Ein internes Kontrollsystem sicherstellen

23.01.2022

Dirk J. Lamprecht

© examio

Gliederung

1. Sicherstellung eines IKS

1.1 Erkennung der Risiken eines Unternehmens

1.4 Frühwarnsysteme und Risikobewertung

1.5 Risikoquellen

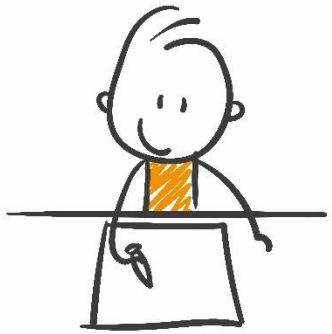
2. Aufbau eines IKS

2.1 Rechtliche Grundlagen eines IKS

2.2 Verringern von Fehlerrisiken

2.3 Risikofrüherkennungssystem

2.4 Kontrollbereiche des IKS



© examio

Gliederung

3.1 Kontrollaktivitäten

3.2 Information und Kommunikation

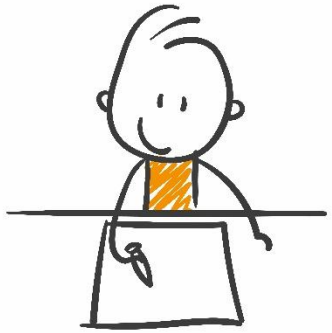
3.3 Überwachungsaktivitäten

4.1 Prozessorganisation und Risiko-Kontroll-Matrix

4.3 Relevante Kennzahlen

5.1 TAX-CMS

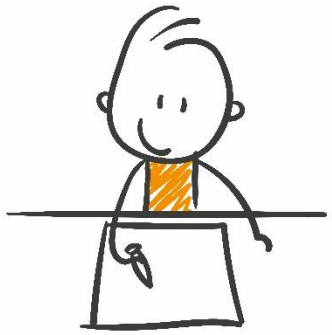
5.2 Aufgaben und Lösungen



© examio

Qualifikationsinhalte lt. Prüfungsordnung

- Arten von Risiken identifizieren,
- Ein internes Kontrollsystem aufbauen,
- Methoden zur Beurteilung von Risiken einsetzen und
- Maßnahmen zur Vermeidung von Risiken ableiten.



© examio

1. Sicherstellung eines IKS

Im Kurs „Ein Internes Kontrollsystem sicherstellen“ gehen wir ein auf

- Grundlagen eines IKS
- Aufbau eines IKS
- Komponenten eines IKS
- Methoden zur Risikobeurteilung und
- Vermeidung von Risiken.

1.1 Erkennung der Risiken eines Unternehmens

- Der Aufbau eines Internen Kontrollsystems (= IKS) ist von Unternehmen zu Unternehmen und von Branche zu Branche unterschiedlich.
- Hierbei ist es wichtig, das IKS auf die **Unternehmensziele abzustimmen** und die **wesentlichen Risiken** im Fokus zu behalten.

© examio

1.1 Erkennung der Risiken eines Unternehmens

Der Wirtschaftsprozess:

- Zielsystem
- Managementsystem
- Leistungsprozess
  - Beschaffung
  - Produktion
  - Absatz
- Finanzprozess

© examio

1.1 Erkennung der Risiken eines Unternehmens

- Aufbauend auf diesem Wirtschaftsprozess der Unternehmung ist es wichtig, **Risiken zu erkennen**, und zwar für die einzelnen Teilbereiche, also für das Zielsystem, das Managementsystem, den Leistungsprozess und den Finanzprozess.
- Der **Begriff Risiko** lässt sich nun unterteilen in eine
    - traditionelle Sichtweise und
    - eine neuere Sichtweise.

© examio

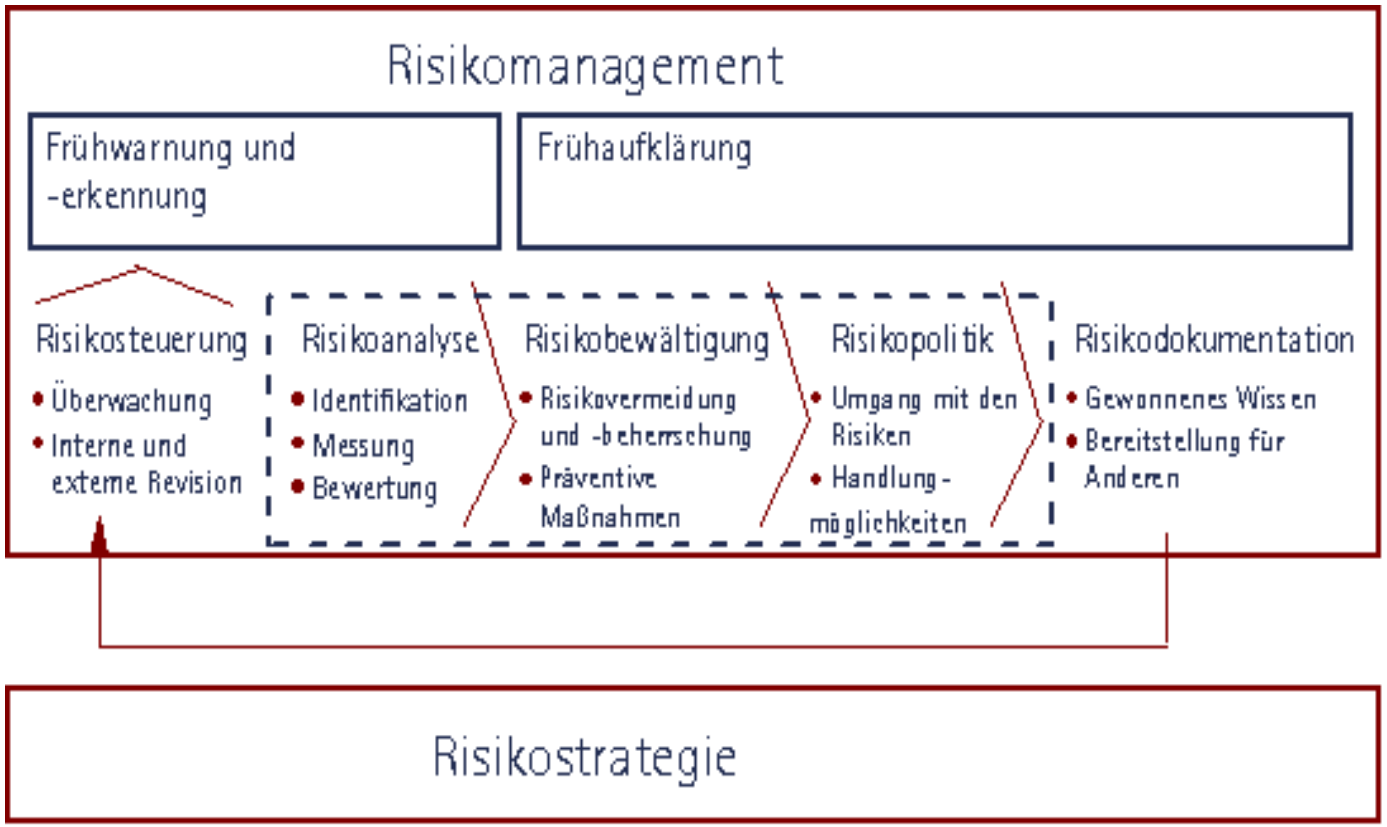
1.1 Erkennung der Risiken eines Unternehmens

- Die **traditionelle** Sichtweise beschreibt **Risiko als möglichen Nachteil** durch **Abweichung** von einer gegebenen **Zielgröße**, welche zu einem schlechteren Ergebnis, zu einem Verlust, führen wird.
- Man spricht hierbei von **Risiko im engeren Sinne** und betrachtet **Risiko ausschließlich** als **negativ**.
- Positive Abweichungen von der Zielgröße finden nicht statt.

- Risiko nach **neuerer Sichtweise** umfasst hingegen **positive, aber auch negative Abweichungen** von einem Ziel.
- **Chancen werden** also explizit **in das Risiko einbezogen**, man spricht von Risiko im weiteren Sinn.

© examio

1.1 Erkennung der Risiken eines Unternehmens



1.1 Erkennung der Risiken eines Unternehmens

Risiko-management - Matrix

	Wenig wahrscheinlich	Wahrscheinlich	Sehr wahrscheinlich
hoch			
mittel			
gering			

Intensiv steuern

Intensiv beobachten

beobachten

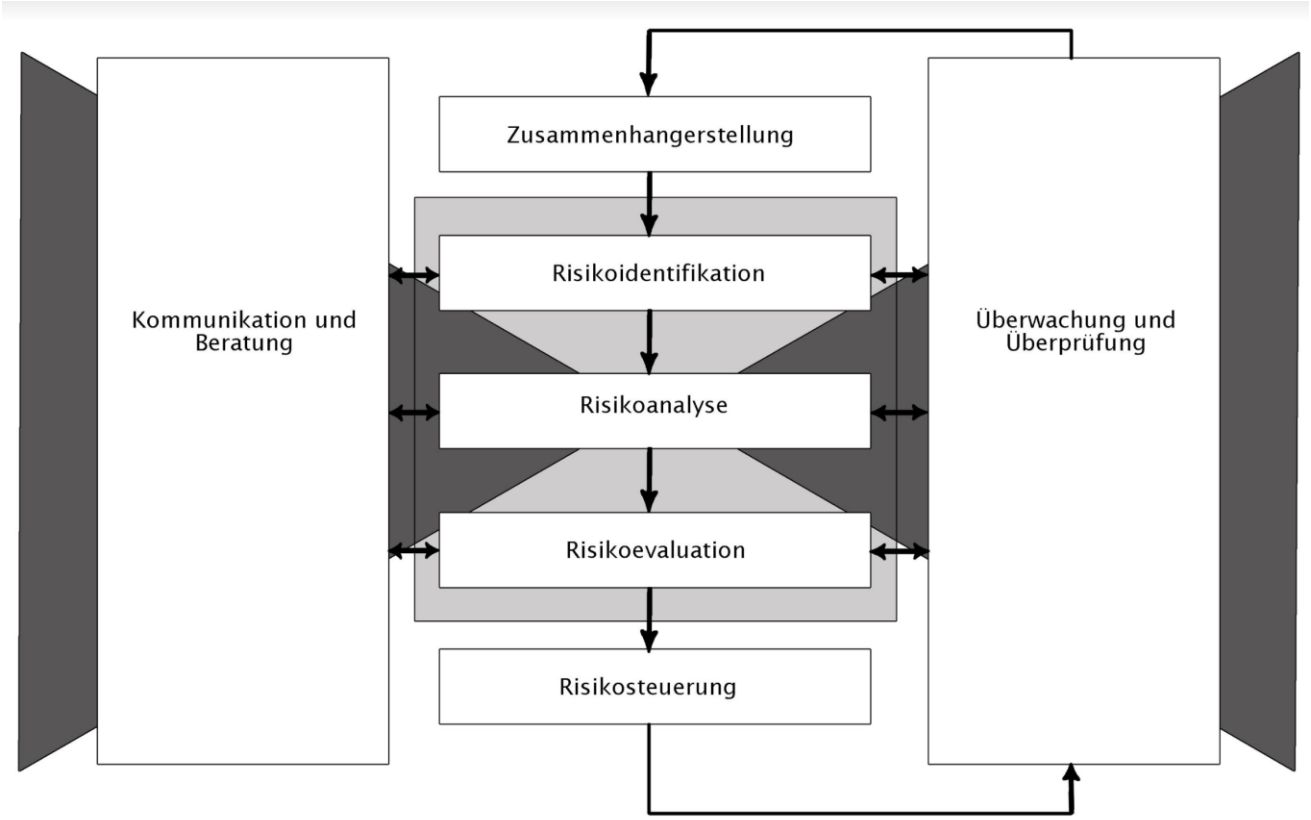
1.1 Erkennung der Risiken eines Unternehmens

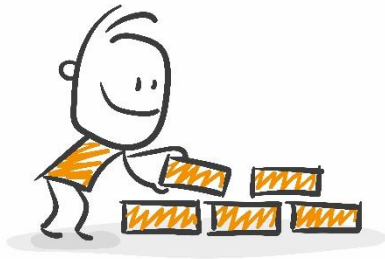
- Bei der **Top-Down-Methode** geht es darum, die **Wirkung des Risikos auf finanzielle Größen** wie Umsätze, Aufwendungen und den Gewinn **zu kalkulieren**.

