

2009/10

Agnes Breitwieser  
Elisabeth Brunmair  
Barbara Lindner  
Marion Maureder



# **[FINANCIAL GOVERNANCE, RISK & COMPLIANCE]**

Status Quo bei den österreichischen  
Top500-Unternehmen

## Vorwort

Aufgrund zahlreicher Finanzskandale werden die Forderungen nach besseren Kontrollmaßnahmen an die Gesetzgebung immer lauter und die Ansprüche an das Management steigen. Daher wurden Richtlinien erstellt, die eine Implementierung und regelmäßige Überprüfung eines funktionierenden Internen Kontrollsystems regeln. Auch das Risikomanagement spielt eine immer größere Rolle.

Im Rahmen eines Praxisprojektes an der Fachhochschule Steyr im Studiengang „Controlling, Rechnungswesen und Finanzmanagement“ haben wir uns mit diesem Thema genauer auseinandergesetzt und eine Studie mit österreichischen Unternehmen durchgeführt. Die Fragen wurden in fünf Kernbereiche eingeteilt. Diese sind zum einen einleitende Fragen, gefolgt von Fragen zum Kontrollumfeld, der Risikobeurteilung, dem betrieblichen Informationssystem im Unternehmen und weiters spezifische Fragen für börsennotierte Unternehmen.

Ziel der Studie war es die Bedeutung des Internen Kontrollsystems und Risikomanagementsystems in Unternehmen zu beleuchten. Ein wesentlicher Bestandteil der Befragung war eine Analyse über die Implementierung und Verwendung des Internen Kontroll- und Risikomanagementsystems sowie die Bedeutung von Softwarelösungen bei diesen Vorgängen. Wichtig bei dieser Umfrage war, herauszufiltern, ob die Unternehmen ein Internes Kontrollsystem implementieren um die Einhaltung der gesetzlichen Richtlinien zu gewährleisten oder ob sie auch einen Nutzen für die Prozesse und Abläufe im Unternehmen erkennen.

Zusätzlich wird unsere Analyse der Ergebnisse durch kurze Zusammenfassungen der wesentlichen Richtlinien für das Interne Kontrollsystem bzw. Risikomanagementsystem im Unternehmensgesetzbuch, dem Börsegesetz, dem österreichischen Corporate Governance Kodex und der Emittenten Compliance Verordnung ergänzt.

Abschließend möchten wir noch denjenigen Unternehmen danken, die sich die Zeit genommen haben, unsere Fragen zu beantworten. Durch sie konnten wir eine hohe Rücklaufquote verzeichnen, die für ein aussagekräftiges Ergebnis nötig war.

Agnes Breitwieser  
Elisabeth Brunmair  
Barbara Lindner  
Marion Maureder

Studentinnen des Studiengangs „Controlling, Rechnungswesen und Finanzmanagement“  
Fachhochschule Steyr

## Inhaltsverzeichnis

<b>VORWORT .....</b>	<b>II</b>
<b>INHALTSVERZEICHNIS.....</b>	<b>III</b>
<b>KURZFASSUNG.....</b>	<b>IV</b>
<b>1 EINLEITUNG .....</b>	<b>5</b>
<b>1.1 Grundlagen der Studie.....</b>	<b>5</b>
<b>1.2 Erhebung der Daten.....</b>	<b>5</b>
<b>2 RELEVANTE RECHTSQUELLEN.....</b>	<b>6</b>
<b>2.1 Unternehmensrechts-Änderungsgesetz (URÄG).....</b>	<b>6</b>
<b>2.2 Österreichischer Corporate Governance Kodex.....</b>	<b>6</b>
<b>2.3 Börsegesetz.....</b>	<b>7</b>
<b>2.4 Emittenten Compliance Verordnung .....</b>	<b>8</b>
<b>2.5 Fachgutachten für Wirtschaftsprüfer: PG1 .....</b>	<b>8</b>
<b>2.6 ISA 400: Risikobeurteilung und interne Kontrolle .....</b>	<b>9</b>
<b>3 ERGEBNISSE DER STUDIE .....</b>	<b>10</b>
<b>3.1 Einleitende Fragen .....</b>	<b>10</b>
<b>3.2 Kontrollumfeld.....</b>	<b>12</b>
<b>3.3 Risikobeurteilung.....</b>	<b>16</b>
<b>3.4 Betriebliches Informationssystem .....</b>	<b>18</b>
<b>3.5 Spezifische Fragen für börsennotierte Unternehmen .....</b>	<b>25</b>
<b>4 FAZIT.....</b>	<b>26</b>

## Kurzfassung

Durch neue gesetzliche Vorschriften und dem wachsenden Druck auf den internationalen Finanzmärkten werden die Anforderungen an das Interne Kontrollsystem und das Risikomanagement immer höher.

Im Rahmen der Studie soll aufgezeigt werden, welche Auswirkungen die aktuellen Gegebenheiten auf die Implementierung und Aufrechterhaltung des Internen Kontrollsystems und Risikomanagements haben.

Insgesamt wurden 421 österreichische Industrieunternehmen kontaktiert, wovon 16 börsennotierte und 44 nicht börsennotierte Unternehmen den Fragebogen ausgefüllt haben. Dies entspricht einer Rücklaufquote von 14,25 Prozent.

Einleitend wurden die Unternehmen nach ihren Zielen gefragt, die sie mit dem Internen Kontrollsystem und dem Risikomanagement-System verfolgen. Mehr als 80 Prozent nutzen das IKS und Risikomanagement um das Vermögen zu bewahren, die Zuverlässigkeit des Rechnungs- und Berichtswesens zu gewährleisten und die Geschäftsrichtlinien und gesetzlichen Vorschriften einzuhalten.

### Kontrollumfeld

Das Rechnungswesen ist jener Bereich der bei nahezu allen Unternehmen durch das IKS abgedeckt wird. Weiters sind bei mehr als 80 Prozent der Unternehmen zusätzlich der Einkauf und der Verkauf durch das IKS abgedeckt. Verantwortlich für das IKS sind in mehr als 50 Prozent der Unternehmen die Geschäftsführung und/oder das Rechnungswesen. In vielen Unternehmen ist auch das Controlling dafür verantwortlich bzw. gibt es eine interne Revision, die dafür zuständig ist. Für das Risikomanagement ist bei mehr als 50 Prozent die Geschäftsführung verantwortlich.

Bei der Frage, in welchen Zeitabständen die Vorgaben des IKS und des Risikomanagements kontrolliert werden, lässt sich erkennen, dass das IKS bei einem Drittel der befragten Unternehmen jährlich und das Risikomanagement bei beinahe der selben Anzahl der Unternehmen quartalsweise kontrolliert wird.

### Risikobeurteilung

In der Mehrheit der Unternehmen wird die Ermittlung der wesentlichen Risiken anhand einer Risikoanalyse durchgeführt. Etwa 30 Prozent der Unternehmen verwenden für die Risikoabschätzung und –steuerung eine Software. Beurteilt werden die Risiken in drei Viertel der Unternehmen mittels Kennzahlen.

### Betriebliches Informationssystem

Die Dokumentation und Steuerung des IKS und Risikomanagements erfolgt in 55 Prozent der Unternehmen durch Microsoft Office. Abteilungsübergreifende Softwarelösungen sind in 83 Prozent der Unternehmen vorhanden, wovon mehr als ein Drittel dieser Softwarelösungen auch mit dem IKS und Risikomanagement verknüpft sind.

# 1 Einleitung

## 1.1 Grundlagen der Studie

Durch zahlreiche Finanzskandale in den letzten Jahren und die folgende Finanzkrise wurde der Kapitalmarkt stark erschüttert und viele Investoren verloren viel Geld. Als Konsequenz dieser Wirtschaftsskandale in den USA und in Europa wurde im Juli 2002 in den USA der Sarbanes-Oxley Act (SOX) verabschiedet, da vieles auf ein Versagen der internen und externen Aufsichtsorgane hinwies. Mit der 8. EU-Richtlinie wurde auf europäischer Ebene ein rechtliches Rahmenwerk für die Abschlussprüfung auf Basis des SOX-Ansatzes festgelegt.

