Wir leben die Stadt

STADT : SALZBURG

Kontrollamt Salzburg

Grundlagen zum Risikomanagement und zu internen Kontrollsystemen sowie daraus abzuleitende Prüfungshandlungen

Kontrollämtertagung 19.-20.9.2023 in Dornbirn

Alexander Niedermoser, LLM - Kontrollamtsdirektor
Mag. Andrea Ibertsberger - Prüferin

Inhalt

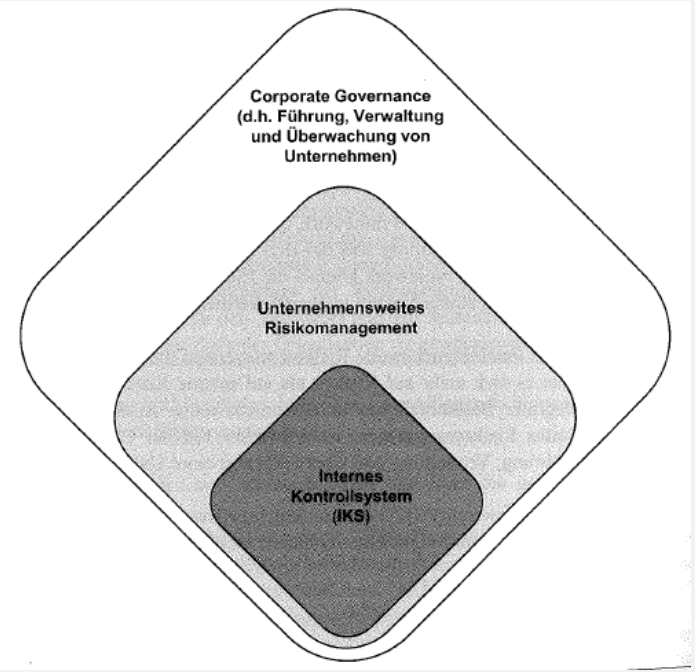
STADT : SALZBURG

Grundlagen
- Corporate Governance
- Definition interne Kontrolle
- Rechtliche Grundlagen

Theoretisches Modell zur Umsetzung
- COSO-Standard
- Aufbau internes Kontrollsystem
- Aufbau Risikomanagement

Prüfungshandlungen
- Vorbereitungen
- Erfahrungen aus der Prüfungspraxis
- Literatur

Corporate Governance



Quelle: Vgl Handbuch Interne Kontrollsysteme (IKS), Oliver Bungartz, Erich Schmidt Verlag, 2014, Seite 490

Corporate Governance bildet das Dach für

- Risikomanagementsystem (RMS)
- Internes Kontrollsystem (IKS)
- Compliance-Management-System (CMS)
- Internes Revisionssystem (IRS)
- Integriertes Managementsystem (IMS)

Corporate Governance

- umfasst die Rechte, Aufgaben und Verantwortlichkeiten aller Akteure
- inkludiert das Wohlverhalten und die Transparenz sowie die Bereitschaft zur Selbstkontrolle

Quelle: Vgl SWK-Heft 20/21, Juli 2017, S 943

Definition interne Kontrolle

Die interne Kontrolle ist ein in der Organisation eingebetteter Prozess, der von den Führungskräften und den Mitarbeitern durchgeführt wird, um

- bestehende Risiken zu erfassen,
- zu steuern und
- um sicherstellen zu können, dass die Organisation ihre Ziele erreicht.

Quelle: Vgl Leitfaden zur Überprüfung von Internen Kontrollsystemen, Rechnungshof Wien, Reihe 2016/3, Seite 8

IKS-Risikomanagement

Die Konzepte sind untrennbar miteinander verbunden, es geht um die Minimierung der Risiken und das Erreichen der Ziele.