- Die Bottom-Up-Methode setzt nicht bei der **Wirkung** des Risikos, sondern bei den **Ursachen** desselben an.

© examio

1.1 Erkennung der Risiken eines Unternehmens





1.1 Erkennung der Risiken eines Unternehmens

- Bezüglich der Möglichkeiten der Risikobegrenzung unterscheiden wir:
    - Vermeidung von Risiken,
    - Verringerung derselben,
    - Begrenzung von Risiken,
    - Risikotransfer und
    - Risikoübernahme.

© examio

1.1 Erkennung der Risiken eines Unternehmens

- Bei der **Vermeidung von Risiken** werden **risikoreiche Aktivitäten nicht durchgeführt**.
- Die **traditionelle Sichtweise** würde hierbei sagen, dass das Risiko **vollständig vermieden** wird, die **neuere Sichtweise** hingegen sieht es anders und stellt fest, dass **nicht nur Gefahren** vermieden werden, sondern **auch Chancen**.

- Bei der **Verringerung von Risiken** soll es **unwahrscheinlicher** gemacht werden, **dass ein risikoreiches Ereignis eintritt**.
- Ebenfalls lässt sich hierbei Risikodiversifikation durchführen: Man gleicht unterschiedliche Risiken miteinander aus.

© examio

1.1 Erkennung der Risiken eines Unternehmens

- Dies ist möglich, wenn die beiden **Risiken negativ miteinander korrelieren**.
- Konkret heißt dies, dass ein Zusammenhangsmaß (welches, vereinfacht gesprochen, mit dem Begriff „Korrelationskoeffizient“ gleichgesetzt werden kann) echt kleiner sein wird als null.
- Wenn **das eine Risiko steigt**, so **sinkt das andere** hierdurch.

1.1 Erkennung der Risiken eines Unternehmens

- Bei der **Begrenzung von Risiken** geht es darum, nicht das Risiko an sich zu vermeiden, sondern vielmehr den **möglichen Schaden**, der hierdurch resultiert, zu **beschränken**.

- Durch **Risikotransfer** soll das Risiko eines Schadens **auf eine Versicherung übertragen** werden, die also für den Schaden aufkommen wird. Man überträgt somit das Risiko auf einen Dritten – **was nicht immer möglich ist**! Z.B. im Steuerrecht.

© examio

1.1 Erkennung der Risiken eines Unternehmens

- Schließlich bedeutet eine **Risikoübernahme**, dass man sich **bewusst für das Eingehen** von Risiken **entscheidet**.
- Grund hierfür könnte sein, dass man die **Chancen auf positive Abweichung** von der **Zielgröße als bedeutungsvoller** ansieht **als** die mögliche **negative Abweichung**, also das Risiko.

1.1 Erkennung der Risiken eines Unternehmens

Wir unterscheiden Risiken nach unterschiedlichen Ansätzen:

- bzgl. der Existenz einer Chance
  - symmetrische Risiken
  - asymmetrische Risiken
- bzgl. der Fristigkeit
  - strategische Risiken
  - operative Risiken

© examio

1.1 Erkennung der Risiken eines Unternehmens

Wir unterscheiden Risiken nach unterschiedlichen Ansätzen:

- bzgl. der Messbarkeit
  - quantifizierbar
  - nicht quantifizierbar
- bzgl. des Bezugs zu Rahmenbedingungen (hier ist die SWOT-Analyse wichtig)
  - externe Risiken
  - interne Risiken der Schädigung

© examio

1.1 Erkennung der Risiken eines Unternehmens

Wir unterscheiden Risiken nach unterschiedlichen Ansätzen:

- bzgl. der Rahmenbedingungen
  - externe Risiken
  - interne Risiken
- bzgl. des betriebswirtschaftlichen Hintergrunds
  - leistungswirtschaftliche Risiken (Forschung und Entwicklung, Absatz und Vertrieb)
  - finanzwirtschaftliche Risiken (Marktpreise, Schuldnerbonität)
- ökologische Risiken (Natur- und Umweltkatastrophen)

© examio

1.1 Erkennung der Risiken eines Unternehmens

- Die **symmetrischen Risiken** haben die Eigenschaft, dass ein mögliches **negatives Risiko**, also ein Verlust, **stets einem positiven Risiko**, also einer Chance, **gegenübersteht**.
- **Asymmetrische Risiken** bieten **diese Chance nicht**.

- **Strategische Risiken** sind durch **langfristige Entscheidungen** im Unternehmen hervorgerufen,
- **operative Risiken** hingegen sind stets **kurzfristig**.

© examio

1.1 Erkennung der Risiken eines Unternehmens

- Bei **quantifizierbaren Risiken** lässt sich das **Schadensausmaß bewerten**, dies ist bei **nichtquantifizierbaren** Risiken **nicht** der Fall.

- **Externe Risiken** sind die Folge von **unvorhergesehenen** unternehmerischen Rahmenbedingungen, **interne Risiken** ergeben sich **aus leistungs- oder finanzwirtschaftlichen Prozessen**.

© examio

1.1 Erkennung der Risiken eines Unternehmens

- Bezüglich der externen und internen Risiken lässt sich die sog. **SWOT-Analyse** anführen. Hierbei stehen die einzelnen Buchstaben für
    - S wie Strength (= Stärke)
    - W wie Weakness (= Schwäche)
    - O wie Opportunities (= Chancen)
    - T wie Threats (= Bedrohungen).

© examio

1.1 Erkennung der Risiken eines Unternehmens

- Die **SWOT-Analyse untersucht**, ob sich **Stärken und Schwächen** des Unternehmens **in der Strategie** des Unternehmens wiederfinden,
- ob also **auf Veränderungen** der Unternehmensumwelt **angemessen reagiert werden kann**.
- Ob also an gewissen Stellen **vorbeugende Reaktionen erforderlich sind**, um bestimmten Risiken zu begegnen.

© examio

1.1 Erkennung der Risiken eines Unternehmens

- Risiken **mit betriebswirtschaftlichem Hintergrund**:
    - Forschung und Entwicklung (z.B. suche nach einem Medikament),
    - Absatz und Vertrieb (z.B. Vertriebsanstrengungen),
    - finanzwirtschaftlichen Risiken (z.B. zu hohe Herstellungskosten),
    - Ökologische Risiken (z.B. Naturkatastrophen)

© examio

1.1 Erkennung der Risiken eines Unternehmens

- Wie lassen sich Risiken identifizieren?
- Es wird unterschieden in Risiken
    - bzgl. der Identifikation (bisher) **bekannter Risiken** (Kollektionsmethoden)
    - bzgl. der Identifikation (bisher) **unbekannter Risiken** (analytische Methoden, Kreativitätsmethoden)

© examio

1.1 Erkennung der Risiken eines Unternehmens

- Wie lassen sich nun Risiken identifizieren?
- Zu den Kollektionsmethoden zählen:
    - Befragungen
    - Prüfung von Dokumenten und
    - Betriebsbesichtigungen.

© examio

1.1 Erkennung der Risiken eines Unternehmens

- Wie lassen sich nun Risiken identifizieren?
- Die **Befragungen** erfolgen mit einem **Fragebogen**.
- Hierbei können allerdings **nicht alle Risiken aufgedeckt** werden.
- Die Dokumentenprüfung erfolgt durch **schriftliche Aufzeichnungen**.
- Bei **Betriebsbesichtigungen** lassen sich **Informationen durch persönliche Besuche** erzielen und **dabei** das Potenzial eines **Risikos einschätzen**.

© examio

1.1 Erkennung der Risiken eines Unternehmens

- Zu den analytischen Methoden zählen:
    - die morphologische Analyse,
    - die Fehlerbaumanalyse und
    - das Ishikawa-Diagramm.
- Bei der **morphologischen Analyse** erfolgt eine **Zerlegung** des Gesamtproblems **in Teilprobleme**.
- Die einzelnen **Einflussgrößen** werden dann **systematisch variiert**, **um die Lösung** des Problems **zu ermitteln**.

© examio

1.1 Erkennung der Risiken eines Unternehmens

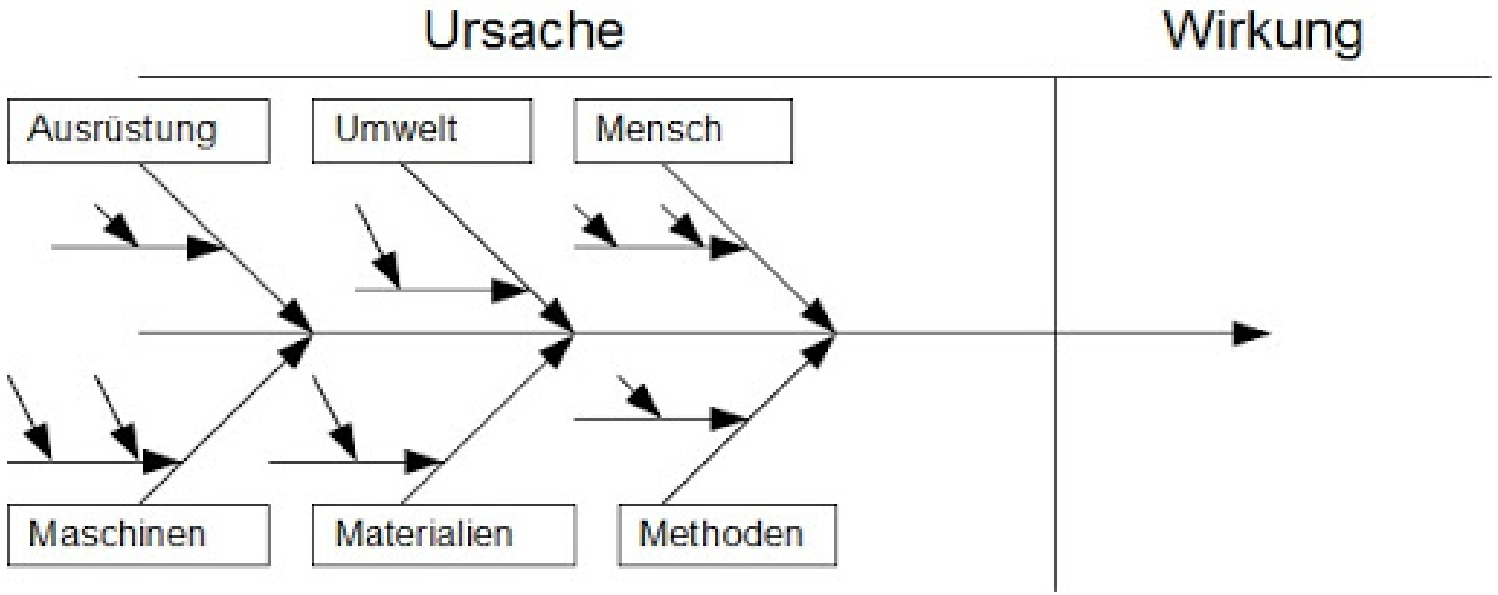
- Mit der **Fehlerbaumanalyse** lässt sich untersuchen, ob und wie das **Verhalten eines Prozesses** bzw.
- das Verhalten eines Produktes **ein Risiko** für die Unternehmung **darstellt**.
- Das Ganze ist eine Analyse von hinten nach vorne, ähnlich eines **Rollback-Verfahrens**.