Der bekannteste Beschluss ist die Forderung nach einer Etablierung eines Internen Kontrollsystems. Hierzu wurden Kriterien, Definitionen und Modelle eines Internen Kontrollsystems anhand eines Fünf-Komponenten-Würfels, COSO I, geschaffen und Elemente und Beziehungen des Internen Kontrollsystems dargestellt. COSO II ist das erweiterte Modell dieses Würfels und schafft Vorgaben und Grundlagen für die Etablierung eines unternehmensweiten Risikomanagements. Diese Rahmenbedingungen sehen das Interne Kontrollsystem als Teil des umfassenden Risikomanagementsystems.

Ein Risikomanagement bzw. Internes Kontrollsystem in einem Unternehmen sollte Maßnahmen beinhalten, die sicherstellen, dass das Vermögen gesichert, die Zuverlässigkeit der Daten und Übereinstimmung sämtlicher Abläufe gewährleistet und die Wirtschaftlichkeit des Unternehmens erhalten bleibt. Weiters sollen Investoren durch ein funktionsfähiges Internes Kontrollsystem und Risikomanagementsystem vor Betrug und überraschenden negativen Bilanzergebnissen geschützt werden.

## 1.2 Erhebung der Daten

Die Umfrage wurde mittels Online-Fragebogen durchgeführt. Dieser wurde am 23. November 2009 gestartet und war bis 18. Dezember 2009 geöffnet.

Bei der Auswahl der Unternehmen die an der Studie teilnehmen sollten, wurden die Top500 Unternehmen Österreichs, laut der Zeitschrift Trend vom Mai 2008, als Ausgangsbasis genutzt. Insgesamt wurden 421 börsennotierte als auch nicht börsennotierte Unternehmen kontaktiert, von denen 60 Unternehmen an der Umfrage teilnahmen. Dies entspricht einer Rücklaufquote von 14,25 %.

## 2 Relevante Rechtsquellen

Im folgenden Abschnitt möchten wir auf Rechtsquellen eingehen, die in Bezug auf das Risikomanagement und Interne Kontrollsystem in Österreich relevant sind.

### 2.1 Unternehmensrechts-Änderungsgesetz (URÄG)

Mit der Verankerung der Bestimmungen des URÄG im UGB fand eine Ausweitung bestehender und eine Einführung zahlreicher neuer Aufgaben für Unternehmen und deren Organe statt. Die neuen Regelungen traten mit 1. Juni 2008 in Kraft und sind für Geschäftsjahre, die nach dem 31. Dezember 2008 beginnen, anzuwenden. Das Ziel des URÄG ist die Rahmenbedingungen für die finanzielle Berichterstattung der Unternehmen sowie die Unabhängigkeit und Verantwortung des Abschlussprüfers zu verbessern. Weiters sind Richtlinien enthalten, die eine Überwachung der Unternehmensorgane vorsehen.

Die Beschreibung eines angemessenen Internen Kontrollsystems ist in §243a Abs. 2 UGB, bzw. §267 Abs. 3b UGB für den Konzernabschluss, geregelt. Dieser sieht vor, dass Gesellschaften, deren Aktien zum Handel auf einem geregelten Markt im Sinn des § 1 Abs. 2 BörseG notieren, im Lagebericht die wichtigsten Merkmale des Internen Kontrollsystems und Risikomanagementsystems in Hinblick auf den Rechnungslegungsprozess anzuführen haben.

Alle Aufgaben, Verantwortungen und Prozesse sind zu definieren, Kontrollsysteme für diese Prozesse sind einzurichten und ein Risikomanagement ist zu implementieren. Weiters sind alle diese Schritte in einer Dokumentation zu erfassen.

In § 273 Abs. 2 UGB sind die gesetzlichen Anforderungen an den Abschlussprüfer verankert. Dieser hat unverzüglich zu berichten, wenn schwerwiegende Verstöße der gesetzlichen Vertreter oder Arbeitnehmer gegen Gesetz, Gesellschaftsvertrag oder Satzung vorliegen oder der Bestand des geprüften Unternehmens gefährdet ist. Darüber hinaus hat er unverzüglich über wesentliche Schwächen bei der internen Kontrolle des Rechnungslegungsprozesses zu berichten. Bei kapitalmarktorientierten Unternehmen ist dies auch im Bestätigungsvermerk anzuführen.

### 2.2 Österreichischer Corporate Governance Kodex

Mit dem Österreichischen Corporate Governance Kodex wird österreichischen Aktiengesellschaften ein Ordnungsrahmen für die Leitung und Überwachung des Unternehmens zur Verfügung gestellt. Dieser enthält die international üblichen Standards für gute Unternehmensführung, aber auch die in diesem Zusammenhang bedeutsame Regelungen des

österreichischen Aktienrechts. Erstellt wird der Kodex vom Österreichischen Arbeitskreis für Corporate Governance.

Der Kodex wird als wirksames Instrument zur Förderung des Vertrauens der Aktionäre durch mehr Transparenz, durch eine Qualitätsverbesserung im Zusammenwirken zwischen Aufsichtsrat, Vorstand und den Aktionären und durch die Ausrichtung auf langfristige Wertschaffung gesehen. Der Österreichische Corporate Governance Kodex ist daher ein wichtiger Baustein für die weitere Entwicklung und Belebung des österreichischen Kapitalmarkts.

Der Kodex richtet sich vorrangig an österreichische börsennotierte Aktiengesellschaften einschließlich in Österreich eingetragener börsennotierter europäischer Aktiengesellschaften. Es wird empfohlen, dass sich auch nicht börsennotierte Aktiengesellschaften an den Regeln des Kodex orientieren, soweit die Regeln auf diese anwendbar sind.

Der Kodex umfasst folgende Regelkategorien:

- **Legal Requirement (L):** Regel beruht auf zwingenden Rechtsvorschriften
- **Comply or Explain (C):** Regel soll eingehalten werden; eine Abweichung muss erklärt und begründet werden, um ein kodexkonformes Verhalten zu erreichen
- **Recommendation (R):** Regel mit Empfehlungscharakter; Nichteinhaltung ist weder offenzulegen noch zu begründen

### 2.3 Börsegesetz

Börsennotierte Unternehmen müssen neben den Richtlinien des UGB bezüglich Risikomanagement und Internes Kontrollsystem auch die Richtlinien des Corporate Governance Kodex, des Börsegesetzes und der Emittenten Compliance Verordnung einhalten.

Paragraph 82 Abs. 4 des Börsegesetzes besagt beispielsweise, dass der Lagebericht den Geschäftsverlauf, das Geschäftsergebnis oder die Lage der Gesamtheit der in die Konsolidierung einbezogenen Unternehmen so darstellen soll, dass ein möglichst getreues Bild der Vermögens und Finanzlage entsteht und dass er die wesentlichen Risiken und Ungewissheiten, denen sie ausgesetzt sind, beschrieben werden sollen. Weiters besagt dieser Paragraph, dass die gesetzlichen Vertreter bestätigen müssen, dass der im Einklang mit den maßgebenden Rechnungslegungsstandards aufgestellte Jahresabschluss ihres Wissens ein möglichst getreues Bild der Vermögens-, Finanz- und Ertragslage des Unternehmens vermittelt.

## 2.4 Emittenten Compliance Verordnung

In der Emittenten Compliance Verordnung werden die Grundsätze der Weitergabe von Informationen im Unternehmen eines Emittenten sowie für die organisatorischen Maßnahmen zur Verhinderung einer missbräuchlichen Verwendung oder Weitergabe von Insider-Informationen geregelt.

## 2.5 Fachgutachten für Wirtschaftsprüfer: PG1

### Definition IKS

Unter dem Internen Kontrollsystem wird der von den mit der Unternehmensleitung und der Unternehmensüberwachung betrauten Personen und anderen Personen entworfene und ausgeführte Prozess verstanden, durch den

- die Wirksamkeit und Wirtschaftlichkeit der betrieblichen Tätigkeiten
- die Zuverlässigkeit der Finanzberichterstattung und
- die Einhaltung der für das Unternehmen maßgeblichen gesetzlichen Vorschriften

überwacht und kontrolliert wird, um zu verhindern, dass das Erreichen des Unternehmensziels durch den Eintritt geschäftlicher Risiken beeinträchtigt wird.

Die Verantwortung für die Ausgestaltung (Konzeption, Umsetzung, laufende Anpassung und Weiterentwicklung) und die Wirksamkeit eines angemessenen Internen Kontrollsystems liegt bei der Unternehmensleitung (siehe § 82 AktG und § 22 GmbHG).