Risikomanagement	IKS
Identifizierung, Analyse und Bewertung der Risiken einer Organisation nach potenziellem Schadensausmaß und Eintrittswahrscheinlichkeit	Festlegung von Prozessen und Verantwortlichkeiten, um die Risiken zu minimieren

Quelle: Vgl Leitfaden zur Überprüfung von Internen Kontrollsystemen, Rechnungshof Wien, Reihe 2016/3, Seite 10f

Rechtliche Grundlagen

GmbHG-Gesetz

- § 22: die Geschäftsführer haben dafür zu sorgen, dass ein Rechnungswesen und ein internes Kontrollsystem geführt werden, die den Anforderungen des Unternehmens entsprechen
- § 30g: fünffach große Gesellschaften benötigen einen Prüfungsausschuss mit den Aufgaben ein internes Kontrollsystem und ein Risikomanagementsystem zu führen

AktG – Aktiengesetz

- § 82: der Vorstand hat dafür zu sorgen, dass ein Rechnungswesen und ein internes Kontrollsystem geführt werden, die den Anforderungen des Unternehmens entsprechen

UGB – Unternehmensgesetzbuch

- § 243a: Rede- und Warnpflicht des Abschlussprüfers bei der Feststellung von wesentlichen Schwächen der internen Kontrollen des Rechnungslegungsprozesses

Rechtliche Grundlagen

Branchenbezogene Regelungen

- WGG – Wohnungsgemeinnützigkeitsgesetz: § 9a: Compliance - unwirksame und genehmigungspflichtige Rechtsgeschäfte
- GRVO – Gebarungsrichtlinienverordnung: § 2b: die Geschäftsführung hat einen jährlichen Corporate Governance Bericht zu erstellen

Corporate Governance Kodex

- Bundes-Public Corporate Governance Kodex
- Salzburger Corporate Gonvernance Kodex

Internationale Standards

- ISO9000
- INTOSAI Internationale Organisation der obersten Rechnungskontrollbehörden

Dienstanweisungen

Verträge

Inhalt

Grundlagen
- Corporate Governance
- Definition interne Kontrolle
- Rechtliche Grundlagen

Theoretisches Modell zur Umsetzung
- COSO-Standard
- Aufbau internes Kontrollsystem
- Aufbau Risikomanagement

Prüfungshandlungen
- Vorbereitungen
- Erfahrungen aus der Prüfungspraxis
- Literatur

COSO-Standard

COSO-Report = zentraler Standard für die Schaffung eines internen Kontrollsystems

Dieser Standard wurde vom Committee of Sponsoring Organizations of the Treadway Commission (private US-amerikanische Vereinigung) entwickelt.

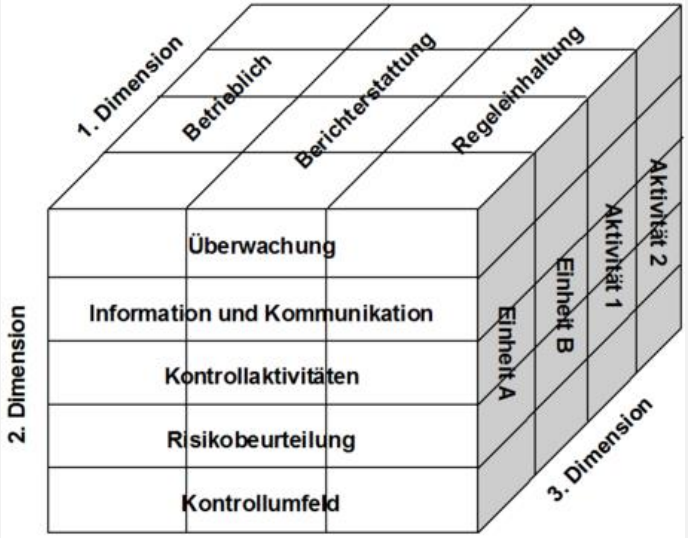


Abb: Drei Dimensionen eines IKS nach COSO

1. Dimension: drei Zielkategorien
2. Dimension: fünf Komponenten
3. Dimension: Organisationseinheiten

Jede der fünf Komponenten bezieht sich auf alle drei Zielkategorien.

COSO-Standard: Ziele - Komponenten

STADT : SALZBURG

Dimension der drei Zielkategorien

1. Betrieblich: Effektivität und Effizienz der Prozesse
2. Berichterstattung: Verlässlichkeit
3. Regeleinhaltung: Einhaltung der Gesetze und Vorschriften

Es besteht eine Wechselwirkung zwischen Zielen und Komponenten.