- Das **Ishikawa-Diagramm** (= Fischgräten-Diagramm) unterteilt die **grobe Struktur eines Problems** in Form eines **Fischgrätenmusters**.

© examio

1.1 Erkennung der Risiken eines Unternehmens

- Das Problem wird am Ende dieses Musters benannt, die Hauptarme werden mit
  - Mensch,
  - Maschine,
  - Methode und
  - Material



1.1 Erkennung der Risiken eines Unternehmens

- Danach werden diesen **einzelnen Kategorien** die **möglichen Ursachen** des Problems **zugeordnet**.
- Es **lässt sich also feststellen**, ob die **Ursache** des Problems „**menschlich** verursacht“ bzw. „durch eine **Maschine** verursacht“ ist oder aber das „**Material**“ für ein Problem verantwortlich ist bzw. die „gewählte **Methode**“.

1.1 Erkennung der Risiken eines Unternehmens

- Kreativitätsmethoden hingegen sind
  - Brainstorming,
  - Delphi-Methode,
  - Szenarioanalyse und
  - Brainwriting.

1.1 Erkennung der Risiken eines Unternehmens

- Beim **Brainstorming** sitzen Menschen zusammen und sammeln in **freier Assoziation Ideen**.
- Streng **verboten** sind hierbei die **Kommentierung der Ideen** der Anderen oder Kritik an ihnen.
- **Lösungen werden** im Rahmen des Brainstorming **nicht erarbeitet**, erst nach der Ideenfindung wertet man die Beiträge aus, **diskutiert und erläutert** sie.

© examio

1.1 Erkennung der Risiken eines Unternehmens

- **Brainwriting** ist eine **Abwandlung des Brainstorming**, hierbei besteht **kein Zeitdruck** beim **Sammeln** der Ideen und beim **schriftlichen Festhalten** derselben.

- Die **Delphi-Methode** ist eine **Schätzmethode**, hierbei wird eine **Gesamtprognose** für die Entwicklung **von Risiken der Zukunft** entwickelt.
- Experten sollen hierbei in **mehreren Befragungsrunden** ihre **Einschätzung zu den Risiken** anonym abgeben.
- **Erst danach** werden die Meinungen der **anderen Teilnehmer mitgeteilt**. Die Delphi-Methode ist also eine **Expertenbefragung**.

© examio

1.1 Erkennung der Risiken eines Unternehmens

- Bei der **Szenarioanalyse prognostiziert** man durch **Vergangenheitsdaten** mögliche Entwicklungen der Zukunft.
- Hierbei werden **Zukunftssituationen simuliert**, um hieraus unternehmerische Entscheidungen für eine bessere Entwicklung abzuleiten.
- **Einzelne Risiken** werden **vollständig erfasst** und unterschiedlichen **Kategorien** von Risiken **zugeordnet**.

1.1 Erkennung der Risiken eines Unternehmens

- Es lassen sich z. B. folgende Risiken unterscheiden:
    - Marktrisiken
    - Produktionsrisiken
    - Finanzierungsrisiken
    - politische Risiken
    - Umweltrisiken.

© examio

1.1 Erkennung der Risiken eines Unternehmens

- Bei den **politischen Risiken** lassen sich z. B. Umwälzungen in anderen Staaten nennen, Finanzierungsrisiken bestehen unter anderem dann, wenn Kreditinstitute Darlehen nicht weiter vergeben.
- Wenn neue Wettbewerber in den Markt dringen oder bestehende Produkte bei den Kunden keinen Absatz mehr finden, spricht man von **Marktrisiken**.
- Stärkere Regulierungen im Umweltbereich durch den Staat lassen sich als Beispiel von **Umweltrisiken** nennen.

© examio

1.4 Frühwarnsysteme und Risikobewertung

- Durch **Frühwarnsysteme** sollen **Risiken früher erkannt** und dadurch **besser gesteuert** werden können, denn man kann **schneller reagieren**.
- Mithilfe von Frühwarnindikatoren sollen Gefahren früher erkannt werden, die bereits vorhanden waren, aber **noch nicht entdeckt wurden**.
- Bei diesen Frühwarnindikatoren lassen sich
    - Umfeldindikatoren sowie
    - Unternehmensindikatoren

  unterscheiden.

© examio

1.4 Frühwarnsysteme und Risikobewertung

- Zu den **Umfeldindikatoren** gehören Zahlen zur **Entwicklung der Löhne**, der allgemeinen **Konsumfreudigkeit**, der **Bevölkerung**, der Entwicklung des **Bruttoinlandsprodukts**, der **konjunkturellen Entwicklung**, aber auch der Entwicklung des **Preisniveaus**.

- Bei den **Unternehmensindikatoren**, welche also **auf das einzelne Unternehmen beschränkt** sind, lassen sich anführen die **Entwicklung der Umsätze**, der **Kosten** und insofern auch der Gewinne.
- Zusätzlich aber ist auch die **Entwicklung der Liquiditätssituation** sowie der **Rentabilität** von Bedeutung.

© examio

1.4 Frühwarnsysteme und Risikobewertung

- Das **Interne Kontrollsystem (IKS)** dient der **Überwachung und der Steuerung von Risiken**.

- Das **Risikomanagementsystem** hingegen, welches das interne Kontrollsystem umfasst, dient vielmehr der **Definition einer Strategie** und der **Risikobereitschaft** des Unternehmens.
- Ein Risikomanagementsystem als Prozess **umfasst die Identifikation von Risiken**, die **Überwachung** und **Analyse** derselben sowie das **Steuern und Bewerten von Risiken**.

© examio

1.5 Risikoquellen

- **Wirtschaftliche Risiken** können aus unterschiedlichen Gründen heraus resultieren, nämlich aus
  - dem Personalbereich,
  - dem Beschaffungsbereich,
  - dem technischen Bereich,
  - dem Absatzbereich und
  - dem Finanzierungsbereich.

1.5 Risikoquellen

- Im **Personalbereich** ist ein mögliches Risiko stets das **Abwandern von Mitarbeitern**.
- Dadurch kann es zu **Produktionsausfällen** kommen und folglich **geringeren Absätzen**, mithin geringeren Umsätzen und schließlich **geringeren Gewinnen**.
- Weiterhin bestehen im Personalbereich **Kostenrisiken**, die durch höhere zu zahlendende Personalaufwendungen bestehen (neuere **Tarifverträge** etc.).
- Weiterhin ist bei Personal möglicherweise zu befürchten, dass dieses **nicht loyal** gegenüber dem Arbeitgeber sein könnte und so z. B. **Firmeninterna weitergetragen** werden könnten.
- Ein **Gesundheitsrisiko** ist im Personalbereich stets zu beachten.

© examio

1.5 Risikoquellen

- Als **Beschaffungsrisiken** sind zum Beispiel, aber nicht nur, **Preiserhöhungen** auf der Inputseite zu beachten.
- Weiterhin ist stets mit **Ausfall von Lieferanten** zu rechnen, d.h. man muss Vorsorge hierfür treffen, dass bestimmte Einsatzgüter, also bestimmte **Einsatzfaktoren nicht lieferbar** sind.
- Die Unternehmung muss sicherstellen, dass die **Produktionskette** des eigenen Gutes hierdurch **nicht gefährdet wird**, d.h. sie muss dafür sorgen, dass **hinreichende Alternativen** bestehen.
- Darüber hinaus sind **Lagerrisiken als auch Bestandsrisiken** zu beachten.

© examio

1.5 Risikoquellen

- **Technische Risiken** sind zum Beispiel der **technologische Wandel**.
- Wenn man **zu lange auf eine bestimmte Technologie** setzt
- Darüber hinaus ist stets mit **Ausfällen der eigenen Maschinen** zu rechnen, Alternativen hierfür müssen geschaffen werden.
- Darüber hinaus lässt sich zu den technischen Risiken die **Möglichkeit** eines **Katastrophenschadens** zählen.

1.5 Risikoquellen

- Im **Absatzbereich** ist es möglich, dass Kunden **Gewährleistungsansprüche** stellen, weil die Qualität
- der Produkte nicht hinreichend gut ist.
- Hierfür müssen dann **Rückstellungen gebildet** werden, wenn die Höhe und/oder Fälligkeit der zukünftigen Auszahlung im Jahr der wirtschaftlichen Verursachung nicht sicher ist.
- Weiterhin kann es sein, dass die **georderte Stückzahl nicht verfügbar** ist und Kunden deswegen unzufrieden werden.
- Außerdem muss bei Absatzrisiken stets eine **abschwächende Konjunktur** gefürchtet werden.

© examio

1.5 Risikoquellen

- Bei **Finanzierungsrisiken** sind zum Beispiel bestimmte **Refinanzierungsrisiken** zu beachten.
- Es könnte möglich sein, dass im schlimmsten Fall **Kredite durch Gläubiger** (also die Banken) **gekündigt** werden und man kurzfristig nicht an neue Kredite eingehen kann.
- Weiterhin kann es passieren, dass bei bestehenden Krediten, welche zu **variablen Zinssätzen** vereinbart waren, die Zinssätze zwischendurch ansteigen und insofern höhere Zinsaufwendungen von der Unternehmung zu leisten sind.
- Ebenso ist ggf. ein **Wechselkursrisiko** zu beachten, denn wenn eine **Forderung in einer fremden Währung** besteht.

© examio

1.5 Risikoquellen

- Weiterhin sind **Zahlungsrisiken** zu beachten, nämlich insbesondere
    - Zahlungsunwilligkeit bzw.
    - Zahlungsunfähigkeit

  von Kunden.
- Hieraus besteht die Verpflichtung, eine **Forderung außerplanmäßig abzuschreiben**, wenn mehr dafür als dagegen spricht, dass diese (teilweise) ausfällt.
- Dies erfolgt im Rahmen von **Einzelwertberichtigungen**, wobei auch zusätzlich **Pauschalwertberichtigungen** buchhalterisch beachtet werden müssen

© examio

1.5 Risikoquellen

- **Rechtlichen Risiken**
    - Risiken durch Schadenersatz,
    - durch Unfälle,
    - bei Verträgen,
    - durch Rechtsstreitigkeiten,
    - durch Strafen als auch
    - steuerliche Risiken

1.5 Risikoquellen

- **Schadensersatzverpflichtungen** können aus privatrechtlichen **Verträgen** bzw. aus **gesetzlichen Regelungen** heraus resultieren.
- Ansprüche des Kunden können erwachsen aus:
    - Gewährleistung, also einer gesetzlichen Verpflichtung des leistenden Unternehmens,
    - aus Garantieleistungen, also einer freiwilligen Verpflichtung und aus
    - Produkthaftung, also einer verschuldensunabhängigen gesetzlichen Verpflichtung

1.5 Risikoquellen

- **Unfälle**, speziell Arbeitsunfälle, führen zu Rechtsstreitigkeiten mit oft erheblichem finanziellem Ausmaß.
- Wichtig zur Vermeidung solcher Streitigkeiten bzw. zur Besserstellung des Unternehmens in diesen ist, dass man (im Vorhinein) die **notwendigen Sicherheitsvorkehrungen** trifft und diese auch lückenlos **dokumentiert**

1.5 Risikoquellen

- Bei **Vertragsrisiken** ist zu beachten, dass ein Vertrag nicht wirksam zustande gekommen sein könnte.
- Weiterhin könnten **schlecht gewählte Formulierungen** innerhalb des Vertrags zu unterschiedlichen **Interpretationen** der Vertragsbeteiligten und damit zu **rechtlichen Auseinandersetzungen** führen.
- Weiterhin könnte ein **Irrtum bei der Abgabe einer Willenserklärung** auf Seiten eines der beiden Vertragspartner außerdem die wirksame Abgabe eines Angebots über die wirksame Annahme des Angebots durch eine **fehlerhafte Stellvertretung** nicht möglich sein.

