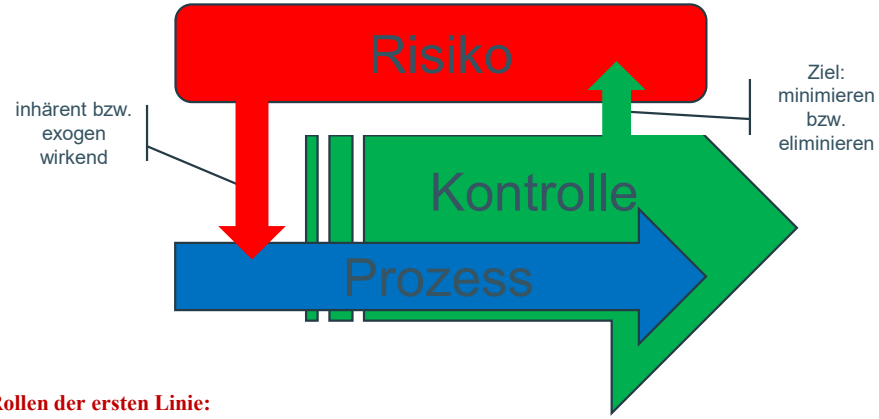
Typische Risiken:
- Strategische Risiken
  - Regulatorische Risiken
  - Wettbewerbsrisiko
  - Versicherungstechnisches Risiko
- Operative Risiken
  - Betriebsrisiko
  - Haftungsrisiko
  - Vermögensrisiko
- Projektrisiken
  - Budget
  - Qualität
  - Termin
- Etc.

Risikobehandlung:
- Vermeiden
- Reduzieren
- Transferieren
- Akzeptieren

Methoden:
- …müssen im Unternehmen etabliert sein
- …müssen dokumentiert sein
- …z. B. DIN EN 31000

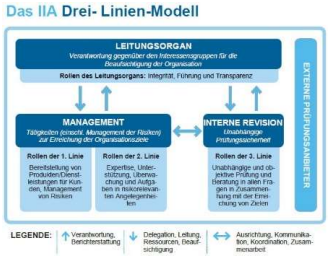


Risikomanagementprozess nach DIN EN 31000



Die Rollen der ersten Linie:
- … managen Risiken in Zusammenarbeit mit den Rollen der zweiten Linie
- …errichten und unterhalten geeignete Strukturen zur Kommunikation von Risikobetrachtungen

Die Rollen der zweiten Linie:
- …stellen Methoden zur Identifizierung und Steuerung von Risiken auf allen Ebenen zur Verfügung
- …identifizieren, analysieren und bewerten Risiken
- …entwickeln das Risikomanagementsystem weiter
- …analysieren und berichten über die Angemessenheit und Wirksamkeit des Risikomanagementsystems

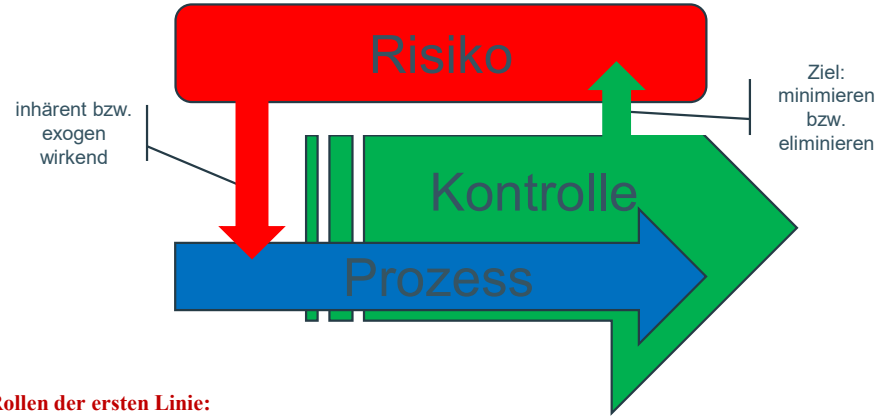


Die Rollen der dritten Linie:
- …prüfen die die Angemessenheit; die Wirksamkeit und die Wirtschaftlichkeit des Risikomanagementsystems
- …stellen ihre Unabhängigkeit sicher