Dimension der fünf Komponenten

1. Kontrollumfeld: Integrität und ethische Werte, zB Verhaltenskodex, Unabhängigkeit der Kontrollorgane, Organisationsstruktur, Personalpolitik
2. Risikobeurteilung: Identifikation und Analyse, zB Risikomatrix nach Auswirkung und Eintrittswahrscheinlichkeit, Voraussetzung ist die Definition von Zielen

Quelle: Vgl Handbuch Interne Kontrollsysteme (IKS), Oliver Bungartz, Erich Schmidt Verlag, 2014, Seite 49ff

COSO-Standard: Ziele - Komponenten

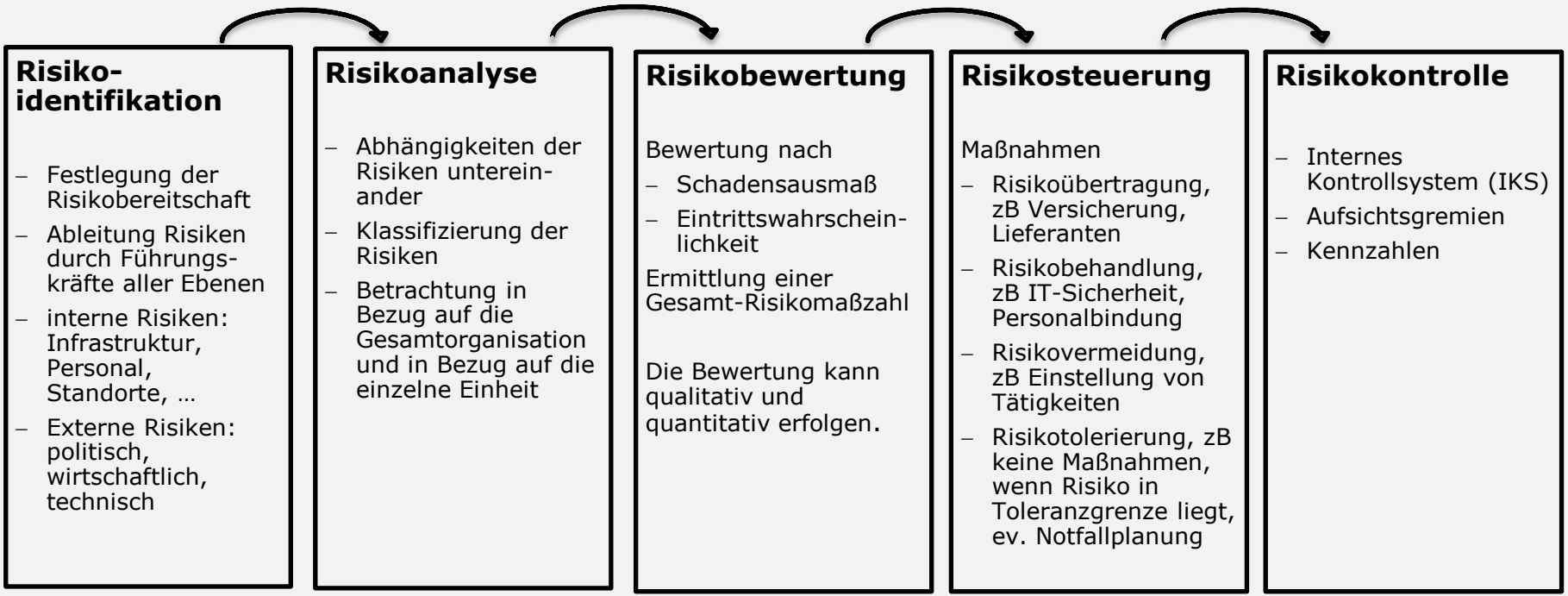
3. Kontrollaktivitäten: manuell oder automatisiert, vorbeugend oder aufdeckend, Routine oder Nicht-Routine Prozesse, Unternehmens- oder Bereichsebene, zB IT gestützte Transaktionen Kontrollen, 4-Augen Prinzip
4. Information und Kommunikation: interne oder externe Quellen/Daten, interne oder externe Empfänger, Beurteilung der Aktualität, Richtigkeit, Zugang zu Informationen, Vollständigkeit, Überprüfbarkeit, ..
5. Überwachungsaktivitäten: Berichterstattung, interne Revision

Hinweis:
Es gibt kein allgemeingültiges IKS-Konzept für alle Organisationen. Abhängig von Größe, Branche und Rechtsform muss ein individuelles IKS entwickelt werden.