© examio

1.5 Risikoquellen

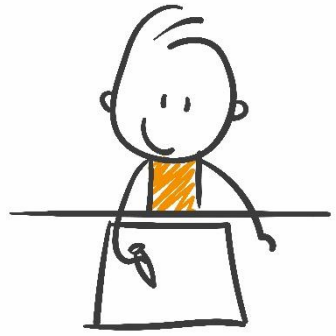
- **Rechtsstreitigkeiten** zählen klarerweise ebenfalls **zu den rechtlichen Risiken**.
- Der **Ausgang** einer Rechtsstreitigkeit, also eines Gerichtsverfahrens, ist **oftmals relativ unklar**.
- So muss, wenn man Beklagter in einem Verfahren ist und ein Verlust in der Zukunft droht, der wirtschaftlich in der Gegenwart verursacht wurde, eine **Rückstellung** hierfür gebildet werden.
- **Strafen** können bei **vertraglicher Vereinbarung** bzw. bei einer **Verwaltungsentscheidung** oder einer
- **gerichtlichen Entscheidung** entstehen.
- Hierbei wollen wir unter Strafen **auch Bußgelder für Ordnungswidrigkeiten** verstehen.

© examio

1.5 Risikoquellen

- Bei den **steuerlichen Risiken** könnte Ursache eine **fehlerhafte Rechtsauffassung** der beteiligten Personen im Unternehmen sein.

- **Datenrisiken**, bei diesen muss sichergestellt werden, dass **Diebstahl und Manipulation** wirksam verhindert werden.



1.5 Risikoquellen

- Beim **Datenverlust** ist zu sagen, dass Daten verloren gehen könnten, wodurch ein **erheblicher Schaden** für die Unternehmung ausgelöst werden könnte.
- Dies kann durch einen **technischen Defekt** passieren, aber auch durch **Katastrophen wie Brand** oder
- einen Stromschaden.
- Außerdem könnten **Bedienungsfehler** von Mitarbeitern Grund für Datenverlust sein.
- Ebenfalls aber könnten Daten absichtlich **gestohlen oder sabotiert** werden.

© examio

1.5 Risikoquellen

Fraud-Risiken

- Man versteht unter Fraud-Risiken **gesetzeswidrige Handlungen** wie **Betrug** bzw. Täuschung oder auch **Unterschlagung.**
- Unter **Täuschungen** versteht man bewusst **falsche Angaben**, aber auch Fälschungen einschließlich **Manipulationen**.
- **Unrichtigkeiten** sind hingegen **nicht beabsichtigte**, sondern unbeabsichtigt falsche Angaben. Diese können zum Beispiel entstehen, wenn ein **Sachverhalt falsch eingeschätzt** wird.

1.5 Risikoquellen

- Im Rahmen eines **Anti-Fraud-Managementsystems** soll nun den Fraud-Risiken, also den gesetzeswidrigen Handlungen, Einhalt geboten werden.
- Diese sollen **vermieden bzw. entdeckt** werden.
- Man unterscheidet hierbei
    - Fraud-Prevention,
    - Fraud-Auditing und
    - Fraud-Detection.

1.5 Risikoquellen

- **Fraud-Prevention** hat zur Aufgabe, das Eintreten gesetzeswidriger Handlungen **zu reduzieren**.
- Sog. **Fraud-Auditing** soll arglistige Handlungen **aufklären**. Für diese arglistigen (= dolosen) Handlungen müssen die **drei Bedingungen des sog. Fraud-Triangle erfüllt** sein, die im Rahmen der **Fraud-Detection** identifiziert werden:
    - ein **Motiv** muss vorhanden sein,
    - der Täter muss **Wissen und Wollen** der Tat haben und
    - die Möglichkeit zur **gesetzeswidrigen Handlung** muss an sich gegeben sein

© examio

2. Aufbau eines IKS

- Ein **Internes Kontrollsystem** soll unternehmerische Aktivitäten **überwachen** und bei möglichen **Schäden** dabei helfen, diese **rechtzeitig zu identifizieren**, damit **frühzeitig Gegenmaßnahmen** eingeleitet werden können.
- Da fast immer **mehrere Personen** aus den **unterschiedlichsten Bereichen** innerhalb einer Unternehmung abzustimmen sind, ergibt sich aus einem Internen Kontrollsystem die **Notwendigkeit der Abstimmung** zwischen den Beteiligten.

© examio

2.1 Rechtliche Grundlagen eines IKS

- **Ziele eines Internen Kontrollsystems** sind u. a., aber nicht nur,
  - die Zuverlässigkeit der Unternehmung als auch die **Vermeidung und Aufdeckung** von Fehlern im Betriebsablauf,
  - die Verhinderung von **Datenverlust**,
  - die **Zuverlässigkeit** der einzelnen Prozesse im Unternehmen und
  - die Einhaltung von (gesetzlichen) Vorschriften (= **Compliance**) zu sichern.

2.1 Rechtliche Grundlagen eines IKS

- Ein **Internes Kontrollsystem** kann niemals über alle Branchen, Unternehmen und Rechtsformen einheitlich aufgebaut werden, sondern ist vielmehr **abhängig von der Rechtsform** eines Unternehmens, seiner **Größe** als auch der **Komplexität der notwendigen Prozesse**.

© examio

2.1 Rechtliche Grundlagen eines IKS

- Ein explizites Gesetz für interne Kontrollsysteme gibt es nicht, vielmehr sind es **einzelne Paragraphen aus mehreren Gesetzen**, die den Aufbau eines IKS bestimmen. Darunter fallen unter anderem:
    - Regelungen aus dem HGB (§ 315 Abs. 2 HGB),
    - Regelungen aus dem AktG (§ 91 Abs. 2 AktG, § 93 I AktG, § 107 Abs. 3 AktG,
    - § 25a KWG.

2.1 Rechtliche Grundlagen eines IKS

- Steuerrechtliche Anforderungen
- BMF-Schreiben vom 28.11.2019: GoBD
- BMF-Schreiben vom 23.05.2016: Abgrenzung Berichtigung zur Steuerverkürzung, RZ 2.6:
- „Hat der Steuerpflichtige ein innerbetriebliches Kontrollsystem eingerichtet, das der Erfüllung der steuerlichen Pflichten dient, kann dies ggf. ein Indiz darstellen, das gegen das Vorliegen eines Vorsatzes oder der Leichtfertigkeit sprechen kann, jedoch befreit dies nicht von einer Prüfung des jeweiligen Einzelfalls.“

Exkulpation der Verantwortlichen

© examio

2.1 Rechtliche Grundlagen eines IKS

- **§ 315 II HGB** bezieht sich hingegen auf den **Konzernabschluss**, nicht auf den Einzelabschluss.
- Hiernach soll der **Konzernlagebericht** auf die Ziele des **Risikomanagements**, seine Methoden sowie auf **Preisänderungs- und Liquiditätsrisiken** sowie die Risiken aus möglichen **Zahlungsstromschwankungen** eingehen.

- Der **§ 91 II AktG** besagt, dass der **Vorstand** geeignete Maßnahmen zu treffen und insbesondere ein **Überwachungssystem** einzurichten hat. Das **GmbHG enthält keine** zum Aktiengesetz analogen **expliziten Regelungen** bezüglich eines Internen Kontrollsystems, aber § 43 GmbHG

© examio

2.1 Rechtliche Grundlagen eines IKS

- **§ 43 I GmbHG**: “Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden.“
- **§ 93 I AktG** verlangt implizit ein **angemessenes Risikomanagementsystem**, denn Vorstandsmitglieder müssen bei **unternehmerischen Entscheidungen** auf der Grundlage angemessener **Information** handeln.
- Hieraus erwächst die implizite Bedeutung eines „angemessen“ Risikomanagementsystems.

2.1 Rechtliche Grundlagen eines IKS

- **§ 107 III AktG** wiederum verpflichtet ein spezielles Organ der Aktiengesellschaft, nämlich den **Aufsichtsrat**, dazu, das **interne Kontrollsystem** als auch das **Risikomanagementsystem** sowie außerdem die Interne Revision zu **überwachen**.

2.1 Rechtliche Grundlagen eines IKS

- Gemäß § 25a KWG müssen **Kreditinstitute und Finanzinstitute** i. S. d. § 1 KWG ein **IKS** haben, bestehend aus:
    - einer klaren **Abgrenzung der Verantwortungsbereiche** in Bezug auf ablauf- und aufbauorganisatorische Regelungen
    - einem **Prozess zur Beurteilung, Steuerung, Kommunikation und Überwachung der Risiken**
    - einer **Risiko- und Controllingfunktion**.

2.1 Rechtliche Grundlagen eines IKS

- Mit Hilfe eines **Tax-Compliance-Managementsystems** (TCMS) sollen u.a. **folgende Risiken vermieden**, aber zumindest minimiert werden:
- **Geldbußen** für das Unternehmen (§§ 30, 130 OWiG),
- **Finanzielle Risiken** (z. B. Steuernachzahlungen, Hinterziehungs-zinsen, Verspätungszuschläge),
- **Strafrechtliche Risiken** und persönliche Haftung für Mitarbeiter (Mitwirkung an Steuerhinterziehung),
- **Geschäftsrisiken** (z. B. Ausschluss von öffentlichen Ausschreibungen),
- **schlechte Reputation**.

© examio

2.1 Rechtliche Grundlagen eines IKS

- Grundsatz der sog. **Totalreparation**, § 249 Abs. 1 BGB.
- Danach hat der Schädiger, unabhängig vom Grad seines Verschuldens und seiner persönlichen Leistungsfähigkeit, für den **gesamten angerichteten Schaden einzustehen**
- Ein **Vorstandsmitglied** trägt nach § 93 Abs. 2 S. 2 AktG die **Darlegungs- und Beweislast** nicht nur für fehlendes Verschulden, sondern auch für die fehlende Pflichtwidrigkeit seines Verhaltens
- Somit müssen Organmitglieder unter Umständen darlegen und beweisen, dass eine **zehn Jahre zurückliegende Geschäftsführungsmaßnahme** nicht pflichtwidrig gewesen ist

© examio

2.1 Rechtliche Grundlagen eines IKS

- Die **Aufsichtsräte sind verpflichtet** potenzielle Organhaftpflichtfälle zu prüfen, um eine rechtlich unangreifbare Entscheidung über eine Geltendmachung von Ansprüchen vorlegen zu können.
- Andernfalls kommen sie **selbst in die persönliche Haftung**, vgl. § 93 Abs. 2 AktG i.V.m. § 116 S. 1 AktG
- Für die **GmbH Geschäftsführung** leitet sich aus § 43 GmbHG die Haftung her

© examio

2.1 Rechtliche Grundlagen eines IKS

- **D&O-Versicherung** (directors' and officers' liability insurances)
- eine **Art Berufshaftpflichtversicherung**, die eingreift, wenn das Vorstands- oder Aufsichtsratsmitglied von der Gesellschaft oder von Dritten auf Schadensersatz in Anspruch genommen wird
- Trotzdem hat das **Organmitglied mindestens 10% des Schadens** bezogen auf jeden einzelnen Schadensfall **selbst zu tragen**, vgl. § 93 Abs. 2 S. 2 AktG.
- **Haftungsausschlüsse**, u.a. für vorsätzliche Schadensverursachung und wissentliche Pflichtverletzung

© examio

2.1 Rechtliche Grundlagen eines IKS

- Compliance ist erforderlich, da:
- 1. Die **Regelungsdichte steigt**. Immer mehr Sachverhalte sind durch immer kompliziertere Vorschriften.
- 2. Die **Risiken der Aufdeckung** von Regelverstößen sind hoch. Kronzeugenregelungen und Hinweisgebersystemen und zum anderen auch an der besseren Arbeit der Ermittlungsbehörden (z.B. Digitale Betriebsprüfung).
- 3. Die **Sanktionen sind erheblich** und werden weiter steigen.