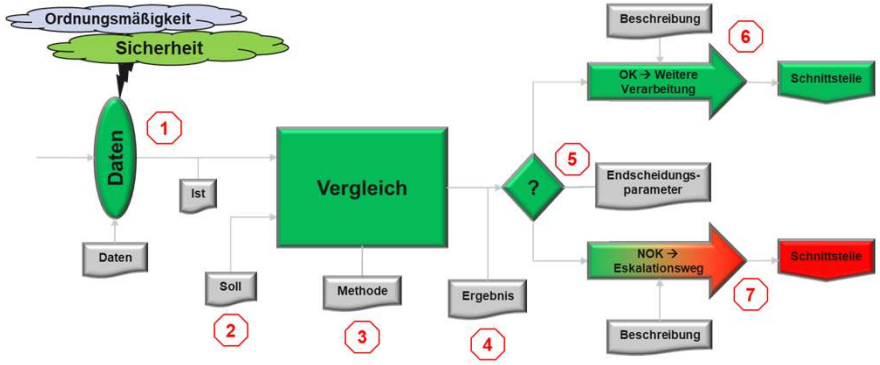
Das Interne Kontrollsystem im Detail – Die Kontrolle

Kontrollinhalte:
- dokumentierte Kontrollziele
- Beschreibung der Kontrollaktivität
- Nachvollziehbarkeit der Kontrollhandlung
- Kontrollverantwortlicher
- Frequenz der Durchführung
- Kontrollcharakter
- Kontrolltyp
- Etc.

Beispielhafte Schutzziele:
- Ordnungsmäßigkeit
  - Vollständigkeit
  - Richtigkeit
  - Zeitgerechtheit
  - Ordnung
  - Nachvollziehbarkeit
  - Belegabarkeit
  - Unveränderlichkeit
- IT-Sicherheit
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Authentizität
  - Autorisierung
  - Verbindlichkeit



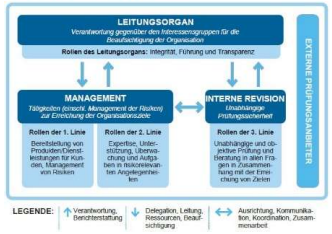
Die sieben Bestandteile der 7735-Kontrolle



Die Rollen der ersten Linie:
- … führen Kontrollhandlungen durch
- …werten Ergebnisse aus
- …kommunizieren Ergebnisse

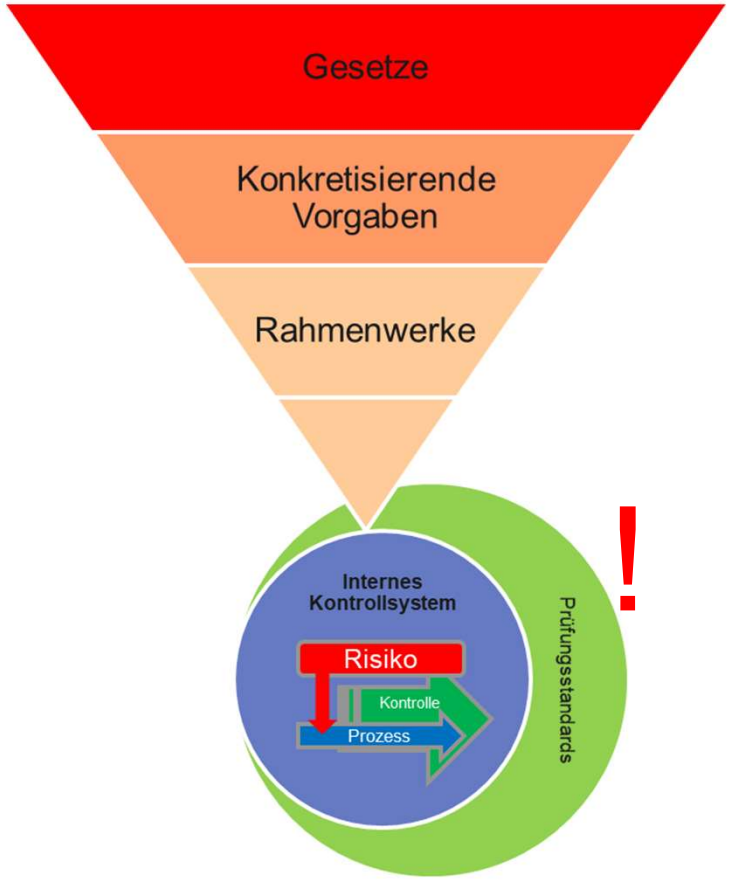
Die Rollen der zweiten Linie:
- …entwickeln Kontrollen zur Minimierung, bzw. Eliminierung von Risiken
- …definieren Handlungsspielräume
- …analysieren , verbessern und berichten über die Angemessenheit und Wirksamkeit der Kontrollhandlungen