Quelle: Vgl Handbuch Interne Kontrollsysteme (IKS), Oliver Bungartz, Erich Schmidt Verlag, 2014, Seite 49ff

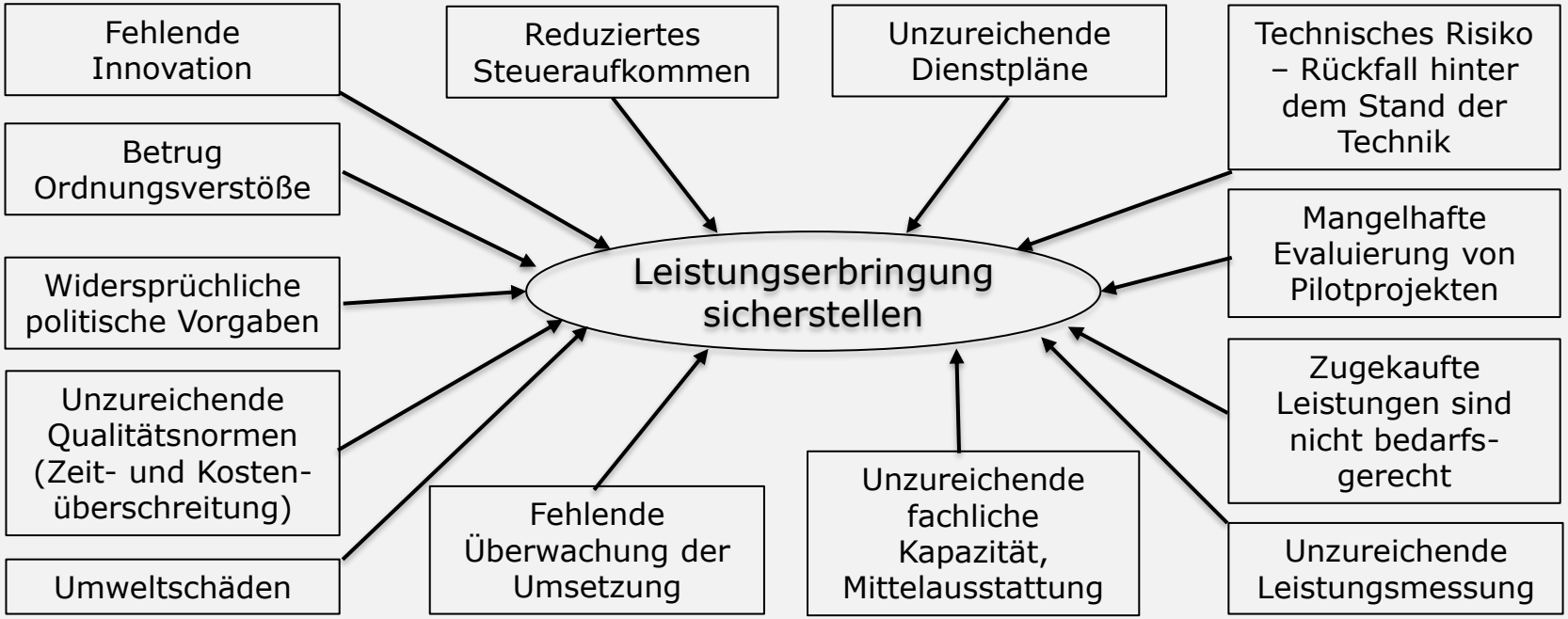
Risikomanagement Aufbau

STADT : SALZBURG



Quelle: Vgl INTSOSAI 9130, Richtlinien für Normen zur internen Kontrolle im öffentlichen Sektor: Weitere Informationen zum Thema umfassendes Risikomanagement, 2004, Seite 19ff