### Das Interne Kontrollsystem besteht aus den folgenden Komponenten

- Kontrollumfeld (ethische Werte, Führungsgremien, Managementprinzipien, Organisation, 4-Augen-Prinzip, Personalpolitik,...)
- betriebliches Informations- und Kommunikationssystem einschließlich der Unternehmensabläufe, die sich mit der Finanzberichterstattung beschäftigen,
  - wer ist berechtigt Transaktionen durchzuführen
  - wer führt welche Aufzeichnungen und erstattet Bericht über diese Transaktionen
  - Informationsgewinnung über nicht unternehmenstypische Transaktionen
  - Berichterstattung über Daten, die bei Erstellung der Rechnungsabschlüsse verwendet werden
- Kontrollmaßnahmen (Ermächtigungen, Leistungskontrollen, allgemeine und anwendungsbezogene IT-Kontrollen, physische Kontrollen, Funktionstrennung,...)
- Überwachung der Kontrollmaßnahmen (Sicherstellung, dass die vorgeschriebenen Kontrollen auch durchgeführt werden, z.B.: organisatorische Sicherungsmaßnahmen, interne Revision, eingerichtete Abstimmungsverfahren (Inventurabgleiche, Saldenabstimmungen), Planungsrechnungen,...)

### Relevanz des IKS für den Abschlussprüfer

Die Beschäftigung des Abschlussprüfers mit dem Internen Kontrollsystem bezieht sich insbesondere (aber nicht nur) auf die Regelungen, welche die Ordnungsmäßigkeit und Verlässlichkeit der Rechnungslegung betreffen (rechnungslegungsbezogenes Internes Kontrollsystem). → Ermessen des Abschlussprüfers welche Bestandteile des IKS bei der Beurteilung des Risikos wesentlicher Fehldarstellungen in die Betrachtung einzubeziehen sind

Die Beurteilung des Internen Kontrollsystems erstreckt sich sowohl auf dessen Gestaltung als auch auf dessen Umsetzung und Aufrechterhaltung. Die Bedeutung des Internen Kontrollsystems für die Planung und Durchführung der Abschlussprüfung wird auch davon beeinflusst, ob die Kontrollen programmgesteuert mit Hilfe von Einrichtungen der Informationstechnik oder manuell durchgeführt werden. In diesem Zusammenhang ist auch zu prüfen, inwieweit der Einsatz von computergestützten Prüfungsverfahren bei der Prüfungsdurchführung möglich bzw. zweckmäßig ist.

## **2.6 ISA 400: Risikobeurteilung und interne Kontrolle**

Nach ISA 400 muss der Abschlussprüfer ausreichendes Verständnis von dem im Unternehmen vorhandenen Rechnungslegungssystem und den IKS haben. Prüfungshandlungen liegen in seinem pflichtgemäßen Ermessen, das bedeutet, der Prüfer muss geeignete interne Kontrollmaßnahmen herausfiltern und prüfen. Erkennt der Abschlussprüfer inhärente Risiken muss eine Adaptierung des Kontrollsystems erfolgen.

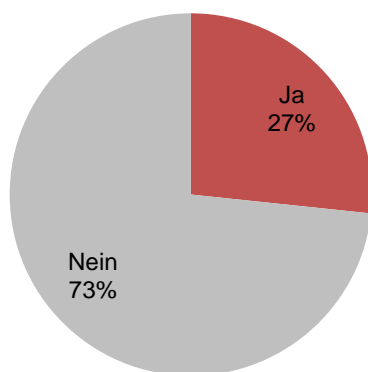
Die Wirksamkeit eines IKS kann durch verschiedene Faktoren wie Umgebung, Missbrauch oder menschliches Versagen beeinflusst werden.

### 3 Ergebnisse der Studie

Im folgenden Abschnitt wird auf die Ergebnisse der Studie näher eingegangen und die Antworten werden erläutert. Die Fragen sind in mehrere Kategorien geteilt um eine bessere Übersichtlichkeit zu gewährleisten. Anzumerken ist jedoch, dass die letzten beiden Fragen nur börsennotierte Unternehmen betreffen.

#### 3.1 Einleitende Fragen

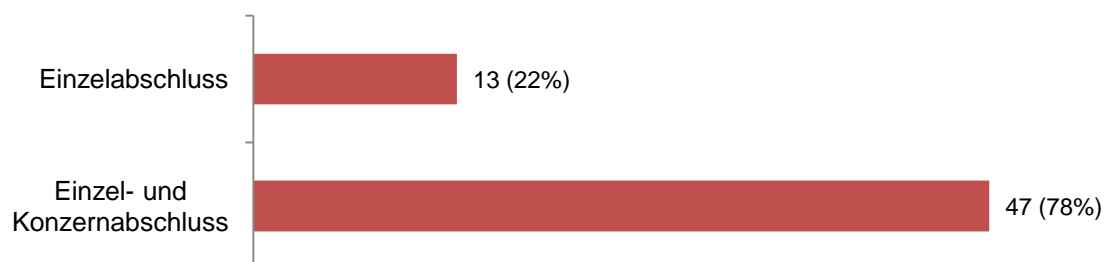
##### Ist Ihr Unternehmen börsennotiert oder planen Sie demnächst einen Börsengang?



Von den befragten Unternehmen sind 16 börsennotiert oder planen einen Börsengang, was einem Anteil von 27 Prozent entspricht. 44 Unternehmen gaben an, nicht an einer Börse gelistet zu sein.

##### Erstellen Sie einen Einzelabschluss oder Einzel- und Konzernabschluss?

Bei dieser Frage gaben 78 Prozent der Unternehmen an sowohl einen Einzel- als auch einen Konzernabschluss aufzustellen. In den restlichen Unternehmen, das sind 22 Prozent, wird ein Einzelabschluss erstellt.

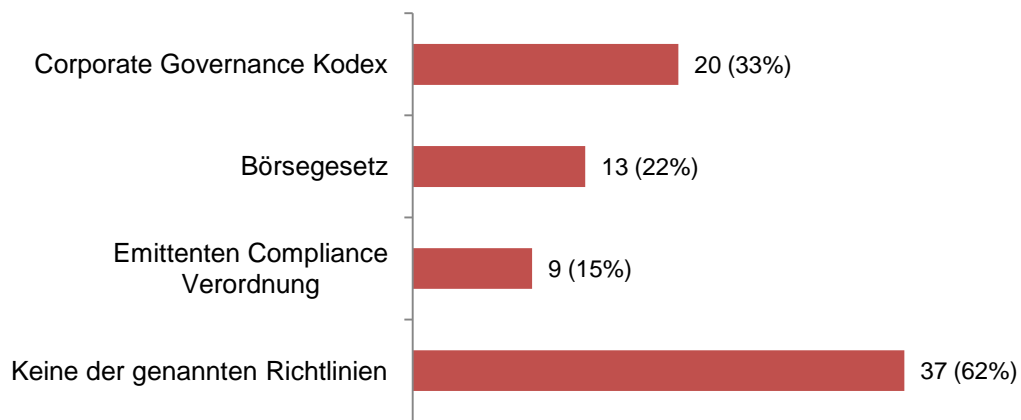


## Welche Richtlinien neben dem UGB müssen in Ihrem Unternehmen bzgl. Risikomanagement und IKS eingehalten werden?

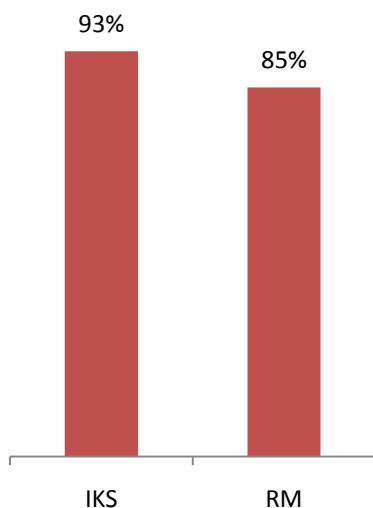
(Mehrfachnennung möglich)

Börsennotierte Unternehmen müssen neben dem UGB auch den Corporate Governance Kodex, das Börsengesetz sowie die Emittenten Compliance Verordnung einhalten.