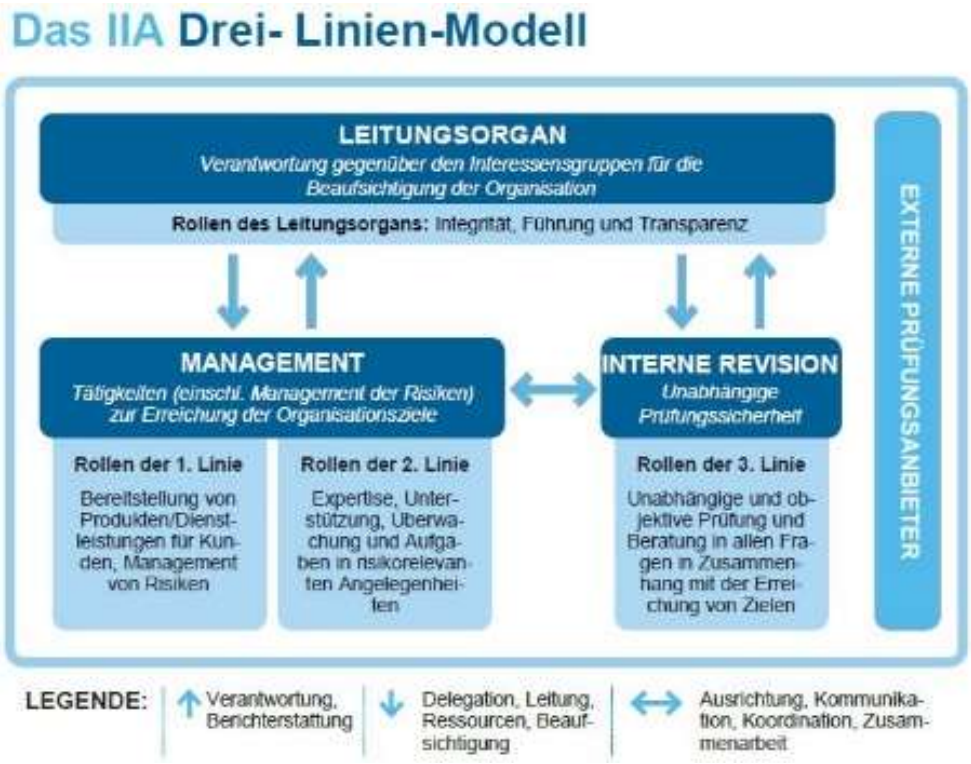
Das IIA Drei- Linien-Modell



Die Rollen der dritten Linie:
- …prüfen die die Angemessenheit; die Wirksamkeit und die Wirtschaftlichkeit der Kontrollen
- …stellen ihre Unabhängigkeit sicher