© examio

2.1 Rechtliche Grundlagen eines IKS

- Auslagerung der Rechnungslegung, **IDW PS 331**
- Führt das Dienstleistungsunternehmen im Auftrag des zu prüfenden Unternehmens in bestimmten Bereichen der Rechnungslegung des zu prüfenden Unternehmens Vorgänge eigenständig durch,
- ist zwar das **Dienstleistungsunternehmen gegenüber** dem **zu prüfenden Unternehmen rechenschaftspflichtig**,
- die **Verantwortung** für die ausgelagerten Vorgänge **verbleibt jedoch bei dem** zu prüfenden **Unternehmen**.

© examio

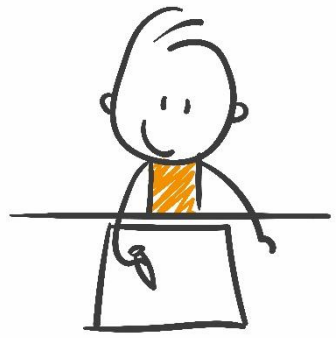
2.2 Verringern von Fehlerrisiken

- Um **Fehlerrisiken zu verringern**, muss das Management die **Verfahren, Maßnahmen und Grundsätze**, welche es im Unternehmen eingeführt hat, **fortwährend überprüfen**.
- Hierbei ist es wichtig, dass diese **Handlungen wirtschaftlich und ordnungsgemäß** sind.
- Ebenfalls gehört zu den Aufgaben eines Managers der **Vermögensschutz des Unternehmens**.

© examio

2.2 Verringern von Fehlerrisiken

- Wir beschreiben im Folgenden
  - die **Anforderungen an Abschlussprüfer** nach den Prüfungsstandards des Instituts der Wirtschaftsprüfer,
  - den **Inhalt eines Lageberichts**, den Kapitalgesellschaften erstellen müssen und
  - den **Umfang des Internen Kontrollsystems**.



2.2 Verringern von Fehlerrisiken

- Wir besprechen im folgenden
  - die Einteilung eines IKS in ein internes Steuerungssystem und ein internes Überwachungssystem,
  - die Anforderungen an den Abschlussprüfer nach IDW,
  - den IDW PS 210 und
  - den IDW PS 340

© examio

2.2 Verringern von Fehlerrisiken

- Regelungsbereiche eines IKS (vgl. Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW):

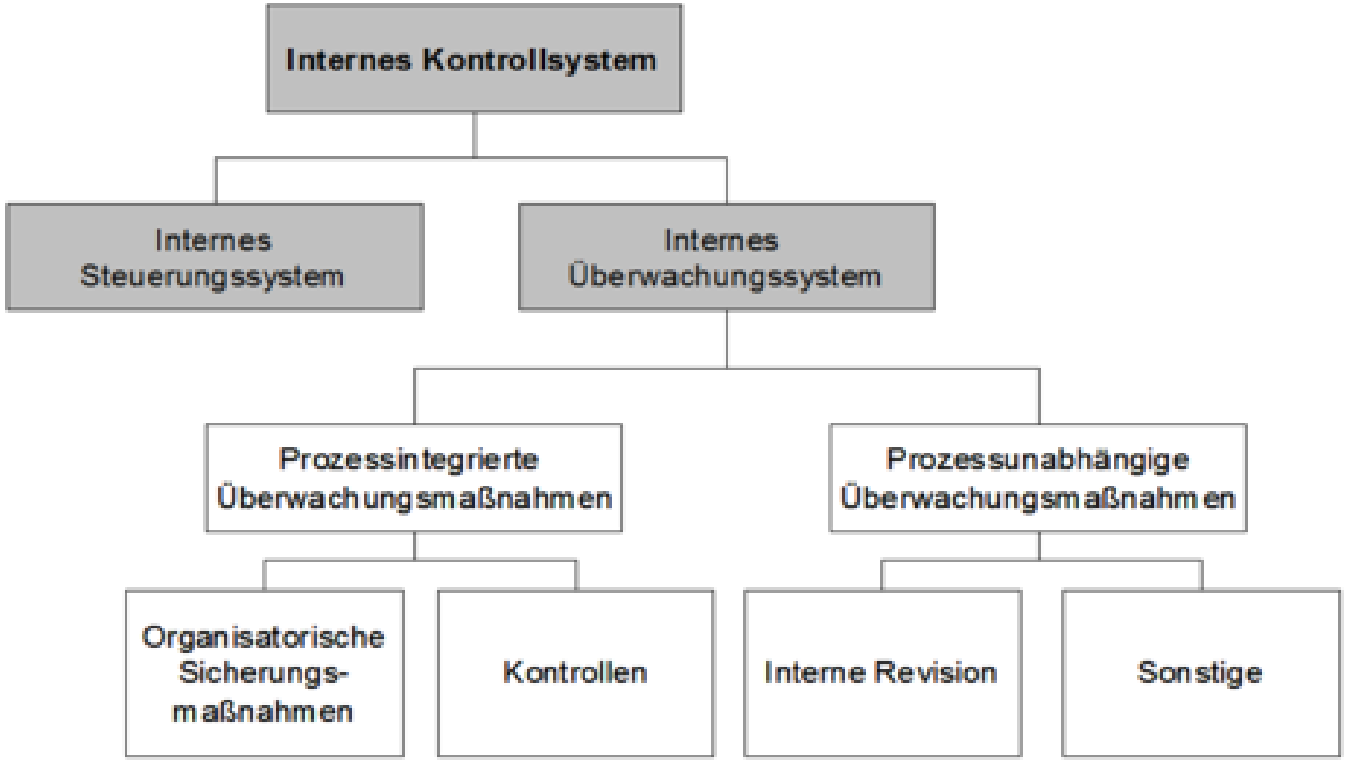
IDW Prüfungsstandard:

Feststellung und Beurteilung von Fehlerrisiken

und Reaktionen des Abschlussprüfers

auf die beurteilten Fehlerrisiken

(IDW PS 261), Tz. 20)



2.2 Verringern von Fehlerrisiken

- Das **IDW** hat in seinen **Standards** folgende **Anforderungen für den Abschlussprüfer** festgelegt:
  - Der Abschlussprüfer ist bei einer ordentlichen Abschlussprüfung **nicht verantwortlich für die Aufdeckung von Betrugsfällen** bzw. von Unregelmäßigkeiten.
  - Der Abschlussprüfer hat jedoch die **Prüfung aus Risikosicht so durchzuführen**, dass mit **hinreichender Sicherheit** Unregelmäßigkeiten **aufgedeckt** werden können.
  - Falls es **Hinweise oder Ausgangspunkte** gibt, die auf einen Betrugsfall oder Unregelmäßigkeiten deuten, **muss der Abschlussprüfer diese Hinweise prüfen**.

2.2 Verringern von Fehlerrisiken

- Der **Umfang der Abschlussprüfung** beinhaltet lediglich **den Nachgang zu Unregelmäßigkeiten** bzw. Betrugsfällen, die die Rechnungslegung beeinflussen.
- Hieraus ergeben sich besondere **Mitteilungspflichten für den Abschlussprüfer**
- Er hat außerdem spezielle Prüfungshandlungen **zur Aufdeckung von Fraud-Risiken** durchzuführen und die **Anwendungen des IKS** im Unternehmen **zu kontrollieren**.

© examio

2.2 Verringern von Fehlerrisiken

- Bei der Prüfung des Jahresabschlusses muss der Abschlussprüfer das **Risikofrüherkennungssystem** als auch die Umsetzung der **Vorschriften zum Risikomanagement** in seine abzuleistende **Prüfung einbeziehen** (§ 317 Abs. 4 HGB).
- Im Falle von **Aktiengesellschaften**, muss der Wirtschaftsprüfer die **Effizienz** und also die **Funktionsfähigkeit des Risikofrüherkennungssystems** attestieren.
- Ein Risikofrüherkennungssystem hat demgemäß zur Aufgabe, zu **verhindern**, dass Rechtsvorschriften verletzt werden, welche die **Ordnungsmäßigkeit des Jahresabschlusses gefährden** könnten (§ 317 Abs. 2 S. 2 HGB).
- Im Bestätigungsvermerk ist das **Ergebnis der Prüfung** festzuhalten (§ 323 HGB).

© examio

2.2 Verringern von Fehlerrisiken

- Der Prüfungsstandard **IDW PS 210** hat Unregelmäßigkeiten zum Inhalt.
- Diese lauten dort wie folgt:
    - **Unrichtigkeiten** (Error)
        - Bei Error handelt es sich um **fahrlässig verursachte Fehler** wie z. B. das **Vertippen** bei der Buchführung oder **unwissentlich falsche Anwendung** von Buchführungsvorschriften (diese Fehler können Auswirkungen auf den Bestätigungsvermerk und den Prüfungsbericht haben

2.2 Verringern von Fehlerrisiken

- Der Prüfungsstandard **IDW PS 210** hat Unregelmäßigkeiten zum Inhalt.
- Diese lauten dort wie folgt:
    - **Verstöße (Fraud)**
        - **Vorsätzliche Fehler** bei der Buchhaltung bzw. Rechnungslegung, die zu einem falschen Jahresabschluss bzw. Lagebericht führen. (Diese haben ebenfalls Auswirkungen auf den Bestätigungsvermerk und dem Prüfungsbericht)

2.2 Verringern von Fehlerrisiken

- Der Prüfungsstandard **IDW PS 210** hat Unregelmäßigkeiten zum Inhalt.
- Diese lauten dort wie folgt:
    - **sonstige Gesetzesverstöße**
        - alle **vorsätzlich oder fahrlässig verursachte Fehler** durch Mitarbeiter oder Vertretungsorgane, die **gegen Gesetze oder Satzungen verstoßen**, aber keine Auswirkung auf den Jahresabschluss bzw. die Rechnungslegung haben (sonstige Gesetzesverstöße haben **keine Auswirkung auf den Bestätigungsvermerk**, müssen **jedoch** gegebenenfalls **im Prüfungsbericht vermerkt** werden.