Der untenstehenden Grafik ist zu entnehmen, dass der Großteil der befragten Unternehmen angibt, keine der genannten Richtlinien neben dem UGB einhalten zu müssen, was auf nicht börsennotierte Unternehmen zutrifft. Bei genauerer Betrachtung erkennt man, dass einzelnen börsennotierten Unternehmen die Verpflichtungen des Börsengesetzes und der Emittenten Compliance Verordnung offensichtlich nicht bewusst sind.



## Verfügen Sie über ein Internes Kontrollsystem/Risikomanagementsystem?



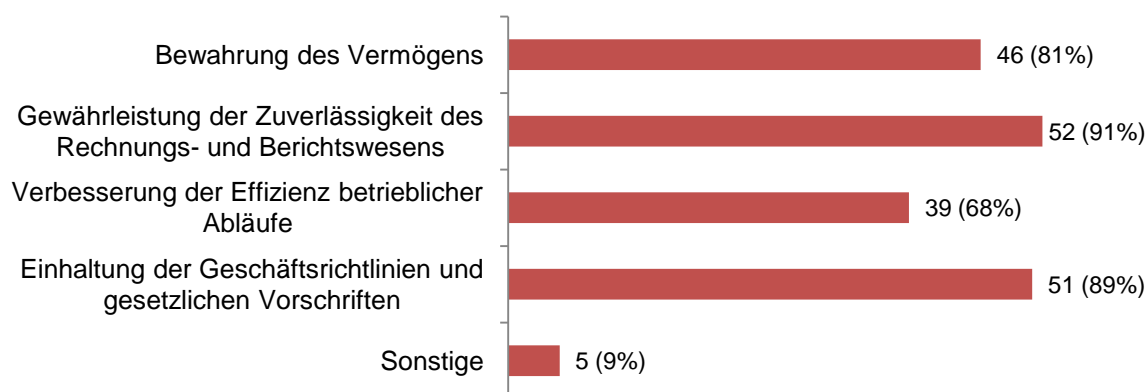
Stellt man gegenüber wie viele Unternehmen über ein Internes Kontrollsystem bzw. Risikomanagementsystem verfügen ist zu erkennen, dass nur ein kleiner Anteil die Implementierung noch nicht durchgeführt hat. Bei den Auswertungen ergab sich, dass vier Unternehmen kein Internes Kontrollsystem und neun Unternehmen kein Risikomanagementsystem haben, wobei davon drei Unternehmen weder über ein Internes Kontrollsystem, noch über ein Risikomanagementsystem verfügen. Anzumerken ist, dass zumindest das Interne Kontrollsystem für alle Unternehmen laut UGB vorgeschrieben ist. Wird diese Vorschrift nicht eingehalten, kommt es zu Sanktionen durch den Abschlussprüfer.

## Welche Ziele verfolgen Sie mit Ihrem Risikomanagement-System und Internen Kontrollsystem?

(Mehrfachnennung möglich)

Mit einem Internen Kontrollsystem oder Risikomanagementsystem werden verschiedene Ziele verfolgt. Mehr als 80 Prozent der Unternehmen gaben an, dass die Bewahrung des Vermögens, die Gewährleistung der Zuverlässigkeit des Rechnungs- und Berichtswesens sowie die Einhaltung der Geschäftsrichtlinien und der gesetzlichen Vorschriften zu den Zielen zählen.

Als sonstige Ziele wurden die Kontrolle der ausländischen Geschäftsführung, die Überprüfung der Kundenbonität, die Limitierung des Preisrisikos des Energiebeschaffungsportfolios, die Rohstoffversorgung sowie die Wahrnehmung von Chancen genannt.



### 3.2 Kontrollumfeld

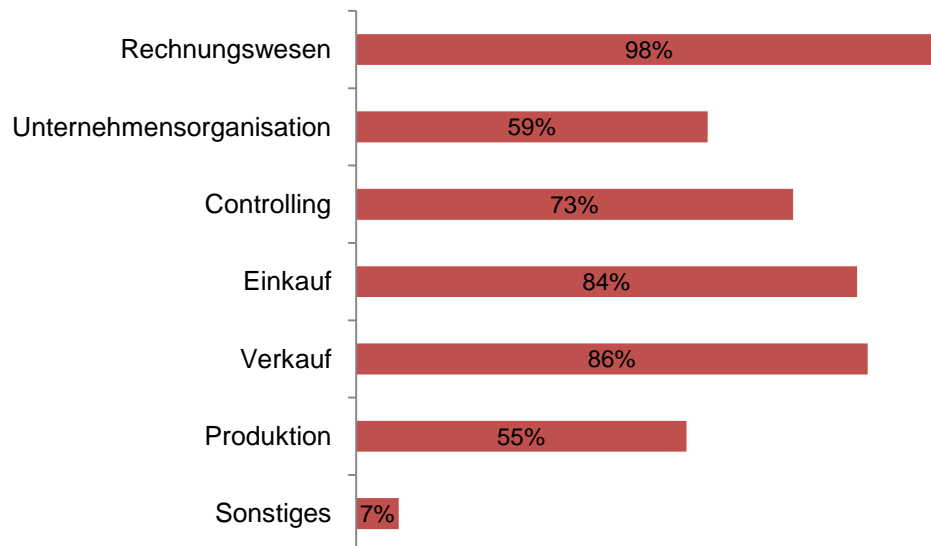
#### Welche Bereiche werden durch das IKS abgedeckt?

(Mehrfachnennung möglich)

Betrachtet man die Grafik, ist auf den ersten Blick erkennbar, dass viele unterschiedliche Bereiche durch das IKS abgedeckt werden. Die Bereiche Rechnungswesen, Einkauf und Verkauf wurden von mehr als 80 Prozent der befragten Unternehmen genannt. Die Bereiche Unternehmensorganisation, Controlling und Produktion werden auch bei mehr als der Hälfte der befragten Unternehmen durch das IKS abgedeckt. Der Bereich Sonstiges beinhaltet:

- IT
- Personal
- F&E
- Recht

- Kostenrechnung
- Corporate Finance
- Finanzierung
- Abwicklung Bauleistungen



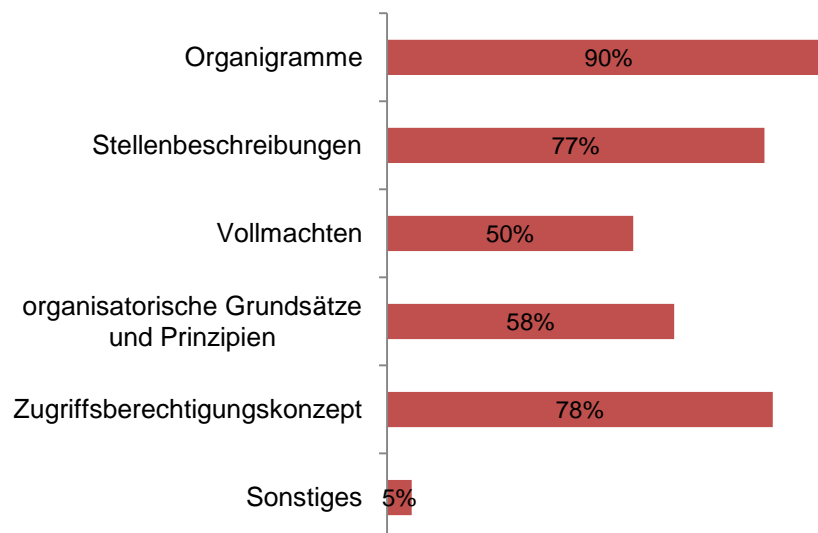
### Wie erfolgt die Abgrenzung von Kompetenzen, Zuständigkeiten und Verantwortlichkeiten im Unternehmen

(Mehrfachnennung möglich)

90 Prozent der befragten Unternehmen gaben an, dass die Abgrenzung durch Organigramme erfolgt.

Eine Abgrenzung durch Stellenbeschreibungen, Vollmachten, organisatorische Grundsätze und Prinzipien und Zugriffsberechtigungskonzepte wurden auch von über 50 Prozent der befragten Unternehmen angegeben.

Sonstige Möglichkeiten um Kompetenzen, Zuständigkeiten und Verantwortlichkeiten abzugrenzen sind z.B. Interne Regelungen, Organisationsvereinbarungen, Arbeitsanweisungen, Richtlinien, Leitfäden und Unterschriftenregelungen.