Das Interne Kontrollsystem in der Gesamtansicht





SellfControl
Revision · Beratung · Seminare

iboWebCON

Die Risiko-Kontroll-Matrix

Gesamtansicht

Risiko-Kontroll-Matrix

Prozess: Muster

SellfControl Revision · Beratung · Seminare

Stand: 01.09.2021

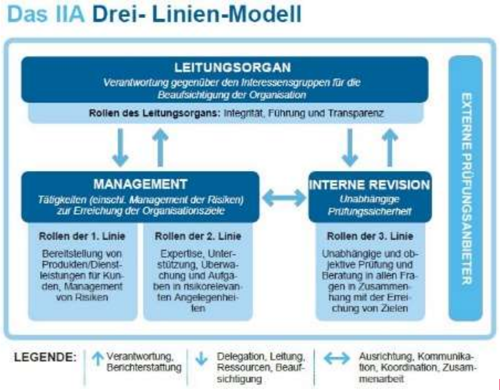
																								Sicherstellung der Ordnungsmäßigkeit						Sicherstellung der (IT-) Sicherheit						Strategische Risiken											
Hauptbuchkonto	Prozessbezeichnung	Risiko-Nr.	Risikobeschreibung	Risikoklasse	Score inhärent	Score residual	Ursache	Auswirkung	Rsikostrategie	Begründung	Eintrittswahrscheinlichkeit	mögliche Schadenhöhe	Schlüsselrisiko	Risikobewertung	Kontroll-ID	Ziel der Kontrolle	Kontrollaktivität Beschreibung	Nachweis der Kontrollhandlung	Kontrolle implementiert?	Kontroll-verantwortlicher	Frquenz der Kontrolldurchführung	Kontroll-charakter	Manuell / IT	Vollständigkeit	Richtigkeit	Zeitgerechtheit	Ordnung der Buchungen	Nachvollziehbarkeit	Unveränderlichkeit	Vertraulichkeit	Integrität von IT-Systemen	Verfügbarkeit der Daten	Autorisierung	Authentizität	Verbindlichkeit	Adressenausfallrisiko	Marktpreisrisiko	Liquiditätsrisiko	Operationelles Risiko	Datenschutzanforderung	Aufbewahrungspflichten	Betrug	Geldwäsche	Compliance	etc.	Festgestellt Kontrollschwäche	Bemerkungen

Die Risiko-Kontroll-Matrix beschreibt

- …die Zusammenhänge von
  - Prozessen,
  - Risiken,
  - Kontrollen und
  - Schutzobjekten
- …in einer Tabelle pro Prozess die zugehörigen Risiken mit den zugeordneten Kontrollen
- …die Charakteristika der einzelnen Kontrollen
- …die Kontrollhandlungen zu jeder Kontrolle
- …die Verantwortlichkeiten für jeden Prozess und jede Kontrolle
- …die Zuordnung der Risiken und Kontrollen zu dem jeweiligen Schutzobjekt
- …die Kontrollhandlungen, die Ergebnisse und dokumentiert die Zuordnung zu den Bewertungskriterien (Ordnungsmäßigkeit und Sicherheit)
- …mögliche Kennzahlen