Risiken staatlicher Stellen



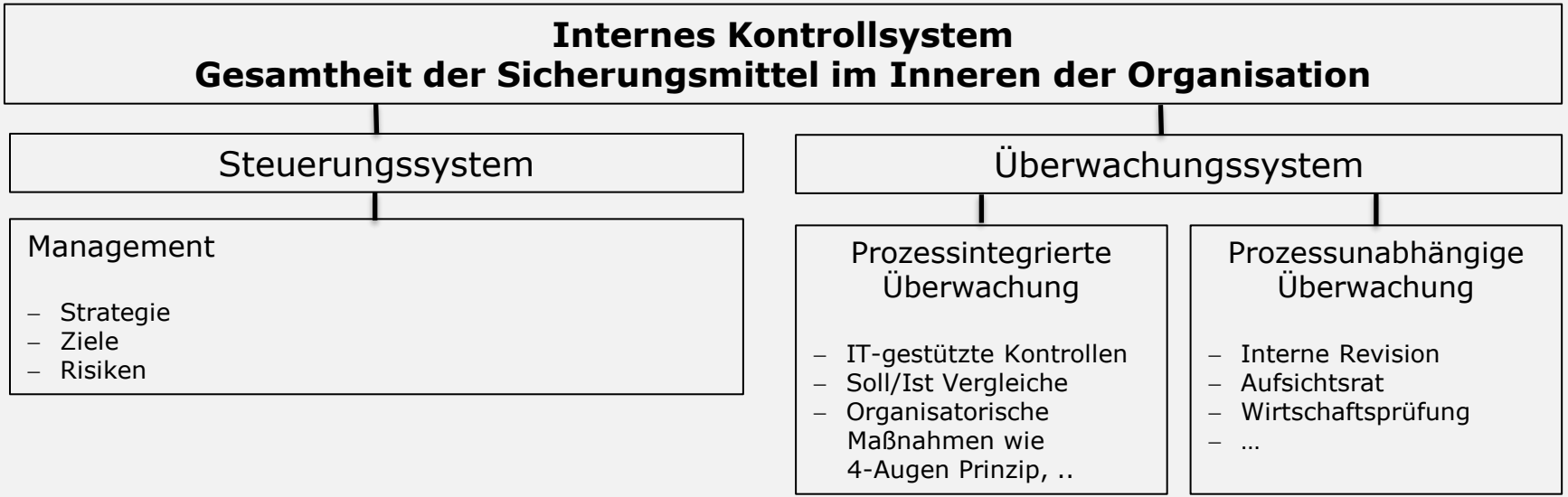
Quelle: Vgl INTSOSAI 9130, Richtlinien für Normen zur internen Kontrolle im öffentlichen Sektor: Weitere Informationen zum Thema umfassendes Risikomanagement, 2004, Seite 16

Risiko-Kontroll-Matrix

STADT : SALZBURG

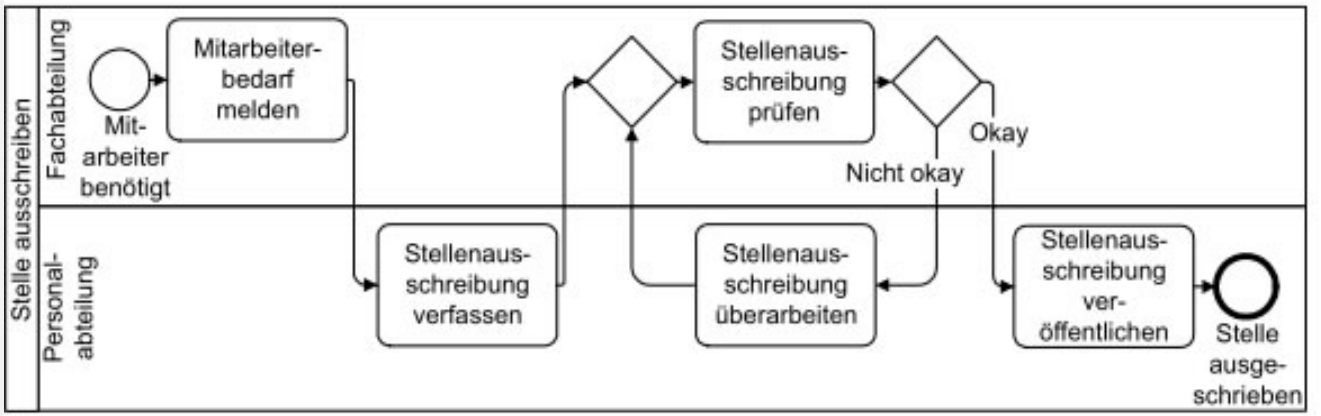
Risiko	Risikosteuerung	Kontrollaktivität	Schadens-ausmaß	Eintrittswahr-scheinlichkeit	Risikomaß-zahl
Liquiditäts-engpass	Rahmen bei Banken erweitern	Akt. Banksalden, Autom. Ermittlung Status, Planung …			
Ausfall IT-Systeme	Externer Security-Check	Täglich, wöchentliche Sicherungen, Lagerung der Backups, Notfallszenario, …			
Personalengpass Kundenservice	Telefonumleitung bei „Überlauf"	Messung Erreichbarkeit über Telefonanlage, Ressourcen planen			
Haftungsrisiken	Versicherung, Verträge anpassen	Versicherungssummen prüfen, Ursachen f. mögliche Haftungen kontrollieren			
Preisrisiken	Langfristige Verträge, Lagerung	Indexverlauf, wirtschaftliche Entwicklung			
Steuer-aufkommen sinkt	Szenarien möglicher Einsparungen, Rücklagen aufbauen	Überwachung der Entwicklung			