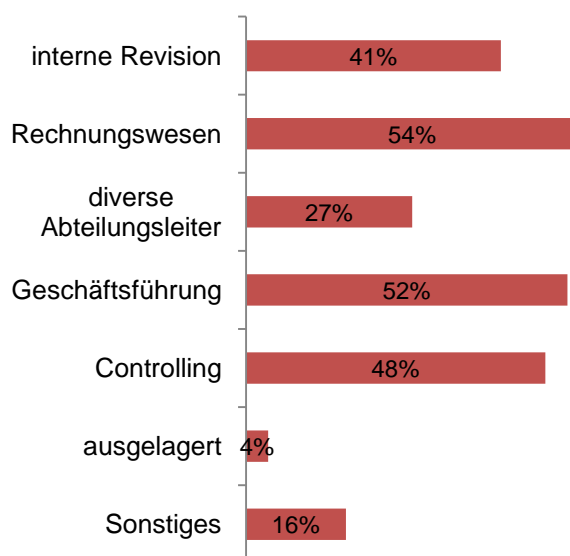


### Wer ist für das IKS im Unternehmen verantwortlich?

(Mehrfachnennung möglich)

Die Verantwortlichkeit des Rechnungswesen oder der Geschäftsführung für das IKS wurde von über 50 Prozent der Unternehmen angegeben. Die Interne Revision wurde von 41 Prozent der Unternehmen angegeben, diverse Abteilungsleiter von 27 Prozent und das Controlling von 48 Prozent. Vier Prozent der befragten Unternehmen haben die Verantwortlichkeit für das IKS ausgelagert.

Unter den Bereich Sonstiges fallen z.B. Corporate Development, eigene Stabstelle, IKS Verantwortlicher, Konzernleitung, Konzernrechnungswesen, Qualitätsmanagement, Risk und Internal Control, etc.

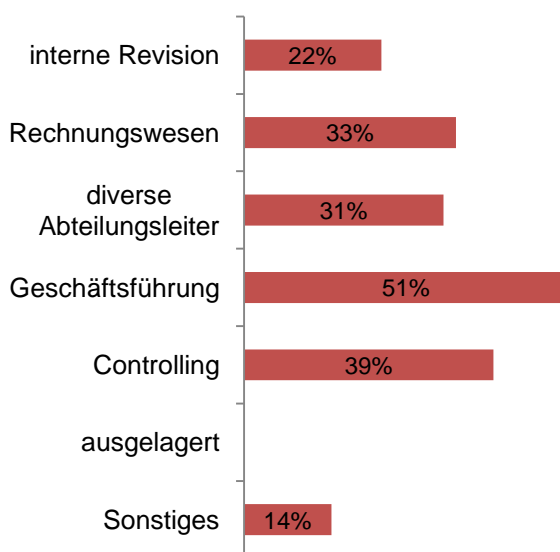


### Wer ist für das Risikomanagement im Unternehmen verantwortlich?

(Mehrfachnennung möglich)

Die Verantwortlichkeit der Geschäftsführung für das Risikomanagement wurde von 51 Prozent der Unternehmen angegeben. Die Interne Revision wurde von 22 Prozent der Unternehmen angegeben, das Rechnungswesen von 33 Prozent, diverse Abteilungsleiter von 31 Prozent und das Controlling von 39 Prozent. Keines der befragten Unternehmen hat die Verantwortlichkeit für das Risikomanagement ausgelagert.

Unter den Bereich Sonstiges fallen z.B. Corporate Finance, eigene Abteilung, eigener Riskmanager, Risikomanagement in der Holding, Risk & Internal Control, Vorstand, ...



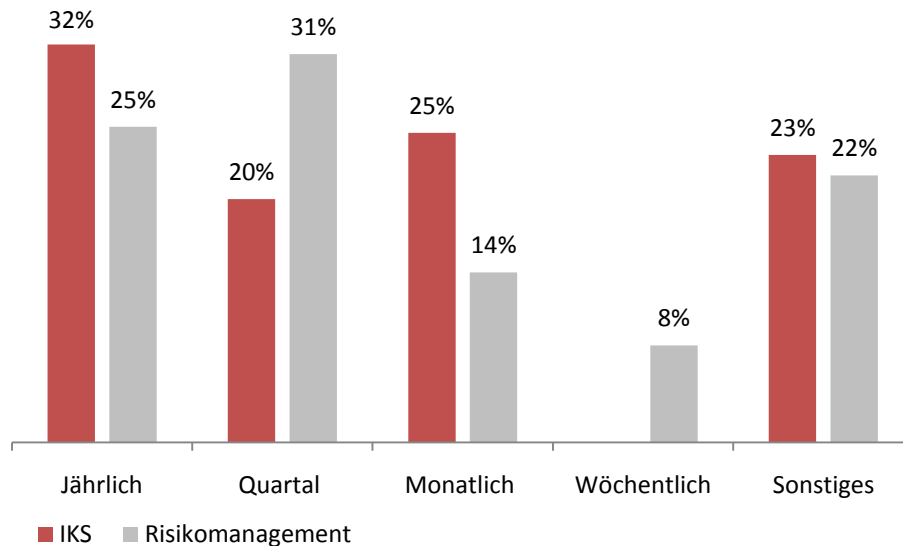
### In welchen Zeitabständen werden die Vorgaben des IKS bzw. des Risikomanagements kontrolliert?

Bei Betrachtung der Grafik ist auf den ersten Blick erkennbar, dass das IKS und das Risikomanagement in unterschiedlichen Zeitabständen kontrolliert werden.

Während das IKS bei 32 Prozent der befragten Unternehmen jährlich kontrolliert wird, wird das Risikomanagement bei beinahe der selben Anzahl von Unternehmen quartalsweise kontrolliert.

Die nächsthäufige Antwort im Bereich IKS war monatlich (25 %) gefolgt von quartalsweise (20 %). Kein Unternehmen kontrolliert das IKS wöchentlich. 26 Prozent der befragten Unternehmen kontrollieren das Risikomanagement jährlich, 14 Prozent monatlich und acht Prozent wöchentlich.

Der Bereich Sonstiges beinhaltet beispielsweise bei Bedarf, fallweise, regelmäßig, anlassbezogen, zu den Planungszeitpunkten, abhängig von der Art des implementierten Kontrollsystems, noch im Aufbau, ....

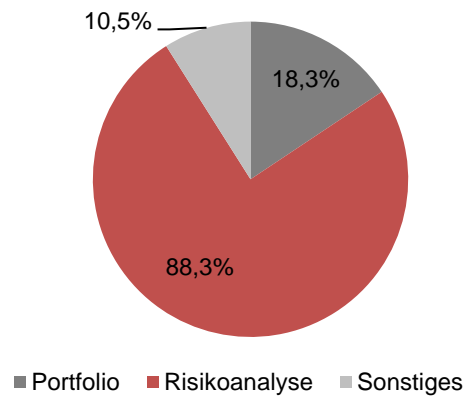


### 3.3 Risikobeurteilung

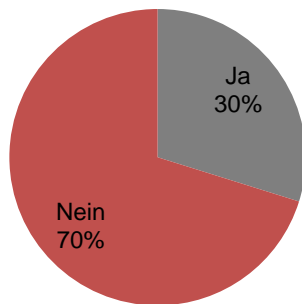
#### Wie ermitteln Sie die wesentlichen Risiken und Ungewissheiten in Ihrem Unternehmen?