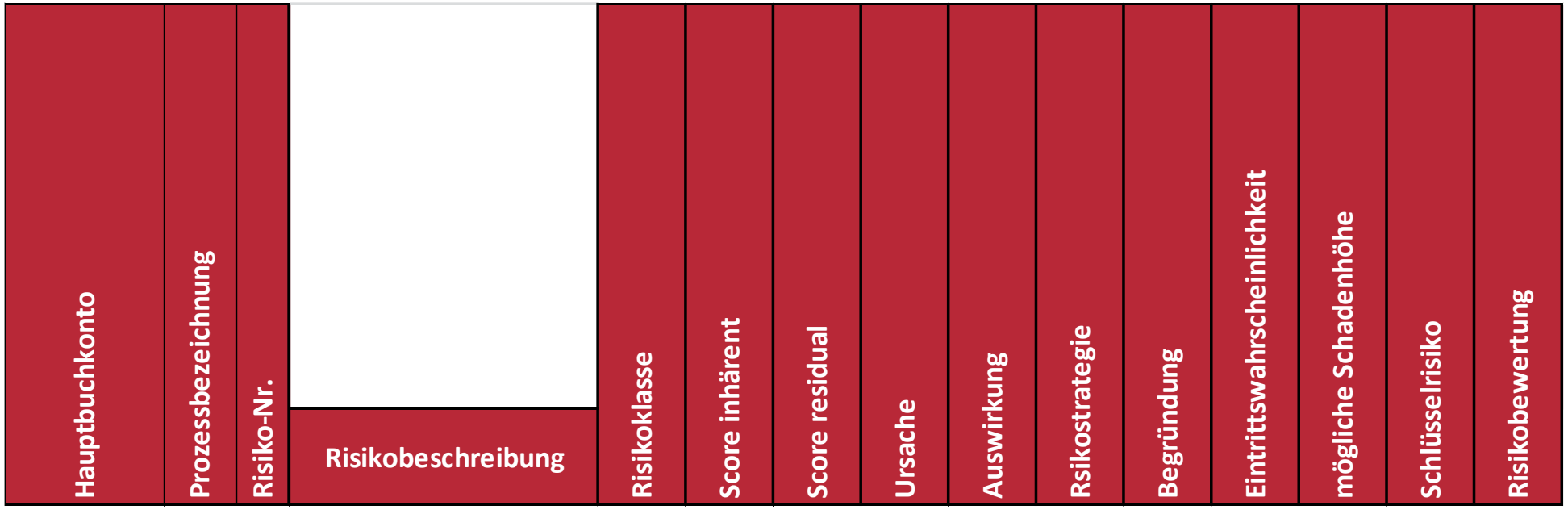
Folgende Rollen sind an der Entwicklung, Pflege und Umsetzung der, in der RKM beschriebenen Inhalte beteiligt:

- Die Rollen des Leitungsorgans,
- die Rollen der ersten Linie,
- die Rollen der zweiten Linie,
- die Rollen der dritten Linie
  - Interne Revision
  - Externe Prüfungsdienstleister



Die Risiko-Kontroll-Matrix

Schutzobjekt und Risikobeschreibung



Die Risiko-Kontroll-Matrix

Kontrollbeschreibung

Kontroll-ID.	Ziel der Kontrolle	Kontrollaktivität Beschreibung	Nachweis der Kontrollhandlung	Kontrolle implementier?	Kontroll-verantwortlicher	Frquenz der Kontrolldurchführung	Kontroll-charakter	Manuell / IT

Die Risiko-Kontroll-Matrix

Schutzziele

Sicherstellung der Ordnungsmäßigkeit						Sicherstellung der (IT-) Sicherheit						Strategische Risiken								
Vollständigkeit	Richtigkeit	Zeitgerechtheit	Ordnung der Buchungen	Nachvollziehbarkeit	Unveränderlichkeit	Vertraulichkeit	Integrität von IT-Systemen	Verfügbarkeit der Daten	Autorisierung	Authemtizität	Verbindlichkeit	Adressenausfallrisiko	Marktpreisrisiko	Liquiditätsrisiko	Operationelles Risiko	Verfahrensdokumentation	Aufbewahrungspflichten	Betrug	Geldwäsche	Compliance

Zusammenfassung / Fazit

Prozess

Die Rollen des Leitungsorgans:
- …stellen Strukturen und Prozesse zum Prozessmanagement zur Verfügung
- …sorgt für die Zielerreichung der Interessengruppen
- …delegiert Verantwortungen zur Umsetzung des Prozessmanagements

Die Rollen der ersten Linie:
- …führen die eigentlichen Prozessabläufe durch
- …sind verantwortlich für den Betrieb und die Unterhaltung der Schutzobjekte
- …sie beachten die gesetzlichen und aufsichtlichen Anforderungen
- …führen Kontrollhandlungen durch

Die Rollen der zweiten Linie:
- …stellen die Aufbauorganisation für die Prozessdurchführung zur Verfügung
- …identifizieren Schutzobjekte
- …identifizieren gesetzliche und aufsichtliche Anforderungen

Die Rollen der dritten Linie:
- …prüfen die Prozessabläufe auf Wirtschaftlichkeit

Risiko

Die Rollen des Leitungsorgans:
- …stellen Strukturen und Prozesse zum Risikomanagement zur Verfügung
- …sorgt für die Zielerreichung der Interessengruppen
- …delegiert Verantwortungen zur Umsetzung des Risikomanagements