2.2 Verringern von Fehlerrisiken

- Zur **Beurteilung des Risikomanagementsystems** hat das Institut der Wirtschaftsprüfer schließlich den Prüfungsstandard **IDW PS 340** festgelegt.
- Die notwendigen Elemente eines **Risikofrüherkennungs- und Überwachungssystems** sind im IDW PS 340 festgelegt.
- Hiernach versteht man unter **Risikomanagement** „die Gesamtheit **aller organisatorischen Regelungen und Maßnahmen** zur **Risikoerkennung** und zum **Umgang mit Risiken** unternehmerischer Betätigung“

2.2 Verringern von Fehlerrisiken

- Die Elemente des IDW PS 340 sind:
  - Dokumentation
  - Einrichtung eines Überwachungssystems
  - Kommunikation des Risikos
  - Festlegen bestandsgefährdender Risiken als auch der Risikofelder
  - Risikoerkennung und Risikoanalyse
  - Zuordnung von Verantwortlichkeiten und Aufgabenbereichen.

© examio

2.2 Verringern von Fehlerrisiken

- Die Elemente des IDW PS 340 sind:
- Die **Dokumentation** soll durch ein **Risikohandbuch** als auch durch die Archivierung der relevanten Dokumente ermöglicht werden.
- Im Nachhinein sollen dadurch die getroffenen **Maßnahmen** stets **nachvollzogen werden können**.

© examio

2.2 Verringern von Fehlerrisiken

- Die **Einrichtung eines Überwachungssystems** bedeutet, dass interne als auch **externe Prüfer** und
- Berater **einbezogen** werden können.
- Die **Kommunikation** des Risikos funktioniert dadurch, dass **Berichtswege und -abläufe festgelegt** werden und außerdem bestimmt wird, ab welchen kritischen Werten **Sofortmitteilungen** herausgegeben werden. **Verantwortlichkeiten und Aufgabenbereiche** müssen **zugeordnet** werden, damit müssen **verantwortliche Mitarbeiter** für die jeweilige **Steuerung der einzelnen Risiken** benannt sein.
- **Unternehmen** müssen für alle Bereiche **interne und externe Risiken bestimmen**.

© examio

2.2 Verringern von Fehlerrisiken

- Ein Internes Kontrollsystem setzt sich aus **zwei Hauptkomponenten** zusammen, zum einen
    - aus einem **internen Steuerungssystem** und zum anderen
    - aus einem **internen Überwachungssystem**.
- Für den **Aufbau eines IKS** und die **Anforderungen** an ein IKS gibt es **verschiedene Quellen** bzw. Richtlinien und Rahmenwerke, z. B. das international etablierte "**Internal Control Framework - COSO** „
- ergänzt um COSO II "Enterprise Risk Management – Integrated Framework" sowie den **IDW PS 261**.

2.2 Verringern von Fehlerrisiken

- Der Report nach **COSO** setzt sich aus **vier Bestandteilen** zusammen,
- im ersten Teil wird eine **Zusammenfassung der Untersuchungen** erstellt (Executive Summary).
- Der zweite Teil umfasst die **Integration eines IKS** im Unternehmen, welches auf den individuellen Kontrollbedarf des Unternehmens abgestimmt ist und die **Systemeinschätzungen** beinhaltet (**Framework**).
- **Reporting to External Parties** ist der dritte Teil des COSO-Reports und dient zur **externen Berichterstattung** des Unternehmens.
- Der letzte Teil **Evaluation Tools** umfasst die **Darstellung von Werkzeugen**, um das IKS zu verstärken.

© examio

2.2 Verringern von Fehlerrisiken

IDW PS 980

- Der PS 980 hat das Ziel einer umfassenden Wirksamkeitsprüfung, ob die in der **Tax CMS-Beschreibung** enthaltenen Aussagen über die Grundsätze und Maßnahmen des Tax CMS in allen **wesentlichen Belangen** angemessen dargestellt sind, dass die dargestellten Grundsätze und Maßnahmen **Risiken** für wesentliche Regelverstöße **rechtzeitig erkennen** als auch solche **Regelverstöße verhindern** können, dass die Grundsätze und Maßnahmen zu einem bestimmten Zeitpunkt implementiert waren und auch während des Prüfungszeitraums wirksam waren.

© examio

2.2 Verringern von Fehlerrisiken

- Der PS 980 dient nur zur Orientierung und definiert sieben Schritte zum Tax-CMS
- 1) Tax Compliance-Kultur,
- 2) Tax Compliance-Ziele,
- 3) Tax Compliance-Organisation,
- 4) Tax Compliance-Risiken,
- 5) Tax Compliance-Programm,
- 6) Tax Compliance-Kommunikation,
- 7) Tax Compliance-Überwachung und Verbesserung

© examio

2.2 Verringern von Fehlerrisiken

- Empfehlung zur Gestaltung eines IKS:
- Die Gestaltung eines Internen Kontrollsystems besteht aus **drei Phasen**:
    - Planung und Konzeption,
    - Prozessaufnahme, Implementierung und Dokumentation und schließlich
    - Überwachung und Planung

© examio

2.2 Verringern von Fehlerrisiken

- Bei der **Planung und Konzeption** ist erst zu beurteilen, **welche Ziele die Führungsebene** mit der Implementierung eines IKS bezwecken möchte und **welcher Umfang** daraus resultiert.
- Wichtig ist, dass bei der Planung eines IKS das **Führungsorgan die Wichtigkeit** eines solchen Systems **verstanden hat** und dieses **mit voller Überzeugung unterstützt** („Management-Support“).

© examio

2.2 Verringern von Fehlerrisiken

- In erster Linie muss man sich in der **Planungsphase** ein **Bild über die Organisation** des Unternehmens machen.
- Dies kann durch die **Befragung der Führungsebene** und durch eine Checkliste mit den wichtigsten Strukturen des Unternehmens erfolgen.
- Während der Konzeption und Planung werden die **wesentlichen Risikomerkmale** eines Unternehmens für die angepasste Erstellung eines IKS **konkretisiert**.

© examio

2.3 Risikofrüherkennungssystem

- Durch das **Gesetz zur Kontrolle und Transparenz** im Unternehmensbereich (**KonTraG**) wurde die **Haftung und die Sorgfaltspflicht** für den Vorstand oder die Geschäftsführung sowie des Aufsichtsrates eines Unternehmens im AktG und GmbHG erweitert.
- Hierdurch haben diese **Organe die Verpflichtung**, ein **Risikofrüherkennungssystem** zu implementieren gem. § 91 Abs. 2 AktG, § 116 AktG und dem § 43 Abs. 1 GmbHG.
- Des weiteren müssen **eventuelle Risiken im Lagebericht** erwähnt werden und der **Abschlussprüfer** hat die Risiken **zu überprüfen**.

© examio

2.3 Risikofrüherkennungssystem

- Die **erweiterten Pflichten des Abschlussprüfers** erstrecken sich nach dem KonTraG auf:
  - **Risikobewusstsein** innerhalb der verschiedenen **Abteilungen und Hierarchien** in einem Unternehmen
  - **Risikoerkennung** durch Abteilungen wie die Interne Revision, Controlling, usw.
  - **Risikovermeidung** durch Dokumentation, Überwachung, usw.

2.3 Risikofrüherkennungssystem

- Die **Mindestanforderungen** an ein Risikofrüherkennungssystem umfassen:
  - **Sollkonzepte** für alle Ebenen, zur Frühaufdeckung von Risiken (**Transparenzprinzip**)
  - Jeden betrieblichen Vorgang einer **Gegenkontrolle** unterziehen (**Vier-Augen-Prinzip**)
  - betriebliche **Vorgänge voneinander trennen** (**Funktionstrennung**)
  - die wichtigen bzw. notwendigen **Informationen an die Mitarbeiter** mitteilen (**Mindestinformationen**)

2.4 Kontrollbereiche des IKS

- Man unterscheidet in Theorie und Praxis üblicherweise zwischen
    - Aufbau- und
    - Ablauforganisation.
- In der Aufbauorganisation werden
    - Teilaufgaben zusammengefasst
    - Sachmittel eingesetzt
    - und Stellen verbunden.

© examio

2.4 Kontrollbereiche des IKS

- Die Aufbauorganisation hat bezüglich eines Internen Kontrollsystems Bedeutung durch
  - Delegation
  - Spezialisierung
  - Koordinationsformen und bezüglich eines
  - Organigramms.

2.4 Kontrollbereiche des IKS

- Durch **Delegation** wird die **Motivation** als auch das **Risikoverhalten** der mit einer Aufgabe betrauten Person deutlich **gesteigert**.
- Nachteilig ist die Spezialisierung, denn die **Wahrnehmung** von Risiken **könnte beeinträchtigt werden**, je **spezialisierter Mitarbeiter** sind, d.h. insb. je geringer ihr Aufgabenbereich ist.
- Bezüglich der **Koordinationsformen** ist zu sagen, dass **durch die Dezentralisierung** die **Wahrnehmung** von Risiken **gefördert** wird, denn einzelne Mitarbeiter können die Wege der **Kommunikation selbst beeinflussen** und selbst aktiv nutzen.
- Mögliche **Risiken** lassen sich schließlich in einem **Organigramm leichter erkennen**, denn kritische Stellen in der Kommunikation lassen sich dadurch leichter identifizieren.

© examio

2.4 Kontrollbereiche des IKS

- Bezüglich der **Ablauforganisation** mit Bezug auf ein Internes Kontrollsystem ist zu sagen, dass **Prozessabläufe**, welche wesentlichen Einfluss auf die Effektivität des Risikomanagementsystems haben, **dargestellt** werden müssen,
- außerdem die **Geschäftsabläufe**, welche wesentliche Risiken enthalten, benannt werden müssen.
- **Zwischen den Teilprozessen** müssen ausreichende **Zwischenkontrollen** etabliert werden und **Datensicherheit** muss gewährleistet sein.
- Schlussendlich müssen die **Verantwortlichkeiten zwischen den Schnittstellen** klar zugeordnet werden, Verantwortlichkeiten dürfen innerhalb der Ablauforganisation nicht verwischt werden.

© examio

3.1 Kontrollaktivitäten

- Kontrollaktivitäten sind **in allen Bereichen** eines Unternehmens durchzuführen und sollen dazu beitragen, dass ggf. **Risiken entgegengewirkt** bzw. ihnen **vorgebeugt** wird.
- In der Regel bestehen Kontrollaktivitäten aus **zwei Elementen**:
    - Bestimmungen über die **Soll-Vorgaben,**
    - Verfahren zur **Ausführung** der Bestimmungen

3.1 Kontrollaktivitäten

- Zu den häufigsten und wichtigsten Kontrollaktivitäten gehören:
  - manuelle oder automatische
  - präventive oder detektive
  - primäre oder sekundäre
  - Routinekontrollen oder Nicht-Routinekontrollen
  - Kontrollen auf Unternehmensebene oder Prozessebene

© examio

3.2 Information und Kommunikation

- **Information und Kommunikation** ist eine **Komponente des COSO-Modells**, welche Einfluss auf alle anderen Komponenten hat.
- Diese Komponente dient zur **Entscheidungsbildung auf Managementebene**.
- Die Manager leiten danach die notwendigen **Informationen an die zuständigen Mitarbeiter** weiter.
- Zu den notwendigen Informationen gehören auch die für eine wesentliche **Risikobeurteilung** notwendigen Informationen sowie die **Zuständigkeit für das IKS** einzelner Mitarbeiter.
- **Informationen** müssen nicht zwingend mündlich erteilt werden, diese können auch anhand von **Richtlinien**, Notizbüchern oder **Organisationshandbüchern kommuniziert** werden.

© examio

3.3 Überwachungsaktivitäten

- Das COSO-Regelwerk ist auf die Unternehmensziele fokussiert und besteht aus unterschiedlichen Elementen:
    - Kontrollumfeld
    - Risikobeurteilung
    - Kontrollaktivitäten und
    - Information und Kommunikation.