Die wesentlichen Risiken und Ungewissheiten werden bei der Mehrheit der Unternehmen (88 %) durch Anwendung einer Risikoanalyse ermittelt. Etwa 18 Prozent der Unternehmen wählen zur Ermittlung der Risiken ein Portfolio und etwa 10 Prozent wählen sonstige Tools wie zum Beispiel:

- firmeneigene Auswertungen
- Beschaffungsportfolio in Verbindung mit Price -Forward-Curves
- laufende Risikobewertungen
- Guideline Riskmanagement (Identifikation, Bewertung, Maßnahmen...)
- softwareunterstützter, quartalsweiser Update durch Risikoverantwortliche
- Erhebung durch die Bereichsverantwortlichen und Meldung in das Risikomanagementsystem
- COSO Framework



### Verwenden Sie für die Risikoabschätzung und –steuerung in Ihrem Unternehmen eine Software?



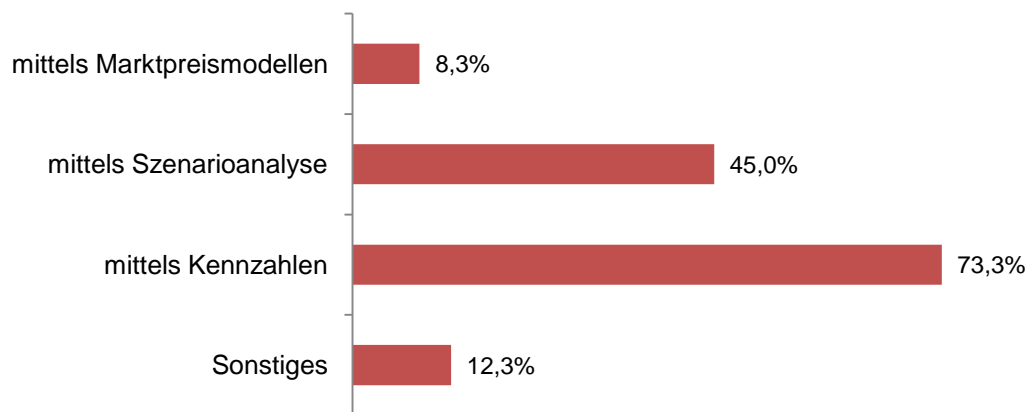
70 Prozent der Unternehmen verwenden für ihre Risikoabschätzung und –steuerung in Ihrem Unternehmen noch keine Software.

### Wie erfolgt die Risikobeurteilung in Ihrem Unternehmen?

(Mehrfachnennung möglich)

In 73 Prozent der Unternehmen erfolgt die Risikobeurteilung mittels Kennzahlen. Weiters führen ca. 45 Prozent der Unternehmen eine Szenarioanalyse durch. Nur 8,8 Prozent der Unternehmen verwenden Marktpreismodelle zur Risikobeurteilung. Der sonstige Teil beinhaltet

- Bewertung von Auswirkung und Eintrittswahrscheinlichkeit
- Beschreibungen, Beurteilungen
- Schätzung
- Beurteilung aufgrund Erfahrungswerten
- Abhängig von Risikoart - zB für Fremdwährungsrisiken: Value-at-Risk-Ansatz



Etwa zwei Drittel der Unternehmen haben angegeben, dass sie die ermittelten Risiken durch zahlenmäßige Größen darstellen. Ebenso zwei Drittel der Unternehmen stellen die Risiken durch eine Kategorisierung in „gering/mittel/hoch“ dar. Zehn Prozent der Unternehmen wählen folgende sonstige Darstellungsformen:

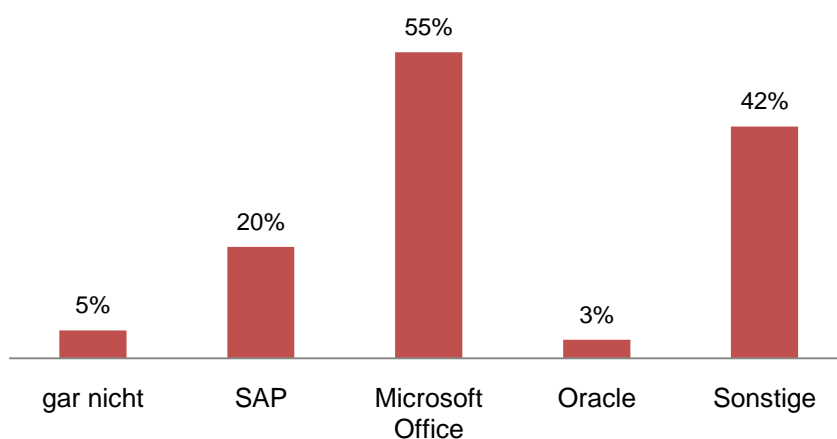
- Monte Carlo Simulation
- quantitative und qualitative Beschreibung
- Grafiken
- Portfoliodarstellungen
- Regelmäßige Berichte inkl. Erklärungen der Grafiken
- Darstellung von Schadenspotenzialen und Eintrittswahrscheinlichkeiten, Überführung in Risikoklassen gem. Ö-NORM
- Derzeit Umstellung auf Kategorisierung

### 3.4 Betriebliches Informationssystem

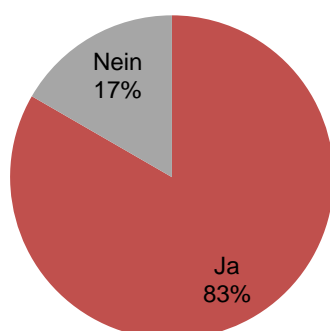
#### Wie dokumentieren und steuern Sie das IKS bzw. Risikomanagement in Ihrem Unternehmen?

(Mehrfachnennung möglich)

Bei der Frage, wie das IKS bzw. Risikomanagement im Unternehmen dokumentiert wird, gaben mehr als die Hälfte der Unternehmen Microsoft Office als Dokumentationsinstrument an. 20 Prozent der befragten Unternehmen verwenden SAP, weitere drei Prozent Oracle. 42 Prozent der Unternehmen gaben andere Dokumentationsformen wie Lotus Notes DB, AS400, Riskmanager, PMS, Microsoft NAV, Adonis, Schleupen (R2C), Share-Point, MIS oder ARIS an. Drei der befragten Unternehmen dokumentieren und steuern das IKS bzw. Risikomanagement nicht. Nur eines davon plant zukünftig den Einsatz einer Softwarelösung.



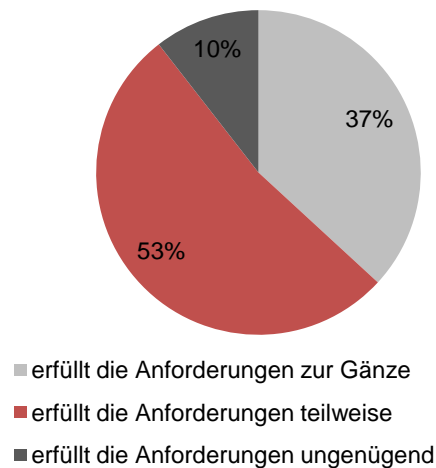
### Sind integrierte abteilungsübergreifende Softwarelösungen für Reporting und Planung vorhanden?



83 Prozent der Teilnehmer bestätigten das Vorhandensein von integrierten abteilungsübergreifenden Softwarelösungen für Reporting und Planung. Von diesen Softwarelösungen sind 43 Prozent mit dem IKS und 37 Prozent mit dem Risikomanagement verknüpft.

### Sind Sie mit der bestehenden Softwareunterstützung im Bereich IKS bzw. Risikomanagement zufrieden?

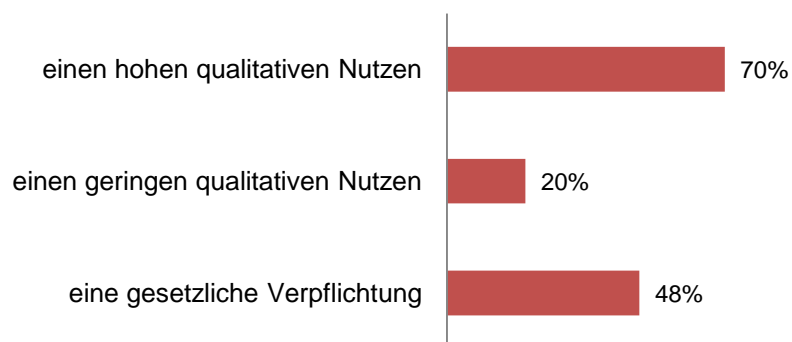
Unter jenen Unternehmen, die eine Software zur Unterstützung im Bereich IKS bzw. Risikomanagement verwenden, gaben mehr als die Hälfte an, die Software würde die Anforderungen nur teilweise erfüllen. Zufrieden mit ihrer bestehenden Software sind 37 Prozent der Teilnehmer unserer Befragung. 10 Prozent sind der Ansicht, ihre Software erfülle die Anforderungen ungenügend.