Die Rollen der ersten Linie:
- … managen Risiken in Zusammenarbeit mit den Rollen der zweiten Linie
- …errichten und unterhalten geeignete Strukturen zur Kommunikation von Risikobetrachtungen

Die Rollen der zweiten Linie:
- …stellen Methoden zur Identifizierung und Steuerung von Risiken auf allen Ebenen zur Verfügung
- …identifizieren, analysieren und bewerten Risiken
- …entwickeln das Risikomanagementsystem weiter
- …analysieren und berichten über die Angemessenheit und Wirksamkeit des Risikomanagementsystems

Die Rollen der dritten Linie:
- …prüfen die die Angemessenheit; die Wirksamkeit und die Wirtschaftlichkeit des Risikomanagementsystems
- …stellen ihre Unabhängigkeit sicher

Kontrolle

Die Rollen des Leitungsorgans:
- …stellen Strukturen und Prozesse zum Kontrollmanagement zur Verfügung
- …sorgt für die Zielerreichung der Interessengruppen
- …delegiert Verantwortungen zur Umsetzung des Kontrollmanagements

Die Rollen der ersten Linie:
- … führen Kontrollhandlungen durch
- …werten Ergebnisse aus
- …kommunizieren Ergebnisse

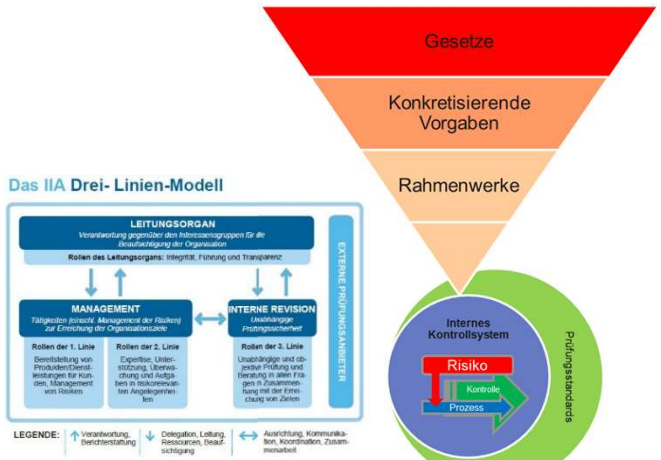
Die Rollen der zweiten Linie:
- …entwickeln Kontrollen zur Minimierung, bzw. Eliminierung von Risiken
- …definieren Handlungsspielräume
- …analysieren , verbessern und berichten über die Angemessenheit und Wirksamkeit der Kontrollhandlungen

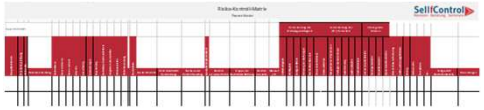
Die Rollen der dritten Linie:
- …prüfen die die Angemessenheit; die Wirksamkeit und die Wirtschaftlichkeit der Kontrollen
- …stellen ihre Unabhängigkeit sicher