3.3 Überwachungsaktivitäten

- Das **Kontrollumfeld** ist stark **durch das Unternehmensleitbild definiert**, es wird also beeinflusst durch **Verhaltensregeln, Leistungsvorgaben** und die Rolle, welche Aufsichtsorgane innerhalb des Unternehmens ausüben.
- Die Risikobeurteilung erfolgt durch
    - die Analyse der Zielsetzung,
    - die Identifikation von Risiken,
    - die Risikocharakteristiken und durch
    - Maßnahmen.

© examio

3.3 Überwachungsaktivitäten

- Zunächst ist es für die **Risikobeurteilung wichtig**, welche **Ziele das Unternehmen folgt**.
- Die **Identifikation von Risiken** ist abhängig von den **Märkten**, in denen sich das Unternehmen bewegt, der jeweiligen **Branche**, den jeweiligen produzierten und verkauften **Produkten** als auch den **Unternehmensprozessen**.
- **Risikocharakteristik** bedeutet, dass man die **möglichen Schäden** und ihre **Eintrittswahrscheinlichkeiten** ermitteln kann, um hieraus aus der **Erwartungswertberechnung** den erwarteten Schaden kalkulieren zu können.
- Schließlich ist es von **Risikoaversion bzw. Risikopräferenz** der Unternehmensbeteiligten abhängig, ob und **welche Maßnahmen** im Rahmen der Risikobeurteilung **getroffen werden**.

© examio

3.3 Überwachungsaktivitäten

- Ein **Internes Kontrollsystem** umfasst insbesondere auch **Überwachungsaktivitäten**, um sicherzustellen dass **rechtlichen Anforderungen** genüge getan wird, **Schwachstellen erkannt** und **Verbesserungen entwickelt** werden können.
- Bei den **Überwachungsmaßnahmen** unterscheiden wir
    - prozessunabhängige und
    - prozessabhängige Überwachungsmaßnahmen.

© examio

3.3 Überwachungsaktivitäten

- Die **prozessunabhängigen Überwachungsmaßnahmen** sollen die Wirtschaftlichkeit der Überwachung sicherstellen und Verbesserungspotenziale aufzeigen.
- **Prozessunabhängig** agieren beispielsweise die **Interne Revision** und der **Abschlussprüfer**, aber auch Organe von Kapitalgesellschaften wie beispielsweise der **Aufsichtsrat**.
- **Prozessabhängige** Überwachungsmaßnahmen hingegen werden durch **einzelne Stellen realisiert**, welche Teil des Risikomanagements sind.

© examio

3.3 Überwachungsaktivitäten

- Die **Beurteilung des Aufbaus eines IKS** ist in den meisten Fällen subjektiv, jedoch kann die Prüfung durch einige Schritte objektiviert werden.
- Ein **Indiz für einen schlechten Aufbau** könnten z. B. **fehlende oder unzureichende Kontrollaktivitäten** sein.

© examio

3.3 Überwachungsaktivitäten

- Um den Aufbau eines IKS objektiv bewerten zu können, sind folgende **Prüfungshandlungen** möglich:
  - Mitarbeiterbefragungen mit Überwachungsfunktionen
  - Beurteilung von Arbeitsabläufen und der IT-Strukturen
  - Kontrolle von Unternehmensrichtlinien oder Organisationshandbüchern usw.
  - Dokumente des IKS kontrollieren
  - die Kontrollaktivitäten nach ihrer Wesentlichkeit und Wirksamkeit beurteilen

© examio

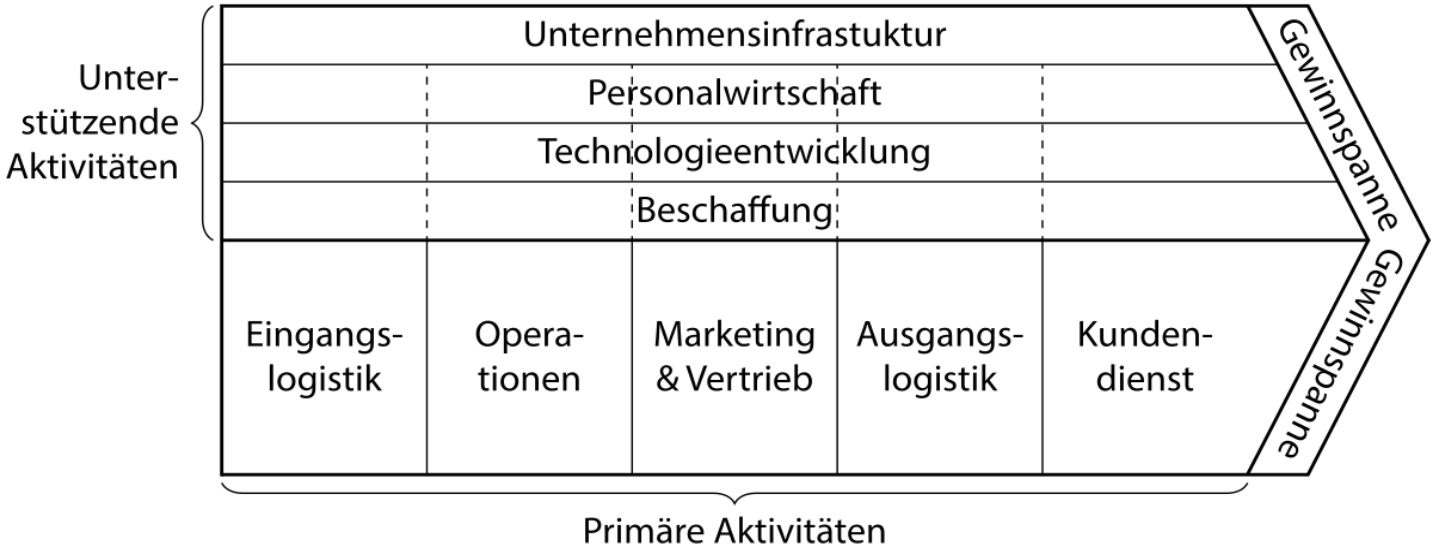
4.1 Prozessorganisation und Risiko-Kontroll-Matrix

- Bei der **Prozessorganisation** unterscheiden wir bei **Maßnahmen zur Vermeidung von Risiken** die sog.
    - Kernprozesse (= primäre Prozesse) und
    - unterstützende (= sekundäre) Prozesse.
- Die **Kernprozesse** sind **Wertschöpfungsprozesse des Unternehmens** und haben einen unmittelbaren Bezug zum Produkt, welche das Unternehmen verkauft.
- **Unterstützende Prozesse** hingegen tragen lediglich **indirekt zur Wertschöpfung** bei.
- Sie haben zwar Bedeutung für einen sicheren Ablauf der Kernprozesse, haben allerdings für sich **keinen unmittelbaren Kundennutzen.**

© examio

4.1 Prozessorganisation und Risiko-Kontroll-Matrix

- Wir beziehen uns hier insg. auf die **Wertschöpfungskette nach Porter**.
- In ihr soll ein **marktfähiges Produkt erstellt** werden, so dass der Verkaufswert größer ist als die gesamten Einstandskosten der kompletten Produktionsfaktoren.



4.1 Prozessorganisation und Risiko-Kontroll-Matrix

- Eine **Risiko-Kontroll-Matrix** dient dazu, **Risiken systematisch darzustellen**.
- Je komplexer das Unternehmen ist, umso komplexer ist auch die Risiko-Kontroll-Matrix.
- Wichtig ist, dass **für einzelne Teilprozesse** auch **unterschiedliche Risiko-Kontroll-Matrizen** angefertigt werden können.
- Eine Risiko-Kontroll-Matrix sollte **in tabellarischer Form** erstellt werden, hier sind die **Ziele** und die **Funktionen zu beschreiben**.
- Des weiteren sollte erfasst werden, wer **die Kontrollen durchführt** und in welcher **Häufigkeit** diese stattfinden.
- Die **Dokumentation der Kontrollen** ist ebenfalls wichtig für eine funktionsfähige Risiko-Kontroll-Matrix.

© examio

4.1 Prozessorganisation und Risiko-Kontroll-Matrix

Verbindung von Prozessinformationen mit Risiken und Schlüsselkontrollen

4.1 Prozessorganisation und Risiko-Kontroll-Matrix

- **Missbrauchsindikatoren (Fraud-Indikatoren)** umfassen als Oberbegriff jede **vorsätzliche und rechtwidrige Handlung** oder schuldhaftes Verhalten, die durch Manager oder durch Mitarbeiter ausgeführt worden sind.
- Ziel eines **funktionierenden IKS** ist es, Fraud, also gesetzeswidrigem Verhalten, **vorzubeugen**, da betrügerisches Verhalten dem Unternehmen großen Schaden zufügen kann.

© examio

4.1 Prozessorganisation und Risiko-Kontroll-Matrix

- Missbrauch kann in **drei Kategorien** unterteilt werden:
    - Management-Fraud:
        - der Manager stellt das Unternehmen besser dar als es ist, um bessere Leistungen vom Unternehmen zu erhalten wie z. B. Höhere Prämien oder größere Boni.
    - Mitarbeiter-Fraud:
        - Mitarbeiter fälschen Kassenbelege, um z. B. Geld zu unterschlagen.
    - Begünstigung Dritter:
        - hier wird Dritten dazu verholfen, Leistungen vom Unternehmen zu erhalten, die ungerechtfertigt sind.

4.3 Relevante Kennzahlen

- Folgende Kennzahlen bzw. Gruppen von Kennzahlen sind besonders relevant in einem Internen Kontrollsystem:
    - Value at Risk, ermittelt durch
        - Varianz-Kovarianz-Modelle
        - historische Simulation
        - Monte-Carlo-Simulation
    - Ausbuchungsquoten
    - Debitorenkennzahlen
    - Kennzahlen zum Wareneinsatz

4.3 Relevante Kennzahlen

- Durch den **Value at Risk** wird **innerhalb eines bestimmten Zeitraums** bei einem gegebenen Konfidenzniveau der **höchste erwartete Verlust** unter weiteren Bedingungen **berechnet**.
- Es handelt sich damit um ein **Risikomaß**, welches unter anderem häufig im Finanzbereich angewendet wird.
- Wichtige Ermittlungsmethoden zur Berechnung des Value at Risk sind
    - die Varianz-Kovarianzmodelle,
    - die historische Simulation und
    - die Monte Carlo Simulation.

4.3 Relevante Kennzahlen

- In den **Varianz-Kovarianzmodellen** (= Delta-Normal-Ansätzen) ermittelt man die **Wahrscheinlichkeit eines Risikos mit einer Normalverteilung**, welche wegen des zentralen Grenzwertsatzes oftmals für in Wahrheit andere richtige Verteilungen angenommen werden kann.
- Bei der **historischen Simulation** hingegen bedient man sich **Daten der Vergangenheit**.
- Diese werden durch Simulation **auf die aktuelle Situation übertragen**.
- Problematisch ist hieran allerdings, dass **man unterstellt**, dass das, was in der **Vergangenheit risikoreich** war, **auch in der Gegenwart** und in der Zukunft in gleicher Art und Weise risikoreich sein wird

© examio

4.3 Relevante Kennzahlen

- Schließlich geht es in der **Monte-Carlo-Simulation** darum, computergestützt und mit einer großen Zahl von **Simulationsläufen** jeweils **Risiken und deren Verteilungen** zu bestimmen.
- Wenn die Zahl von Simulationen hinreichend groß ist, können dadurch Risiken des Unternehmens besser abgeschätzt werden.