IKS Aufbau



Quelle: Vgl Handbuch Interne Kontrollsysteme (IKS), Oliver Bungartz, Erich Schmidt Verlag, 2014, Seite 24

IKS – Prozessbeschreibungen



- je klarer die Prozessschritte und Zuständigkeit, desto effizienter die Arbeitsweise
- die Mitarbeiter:innen sollten die Prozesse in ihrem Bereich kennen
- Kontrollschritte sollten im Prozess integriert werden

IKS Reifegrad

IKS–Reifegrad	Merkmale der einzelnen IKS–Reifegrade
Stufe 5: Optimiert	– Ausgeprägtes Kontrollbewusstsein im ganzen Unternehmen – Weitgehende Automatisierung der Kontrollaktivitäten – Hohe Reaktionsfähigkeit auf Veränderungen durch Tools – Integriertes IKS, Revisions– und Risikomanagementsystem
Stufe 4: Überwacht	– IKS–Grundsätze und Richtlinien sind detailliert dokumentiert – Regelmäßige Überwachung der Kontrollen – Laufende Aktualisierung der Kontrollen – Regelmäßige IKS–Berichterstattung
Stufe 3: Definiert	– IKS–Grundsätze und Richtlinien sind dokumentiert – Kontrollen sind in den Prozessen integriert und dokumentiert – Nachvollziehbarkeit der Kontrollen ist gegeben – Information, Kommunikation und Schulung existieren
Stufe 2: Wiederholbar	– Interne Kontrollen sind vorhanden, aber nicht standardisiert – Fehlende Nachvollziehbarkeit der Kontrollen – Kontrollen sind personenabhängig und nicht dokumentiert – Fehlende Information, Kommunikation und Schulung
Stufe 1: Initial	– Unstrukturiertes Kontrollumfeld im Unternehmen – Interne Kontrollen sind kaum oder nicht vorhanden – Vorhandene Kontrollaktivitäten werden fallweise ausgeführt – Vorhandene Kontrollen sind nicht verlässlich

Je höher der Reifegrad desto ausgeprägter ist das IKS.

In der Literatur wird gefordert, dass ein Unternehmen eine IKS-Reifegrad von Stufe 3 erreichen sollte, bei Aktiengesellschaften sollte Stufe 4 erreicht werden.

Quelle: Vgl Handbuch Interne Kontrollsysteme (IKS), Oliver Bungartz, Erich Schmidt Verlag, 2014, Seite 457

Inhalt

STADT : SALZBURG

Grundlagen
- Corporate Governance
- Definition interne Kontrolle
- Rechtliche Grundlagen

Theoretisches Modell zur Umsetzung
- COSO-Standard
- Aufbau internes Kontrollsystem
- Aufbau Risikomanagement

Prüfungshandlungen
- Vorbereitungen
- Erfahrungen aus der Prüfungspraxis
- Literatur

Vorbereitung

STADT : SALZBURG

Prüfungplanung

- Ziele für die Prüfung iZ mit dem IKS und Riskomanagement festlegen

Unterlagenanforderung

- Organisationshandbuch
- IKS Handbuch
- Prozessbeschreibungen abgeleitet aus den Prüfungszielen (Stichproben)
- Risikomatrix
- Sonstige Berichte Jahresabschluss, IKS Bericht, Compliance Bericht, Protokolle Prüfungsausschuss, …