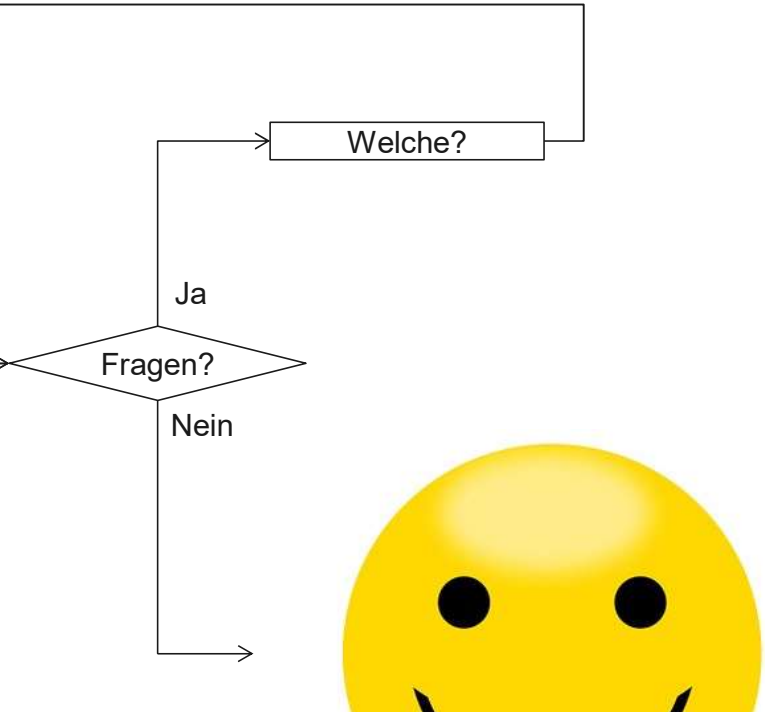
Das Drei-Linien-Modell des DIIR beschreibt in angemessener Form die grundsätzlichen organisatorischen Anforderungen zur Umsetzung eines wirksamen IKS. Es stellt für den Prüfer eine geeignete Grundlage zur Vorbereitung einer Prüfung des IKS um die Ordnungsmäßigkeit, die Angemessenheit und die Wirtschaftlichkeit des IKS bewerten zu können.

Todo‘s: Checkliste entwickeln…

Alles klar?







Lust auf mehr?

Seminarinhalt
Prüfen des internen Kontrollsystems

Grundlagen

Schutzobjekte, Gesetzliche Anforderungen

IKS – Konkretisierende Verordnungen

GoBD, IDW RS FAIT 1-5, MaRisk,
ISO 27000, ISO 31000

IKS – Rahmenwerke

Cobit 5, BSI-Standards, BSI-Grundschutz,
Sicherer IT-Betrieb (SITB), SOIT, COSO ERM,
COSO 2013 (IKS)

IKS – Prüfungsstandards

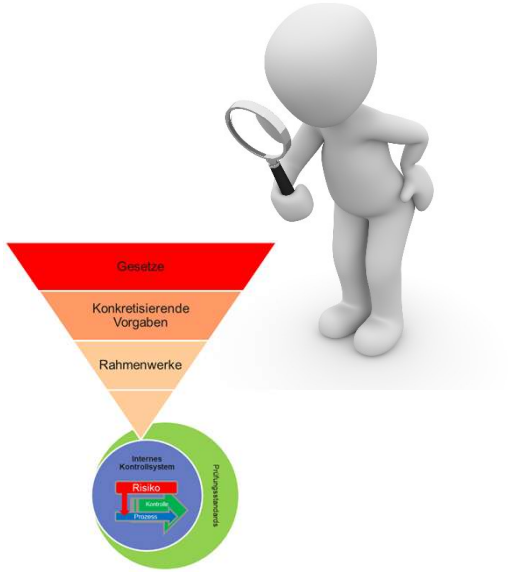
IDW PS 262, IDW PS 330, IDW PS 951,
IDW PS 982, Corporate Governance

Darstellung des IKS

Risiko, Prozess, Kontrolle,
Ordnungsmäßigkeits- und Sicherheitskriterien

Prüfen des IKS

Angemessenheit, Wirksamkeit,
Risiko-Kontroll-Matrix, Funktionstrennung,
Kennzahlensysteme, Stichprobenverfahren



Rückfrage über Abfrage…

Haben Sie Interesse an der Teilnahme eines Seminars „Prüfen des internen Kontrollsystems“?

https://www.diir.de/fileadmin/fachwissen/downloads/Three-Lines-Model-Updated-German.PDF

Tschüss, bis bald…

Vielen Dank für Ihre Aufmerksamkeit

Kontakt

Joachim Sell

www.SellfControl.de

Joachim.Sell@SellfControl.de

iboWebCON

Wir
organisieren
Zukunft.

ibo Akademie GmbH · Im Westpark 8 · D-35435 Wettenberg · T: +49 641 982 10-300 · training@ibo.de · www.ibo.de
ibo Software GmbH · Im Westpark 8 · D-35435 Wettenberg · T: +49 641 982 10-700 · info@ibo.de · www.ibo.de