### 19. Was stellt das IKS für Ihr Unternehmen dar?

(Mehrfachnennung möglich)

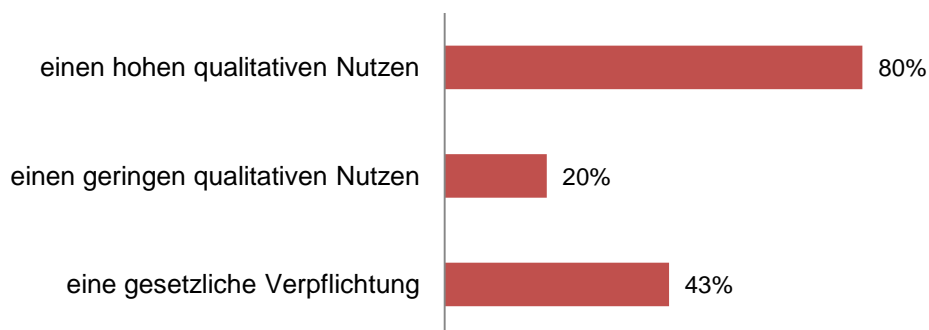
70 Prozent der Unternehmen erkennen in ihrem IKS einen hohen qualitativen Nutzen. Zusätzlich dazu geben fast die Hälfte der Befragten an, das IKS sei für ihr Unternehmen eine gesetzliche Verpflichtung. Nur 20 Prozent halten den Nutzen ihres IKS für gering. Verbesserungspotentiale werden vor allem bei integrierten Softwarelösungen (41%) gesehen. Im Zuge eines Verbesserungsprozesses fordern einige Unternehmen einen gewissen Grad an Standardisierung und Systematisierung, eine verstärkte Transparenz, eine Integration in die Unternehmenskultur bzw. in tägliche Abläufe, ein grundsätzliches Verständnis für IKS, zusätzliches Personal, Konsequenzen bei Nicht-Einhaltung der Regelungen und kontinuierliche Weiterentwicklung.



## Was stellt das Risikomanagement für Ihr Unternehmen dar?

(Mehrfachnennung möglich)

80 Prozent der Unternehmen erkennen in ihrem Risikomanagement einen hohen qualitativen Nutzen. Zusätzlich dazu geben 43 Prozent der Befragten an, das Risikomanagement sei für ihr Unternehmen eine gesetzliche Verpflichtung. Nur 20 Prozent halten den Nutzen ihres Risikomanagements für gering. Verbesserungspotentiale werden wiederum vor allem bei integrierten Softwarelösungen (37%) gesehen. Möglichkeiten zur Optimierung ihres Risikomanagements sehen einige Befragte in der Zusammenführung der verschiedenen Tätigkeiten in ein zentrales Dokument, in der Weiterentwicklung bestehender Systeme, in der Verbesserung der Reports bzw. Abbildung von Soll- vs. Ist-Risikoprofilen, in einer laufenden Risikoüberwachung und in der Umsetzung von Risikomaßnahmen.



## Welche Anforderungen stellt Ihr Unternehmen an eine IKS-Software?

Nachfolgend werden die Anforderungen aufgelistet, die die österreichischen Industrieunternehmen an eine IKS-Software stellen.

- Benutzerfreundlichkeit
- Kein wesentlicher zusätzlicher Arbeitsaufwand, muss den Prozess unterstützen und gleichzeitig die Dokumentationsanforderungen erfüllen; Berechtigungskonzept Dem jeweiligen Kontrollverantwortlichen müssen seine Kontrollaufgaben direkt zugewiesen werden, der weitere Prozessablauf sollte blockiert sein, solange die Kontrolle nicht wahrgenommen wurde; Reportmöglichkeiten (wann wurde von wem welche Kontrolle durchgeführt)
- Vollintegrierte Software, die sämtliche Unternehmensbereiche mit einbezieht
- Einfache Bedienung, dzt. MS Excel
- Umfassende Unterstützung bei Erkennung, Analyse, Bewertung, Steuerung und Überwachung von Risiken und bei der Dokumentation der Kontrollmaßnahmen
- Differenzierung nach und Abdeckung aller Geschäftsarten; Verknüpfung mit internen und externen Regelwerken; Einbindung der Risikoevaluierung pro Kontrolle

- Einfach zu bedienen, mehr als nur Standard - anpassbar
- Dokumentation, Effizienz in den Abläufen, Zuordnung von Verantwortungen
- Umfassende Information bei geringem Aufwand.
- Frühwarnsystem, vordefinierte Prozesse, etc.
- Zuverlässigkeit und Sicherheit
- Soll alle wesentlichen Gefahrenquellen berücksichtigen, Vieraugenprinzip, Vernetzung
- Sinnvolle Datenbasis
- Muss gesetzliche Anforderung abdecken
- Nachvollziehbar, überschaubar, logisch
- Mehr Kompatibilität hinsichtlich Schnittstellen verschiedenartiger angewendeter Programme und Tools
- Flexibel bei Erweiterungen & geringer Aufwand bei Veränderungen, Zentrale Wartung & lokale Abarbeitung der Kontrollen
- Aussagekräftig, prägnant
- Einfache Handhabung, Abbildung der internen Prozesse und Kompetenzdefinitionen
- Soll natürlich userfreundlich sein und das IKS nicht als gesondertes System sondern Teil der Regelprozesse sehen, charakteristische Abbildungen sollen möglich sein, Verknüpfung zum Risikomanagementsystem
- Compliance to SOX, vollständige Integration im REWE und CO
- Vollständigkeit, Transparenz
- Branchenspezifika müssen einfach darstellbar sein
- Einfach, praktikabel, schnell, multifunktionell, mehrsprachig, von überall aufrufbar, günstig
- Leicht bedienbar
- Praktikable Checklisten, Hinweise zur Umsetzung mit Beispielen
- Funktionsfähigkeit und Wirtschaftlichkeit von Geschäftsprozessen, Zuverlässigkeit von betrieblichen Informationen, Vermögenssicherung, Regeleinhaltung
- Umfassende Bearbeitung des Themas
- Bereichs- und abteilungsübergreifende Implementierung
- Einfache Handhabung und klare Information
- Flexibel, Bedienerfreundlich, Transparenz
- Stellt sicher, dass die definierten Prozesse eingehalten werden, über Darstellen von Information, Genehmigung, und Dokumentation des Ablaufs (Workflow)
- Papierloser Workflow
- Einfache Bedienbarkeit
- Klare Überblickvernetzung mit ERP und Finanzsystemverfolgung der Veränderungen

- Benutzerfreundlich, konzernweite Einsatzmöglichkeit, Abbildung der Unternehmensorganisation
- Gute Möglichkeit der Darstellung der Prozesse und Kontrollen.
- Prozesse und Berechtigungen analysieren, Risiken bewerten und gewichten, Maßnahmen ableiten
- Schnittstellen zu mehreren Systemen (SAP, Office Paket, sonstige Datenbanken), Benutzerfreundlichkeit (nur geringe Einschulung notwendig)
- Gute Integration, Preis/Leistungsverhältnis
- Kontrollpunkte in Abläufen darstellen, Verbindung von Kontrollpunkten zu Risiken
- Schlüssige und effiziente Auswertungen
- Integrationsfähigkeit
- Leichtes und unbürokratisches Handling der Anforderungen und Rückmeldungen
- Bereichsübergreifende Kontrolle soll möglich sein

Etwa zwanzig Prozent der befragten Unternehmen haben keine Anforderungen angegeben.

### **Welche Anforderungen stellt Ihr Unternehmen an ein Risikomanagementsystem?**

Nachfolgend werden die Anforderungen aufgelistet, die die österreichischen Industrieunternehmen an ein Risikomanagementsystem stellen.