Prüfungshandlungen

- Klärung der rechtlichen Grundlagen (AktG, GmbHG, …)
- Gibt es sonstige Richtlinien wie zB Corporate Governance, Gesellschaftsvertrag, Geschäftsführervertrag, Dienstanweisungen
- Reifegrad des IKS bestimmen
- Analyse des Risikomanagementprozesses: wer ist wofür zuständig, ab wann greifen welche Mechanismen, ..
- Analyse der Risikomatrix
- Quervergleich der genannten Risiken mit sonstigen Dokumenten wie Protokollen, dh wurden in Protokollen Risiken angesprochen, die in der Risikomatrix nicht vorhanden sind, wurden Risiken genannt, die nicht überwacht werden
- Quervergleich tatsächliche Auswirkungen vs Risikomatrix im Prüfzeitraum
- Interview mit den verantwortlichen Personen

Prüfungshandlungen - Checklisten

STADT : SALZBURG

Beispiele von Beurteilungen auf Basis von Checklisten:

Aufbauorganisation
- liegt ein schriftliches Organigramm vor
- sind Stellenbeschreibungen vorhanden
- sind Stellvertretungen ausreichend geregelt

Rechnungswesen:
- Mahnwesen: Ablauf, Intervalle, Übergabe an Inkasso
- Protokollierung von Änderungen der Stammdaten
- Abgleich Nebenbücher mit Hauptbuch
- Funktionstrennung Kassa, Wertpapierverwaltung, Einkauf, Wareneingang
- wer kann erfolgswirksame Um- und Ausbuchungen vornehmen

Quelle: Vgl ABC der Gestaltung und Prüfung des Internehmen Kontrollsystems im Unternehmen, Klinger/Klinger, 2011, Seite 71ff

Prüfungspraxis Risikomanagement

STADT : SALZBURG

Sachverhalt

- Prüfungsschwerpunkt lag auf einem Geschäftsbereich mit untergeordneter Bedeutung für das Gesamtunternehmen
- IKS und Risikomanagementprozess war vorhanden
- Risikomatrix war vorhanden
- die Beurteilung der Risiken erfolgte nach den folgenden Kriterien:
  - Eintrittswahrscheinlichkeit
  - Auswirkung
  - Entdeckungswahrscheinlichkeit

  Jedes Kriterium wurde von Stufe 1 bis 10 bewertet. Ergebnis war eine Risiko-Prioritätszahl mit einer Bandbreite von 1 bis 1.000. Je höher der Wert, desto höher das Risiko.

Prüfungspraxis Risikomanagement

STADT : SALZBURG

<u>Feststellung</u>:

- Es wurden für den Geschäftsbereich 71 Risiken identifiziert, wobei nur 3 Risiken einen Risikoprioritätszahl > 500 hatten
- die höchsten Risiken wurden in eher unwahrscheinlichen strategischen Themen gesehen
- die Eintrittswahrscheinlichkeit und die Auswirkung technischer und personeller Risiken wurden völlig falsch eingeschätzt
- Widerspruch der Risikomatrix zu anderen Dokumenten wie zB Protokollen
- die negativen Auswirkungen dieser Risikobeurteilungen konnten im Prüfzeitraum aufgezeigt werden
- notwendige Maßnahmen wurden nicht zeitgerecht eingeleitet

Prüfungspraxis IKS - Risikomanagement

STADT : SALZBURG

Sachverhalt

- der Prüfungsschwerpunkt lag auf der gesamten Gebarung
- einzelne Risiken wurden im Jahresabschluss oder im IKS Bericht aufgezeigt und es gab dazu ein laufendes Reporting und Maßnahmen
- es wurden Risiken im Rahmen von Aufsichtsratssitzungen angesprochen
- ein Risikomanagementprozess war nicht dokumentiert
- eine Risikomatrix mit Eintrittswahrscheinlichkeit und Auswirkung war nicht vorhanden

Feststellung

- das Risikomanagement entsprach nicht dem GmbH-Gesetz und dem Salzburger Corporate Governance Kodex
- es bestand die Gefahr, dass neu auftretende Risiken nicht identifiziert wurden

Prüfungspraxis Verwaltung

Die Stadt Salzburg begann ab 2014 ein Risikomanagement zu implementieren.