4.3 Relevante Kennzahlen

- Bei den **Ausbuchungsquoten** geht es darum, dass **Forderungen** zu eliminieren (= auszubuchen) sind, wenn und sobald sie **vollständig bezahlt** wurden.
- Werden sie **ganz oder teilweise nicht bezahlt**, so wird eine entsprechende **außerplanmäßige Abschreibung** (= Wertberichtigung) vorgenommen. Dies erfolgt nach dem strengen Niederstwertprinzip des § 253 Abs. 4 HGB.
- Bei den Debitorenkennzahlen reden wir über das
    - Debitorenziel (bzw. Debitorenlaufzeit) und den
    - Debitorenumschlag.

© examio

4.3 Relevante Kennzahlen

- **Debitorenziel** = Durchschnittlicher Forderungsbestand * 360/Umsatz

  Je höher der durchschnittliche Forderungsbestand, desto schlechter ist die Kennzahl.

- **Debitorenumschlag** = Umsatzerlöse / durchschnittlichen Debitorenbestand

  Ein Rückgang, wäre negativ zu werten, da die Kapitalbindung in den Forderungen damit zunimmt.

4.3 Relevante Kennzahlen

- Wir unterscheiden bei den Kennzahlen zum **Wareneinsatz** den
    - Wareneinsatz selbst,
    - die Wareneinsatzquote (= Wareneinsatz/Gesamtumsatz),
    - die Materialaufwandsquote (= Materialaufwand/Gesamtleistung),
    - Rohertrag (= Umsatzerlöse – Wareneinsatz) und
    - die Rohertragsquote (= Rohertrag/Betriebsleistung).

© examio

4.3 Relevante Kennzahlen

- Weitere Kennzahlen:
    - Personalrisiken (z.B. Fluktuationsrate oder die Ausfallzeiten)
    - technische Risiken (Stillstandquote),
    - Risiken des Anlagevermögens (Schadensfälle),
    - Absatzrisiken (Auftragsreichweite),
    - Zahlungsrisiken (Ausfallquote, Bonität der Kunden) und
    - Finanzierungsrisiken (Fremdkapitalquote oder Verschuldungsgrad).

5.1 TAX-CMS

- Tax Compliance = „Steuerehrlichkeit“
- Implementierung und Pflege eines Systems zur Sicherstellung der steuerlichen Rahmenbedingungen (Gesetze, Richtlinien und Rechtsprechung)
- Aber auch die daraus abgeleiteten Rechte

5.1 TAX-CMS

- Tax Compliance: BMF-Schreiben vom 23.5.2016
- Rz. 2.6: „Hat der Steuerpflichtige ein **innerbetriebliches Kontrollsystem** eingerichtet, das der Erfüllung der steuerlichen Pflichten dient, kann dies ggf. **ein Indiz darstellen**, das **gegen** das Vorliegen eines **Vorsatzes oder der Leichtfertigkeit** sprechen kann, jedoch befreit dies nicht von einer Prüfung des jeweiligen Einzelfalls.“

5.1 TAX-CMS

- Tax Compliance: BMF-Schreiben vom 23.5.2016
- Interpretation:
- …das System muss risikobehaftete **Sachverhalte beschreiben**,
- …das System muss dahingehend den **Prozess beschreiben**,
- …das System muss die entsprechenden **Kontrollen beschreiben**,
- …das System muss diese Informationen **versioniert vorhalten**,
- …das System muss **verschriftete Kontrollen** vorhalten,
- …das System muss **aktuell** sein.

© examio

5.1 TAX-CMS

- Der PS 980 (IDW) hat das Ziel einer umfassenden **Wirksamkeitsprüfung**,
- ob die in der Tax CMS-Beschreibung **enthaltenen Aussagen** über die Grundsätze und Maßnahmen des Tax CMS in allen wesentlichen Belangen angemessen dargestellt sind,
- dass die dargestellten Grundsätze und Maßnahmen **Risiken für wesentliche Regelverstöße** rechtzeitig **erkennen** als auch solche Regelverstöße **verhindern** können,
- dass die Grundsätze und Maßnahmen **zu einem bestimmten Zeitpunkt implementiert** waren und
- auch während des Prüfungszeitraums **wirksam** waren.

© examio

5.1 TAX-CMS

RACI Modell

- **Responsible** = Durchführungsverantwortung, zuständig für die eigentliche Durchführung – z.B. Kreditorenbuchhalter
- **Accountable** = rechenschaftspflichtig (Kosten-, bzw. Gesamtverantwortung), verantwortlich im Sinne von „genehmigen“, „billigen“ oder „unterschreiben“ – z.B. Teamleitung
- **Consulted** = konsultiert. Eine Person, die in der Regel nicht direkt an der Umsetzung beteiligt ist, aber relevante Informationen für die Umsetzung hat – z.B. Leitung der Steuerabteilung
- **Informed** = zu informieren (Informationsrecht). – z.B. Geschäftsführung

© examio

5.2 Aufgaben und Lösungen

- 1) Stellen Sie Maßnahmen zur Erstellung eines Internen Kontrollsystems bezogen auf Gewährleistungen dar.
- Lösung: Maßnahmen zur Erstellung eines Internen Kontrollsystems sind zum Beispiel, aber nicht nur,
    - Analyse der Gewährleistungsfälle
        - Erfassung,
        - Dokumentation,
        - Auswertung
    - Einholung zusätzlicher Informationen und
    - Einrichtung von Reporting-Standards.

5.2 Aufgaben und Lösungen

- Gewährleistungsfälle müssen **erfasst und dokumentiert** werden, und zwar zunächst durch das Rechnungswesen. Es ist hierbei insbesondere nämlich fraglich, ob eine **Rückstellung** für ungewisse Verbindlichkeiten (für Rückstellungen für Gewährleistungen mit rechtlicher Verpflichtung) oder Rückstellungen für Gewährleistungen ohne rechtliche Verpflichtung (die sog. Kulanzrückstellung), gebildet werden.
- Eine **Qualitätssicherungsabteilung** muss den Grund, welcher zu dem Gewährleistungsfall geführt hat, auswerten und analysieren, was aus dem Fehler gelernt werden kann.
- Wichtig ist, dass Gewährleistungsfälle innerhalb einer relativ kurzen Zeit **nach Bekanntwerden erfasst und ausgewertet** werden.

© examio

5.2 Aufgaben und Lösungen

- 2) Was sind die Anforderungen an den Abschlussprüfer nach IDW?
- Lösung: Der Abschlussprüfer hat die Prüfung aus Risikosicht so durchzuführen, dass mit höchstwahrscheinlich **Unregelmäßigkeiten aufgedeckt** werden können.
- Falls es **Hinweise** oder Ausgangspunkte gibt, die auf einen Betrugsfall oder Unregelmäßigkeiten deuten, muss der Abschlussprüfer diese Hinweise **prüfen**.
- Der Umfang der Abschlussprüfung beinhaltet lediglich den **Nachgang zu Unregelmäßigkeiten** bzw. Betrugsfällen, die die Rechnungslegung beeinflussen.
- Hieraus ergeben sich besondere **Mitteilungspflichten** für den Abschlussprüfer.

© examio

5.2 Aufgaben und Lösungen

- 3) Wie ist das Interne Kontrollsystem im HGB verankert?
- Lösung: Der **§ 289 Abs. 2 HGB** verpflichtet speziell **kapitalmarktorientierte Kapitalgesellschaft** dazu, die einzelnen **Bestandteile eines Internen Kontrollsystems**, welche rechnungslegungsbezogen sind, in ihrem Lagebericht **darzustellen**.
- Der **§ 315 Abs. 2 HGB** bezieht sich hingegen auf den **Konzernabschluss**, nicht auf den Einzelabschluss.
- Hiernach soll der Konzernlagebericht auf die **Ziele des Risikomanagements**, seine Methoden sowie auf **Preisänderungs- und Liquiditätsrisiken** sowie die Risiken aus möglichen **Zahlungsstromschwankungen** eingehen.

© examio

5.2 Aufgaben und Lösungen

- 4) Nennen Sie die Elemente des IDW PS 340.
- Lösung: Die Elemente des IDW PS 340 sind
    - Dokumentation,
    - Einrichtung eines Überwachungssystems,
    - Kommunikation des Risikos,
    - Festlegen bestandsgefährdender Risiken als auch der Risikofelder,
    - Risikoerkennung und Risikoanalyse,
    - Festlegen bestandsgefährdender Risiken als auch der Risikofelder,
    - Zuordnung von Verantwortlichkeiten und Aufgabenbereichen.

© examio

5.2 Aufgaben und Lösungen

- 5) Nennen Sie unterschiedliche Kontrollaktivitäten
- Lösung: Zu den häufigsten und wichtigsten Kontrollaktivitäten gehören:
    - manuelle oder automatische,
    - präventive oder detektive,
    - primäre oder sekundäre,
    - Routinekontrollen oder Nicht-Routinekontrollen
    - Kontrollen auf Unternehmensebene oder Prozessebene

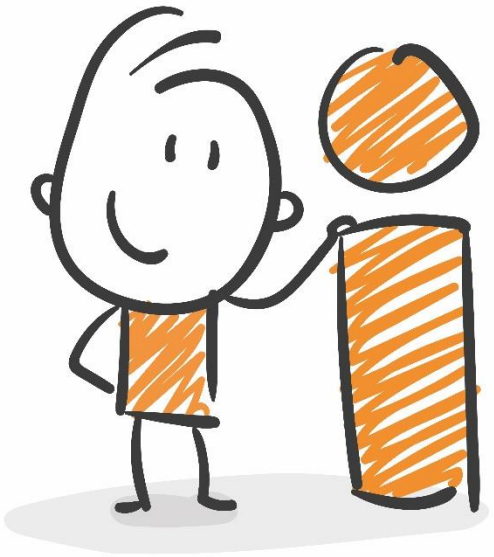
© examio

5.2 Aufgaben und Lösungen

- 6) Stellen Sie unterschiedliche Überwachungsaktivitäten in einem Unternehmen dar.
- Lösung: Bei den Überwachungsmaßnahmen sind folgende zu unterscheiden:
  - **Prozessunabhängigen** Überwachungsmaßnahmen: Sollen die Wirtschaftlichkeit der Überwachung sicherstellen und Verbesserungspotenziale aufzeigen.

    Prozessunabhängig agieren beispielsweise die **Interne Revision** und der **Abschlussprüfer**, aber auch Organe von Kapitalgesellschaften wie beispielsweise der **Aufsichtsrat**.
  - **Prozessabhängige** Überwachungsmaßnahmen: Werden **durch einzelne Stellen** realisiert, welche Teil des Risikomanagements sind.

5.2 Aufgaben und Lösungen

- 7) Stellen Sie unterschiedliche Kategorien von Missbrauch dar.
- Lösung: Missbrauch kann in **drei Kategorien** unterteilt werden, diese Kategorien lauten wie folgt:
    - Management-Fraud: Der Manager stellt das Unternehmen besser dar als es ist, um bessere Leistungen vom Unternehmen zu erhalten wie z.B. Höhere Prämien oder größere Boni.
    - Mitarbeiter-Fraud: Mitarbeiter fälschen Kassenbelege, um z. B. Geld zu unterschlagen.
    - Begünstigung Dritter: Hier wird Dritten dazu verholfen, Leistungen vom Unternehmen zu erhalten, die ungerechtfertigt sind.

Ein internes Kontrollsystem sicherstellen