Eine Prüfung des Rechnungshofes (Reihe Salzburg 2020/5) stellte folgende Mängel fest:

- Die Stadt bestimmte keine Risikokategorien; eine Analyse der bisher identifizierten Risiken wurde noch nicht durchgeführt. Es fehlte somit eine Gesamtübersicht über die Einzelrisiken.
- Die Risiken wurden nicht nach Einrittswahrscheinlichkeit und Schadensausmaß bewertet; alle Risiken waren demnach gleich gewichtet.
- Es wurden keine Risikomanager bestimmt (die Amtsleiter waren Risikomanager und Risikoeigner).
- Eine regelmäßige Evaluierung war nicht vorgesehen.

Prüfungspraxis Verwaltung

Die vom Kontrollamt durchgeführten Prüfungen der letzten Jahre ergaben folgende Risiken:

- Die im IKS hinterlegten Prozessbeschreibungen entsprachen nicht den tatsächlichen Abläufen

  → Prüfungshandlung: Prozesse mit den dafür verantwortlichen Mitarbeitern besprechen

- In der Stadt Salzburg existierte keine zentrales Vertragsverwaltung, die Verträge konnten teilweise nur schwer aufgefunden werden.

  → Risiko: Zivilrechtliche Ansprüche können nicht durchgesetzt werden.

  Vertragbestimmungen (zB Indexvereinbarungen, Kündigungsfristen etc) werden nicht vollzogen

  → Empfehlung: Aufbau eines digitalen Vertragsmanagements mit „Erinnerungsfunktion"

Prüfungspraxis Verwaltung

Die vom Kontrollamt durchgeführten Prüfungen der letzten Jahre ergaben beispielsweise folgende Risiken:

- Keine zentrale Mahnevidenz
  - → Risiko: Forderungen werden nicht eingetrieben und verjähren
  - → Besonderes Risiko: gesonderte EDV-Systeme für einzelne Bereiche
- Keine Kontrollmechanismen zB Mahnwesen
- Begräbnisvoreinzahlungen wurden auf Sparbüchern verwaltet und mittels Excellisten in Evidenz gehalten
  - → Risiko: kein Vier-Augen-Prinzip

→ Datenverlust, Datenmanipulation

Stand öffentliche Verwaltung

Auszug der Ergebnisse der empirischen Untersuchung zum Entwicklungsstand des Risikomanagements im kommunalen Bereich:

- 10 % der Gemeinden haben ein ausgeprägtes, 40 % ein wenig ausgeprägtes Risikomanagement
- 28 % der Gemeinden sehen aufgrund der Größe keine Relevanz für ein Risikomanagement
- gibt es ein Risikomanagement, dann vor allem in der Finanzabteilung
- Vier-Augen-Prinzip kommt bei 90 % der Gemeinden zur Anwendung
- nur 6 % verwenden Risikokennzahlen
- größte Herausforderung: mangelnde Sensibilität und Fachkenntnisse der Mitarbeiter:innen und Ressourcen wie Zeit bzw Budget
- mehrheitlich wird von einer steigenden Relevanz des Risikomanagements ausgegangen

Quelle: Vgl Risikomanagement in der öffentlichen Verwaltung, Christian Theuermann, GRC aktuell, 4/2018, Seite 149f

Literatur

- Handbuch Interne Kontrollsysteme (IKS), Oliver Bungartz, Erich Schmidt Verlag, 2014
- Leitfaden zur Überprüfung von Internen Kontrollsystemen, Der Rechnungshof Wien, Reihe 2016/3
- Richtlinien für die internen Kontrollnormen im öffentlichen Sektor, INTOSAI 9100, www.issai.org/pronouncements/endorsed-as-intosai-gov-9100/
- Weitere Informationen zum Thema umfassendes Risikomanagement, INTOSAI 9130, www.issai.org/pronouncements/endorsed-as-intosai-gov-9130/
- ABC der Gestaltung und Prüfung des Internen Kontrollsystems im Unternehmen, Klinger/Klinger, Linde Verlag, 2011
- Revision des Internen Kontrollsystems, Deutsches Institut für Interne Revision e.V., Erich Schmidt Verlag, 2020
- Risikomanagement der öffentlichen Hand, Scholz/Schuler/Schwintovski, Physica Verlag, 2008

Vielen Dank für Ihre Aufmerksamkeit!