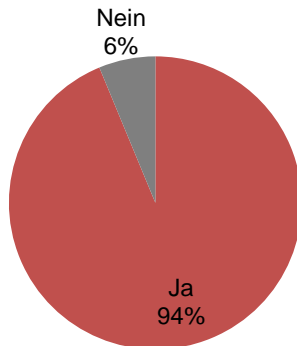
- Abbildung mit geringer Komplexität
- Strukturierte Dokumentation der wesentlichen Risiken sowie der Maßnahmen zur Risikoreduzierung inkl. Verantwortlicher, Bewertung des Restrisikos
- Sollte in Form eines Cockpit sein mit Warnampeln
- Einfache Bedienung, dzt. MS Excel mit Crystal Ball add in, Dokumentation in Lotus Notes DB
- Umfassende Unterstützung bei Erkennung, Analyse, Bewertung, Steuerung und Überwachung von Unternehmensrisiken; möglichst themen-, abteilungs- und länderübergreifend
- Differenzierung nach und Abdeckung aller Geschäftsarten; Verknüpfung mit internen und externen Regelwerken; Einbindung der Risikoevaluierung pro Kontrolle
- Einfach zu bedienen, mehr als nur Standard - anpassbar
- Simulationsmöglichkeiten
- Analyse und Frühwarnung betreffend der wesentlichen Unternehmensrisiken
- Rasches Aufzeigen von neuen Risiken und deren Auswirkungen.
- Frühwarnsystem, etc.
- Der Nutzen sollte erkennbar sein.
- Genauigkeit

- Soll alle wesentlichen Risiken abdecken, Vieraugenprinzip, Vernetzung und dadurch Möglichkeit zum Quercheck
- Sinnvolle Datenbasis
- Muss Risiken abbilden können
- Risikominimierung
- Gute Analysemöglichkeiten für Risikobetrachtungen, Einfache und flexible Änderungsmöglichkeiten
- Reduziert auf das Wesentliche
- Konsolidierungsfähigkeit, einfache Handhabung
- Einfach handhabbar, Verbindung ins Prozessmanagement (IKS!)
- Wirtschaftlichkeit (Kosten/Nutzen)
- Integrierte Softwarelösung inklusive Reporting
- Vollständigkeit, Transparenz
- Branchen- und Unternehmensspezifika müssen einfach darstellbar sein
- Einfach, praktikabel, leicht umzusetzen, uvm.
- Absicherung von Rohstoffpreisen = Erhaltung & Optimierung der Profitabilität der Produktion; Verbesserung der Vermögensstruktur; Dokumentation ggü. dem Eigentümer
- Leicht bedienbar
- Systematische Erfassung und Bewertung von Risiken sowie die Steuerung von Reaktionen auf festgestellte Risiken
- Umfassende Bearbeitung des Themas
- Einfache Handhabung und rasche Anpassung an geänderte Marktsituationen
- Einfach, Fokussiert
- Einfache Bedienbarkeit, Maßgeschneiderte Reports
- Limitverfolgung bei kundenspezifischen Warnhinweisen
- Wertschöpfung und "Alert" System
- Risikosteuerung, Dokumentation und Reporting.
- Darstellung von Portfolios, Hinterlegung eines Berechtigungskonzeptes möglich, Aggregation von Risiken möglich, qualitative und quantitative Risikobewertung möglich
- Analyseunterstützung
- Einfach zu erstellende Portfolio-Grafiken (Schadensausmaß zu -wahrscheinlichkeit), Entwicklung der Risiken im Zeitablauf
- Schlüssige und effiziente Auswertungen
- Leichte Bedienbarkeit und unkomplizierte Info- bzw. Meldeverfahren
- Die wesentlichen Risiken müssen ersichtlich sein

28 Prozent der befragten Unternehmen haben keine Anforderungen angegeben.

### 3.5 Spezifische Fragen für börsennotierte Unternehmen

#### Verlangt der Aufsichtsrat Informationen zum IKS und zum Risikomanagement des Unternehmens?



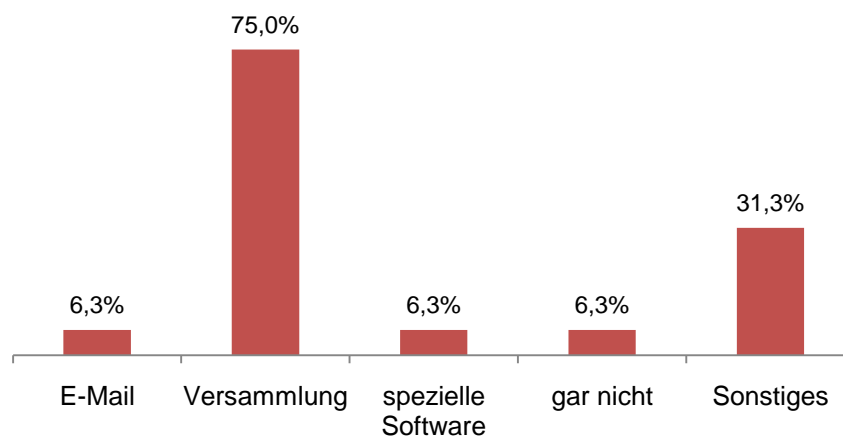
Wie im Chart ersichtlich verlangt in fast allen Fällen der Aufsichtsrat Informationen zum IKS und Risikomanagement. Diese Frage wurde nur börsennotierten Unternehmen gestellt und wurde von 16 Unternehmen beantwortet.

#### Wie erfolgt die Berichterstattung über das IKS und das Risikomanagement an den Aufsichtsrat?

Die Berichterstattung an den Aufsichtsrat erfolgt in drei Viertel aller Fälle durch eine Versammlung. Eine Berichterstattung via E-Mail oder durch eine spezielle Software erfolgt in jeweils nur einem Unternehmen. Ebenso berichtet nur ein Unternehmen gar nicht zum Thema IKS und Risikomanagement an den Aufsichtsrat.

Beachtung sollte man auch den 31 Prozent der Unternehmen schenken, die folgende sonstige Formen der Berichterstattung angegeben haben:

- Berichte, Präsentationen
- Eigenständige unabhängige Berichterstattung an Aufsichtsrat bezüglich IKS
- gezielte Reports
- Prüfungsausschuss-Termine
- Berichte, Präsentationen durch Abteilungsleiter



## 4 Fazit

**„In einer Welt voller Unsicherheit muss man eine Menge Dinge ausprobieren. Man kann nur hoffen, dass einige davon funktionieren.“**

(Douglass North, amerikanischer Wirtschaftshistoriker und Ökonom)

Die Forderung nach einem funktionierenden Internen Kontroll- und Risikomanagementsystem, welches ermöglichen soll, dass das Vermögen gesichert, die Zuverlässigkeit der Daten und Übereinstimmung sämtlicher Abläufe gewährleistet und die Wirtschaftlichkeit des Unternehmens eingehalten wird kommt nicht nur von Jahresabschlussadressaten, die sich durch die damit geschaffene Transparenz Schutz vor Betrug erhoffen, sondern auch von Unternehmen selbst, die erkannt haben, dass dadurch ein hoher qualitativer Nutzen für das Unternehmen entsteht. Sowohl dem Internen Kontrollsystem, über das 93 Prozent der befragten Unternehmen verfügen als auch dem Risikomanagementsystem, das 85 Prozent der 60 Unternehmen, die an unserer Umfrage teilnahmen, bereits implementiert haben, wird eine hohe Zweckmäßigkeit zugeschrieben.

Das Hauptziel, das laut unserer Befragung mit dem Risikomanagement- und dem Internen Kontrollsystem verfolgt wird, ist die Gewährleistung der Zuverlässigkeit des Rechnungs- und Berichtswesens vor allem in Unternehmensbereichen wie Rechnungswesen, Verkauf, Einkauf und Controlling. Diese Gewährleistung erfolgt in der Praxis meist durch die Geschäftsführung oder durch Mitarbeiter im Rechnungswesen oder Controlling, wobei die Einhaltung der Vorgaben im Bereich des Internen Kontrollsystems jährlich kontrolliert wird und das Risikomanagement vorwiegend quartalsweise überprüft wird.

Allgemein gaben die befragten Unternehmen an, ihr bestehendes Internes Kontrollsystem ließe sich durch einen gewissen Grad an Standardisierung und Systematisierung, durch eine verstärkte Transparenz, durch eine zunehmende Integration in die Unternehmenskultur und durch den Einsatz von integrierten Softwarelösungen verbessern. Vor allem an eine IKS-Software wurden folgende Anforderungen gestellt:

- Zuverlässigkeit, Benutzerfreundlichkeit, Effizienz
- Überschaubarkeit, Nachvollziehbarkeit, Transparenz
- Bereitstellung von umfassenden Informationen
- Vernetzung mit sämtlichen Unternehmensbereichen
- Verknüpfung zum Risikomanagement
- Sicherheit in Form eines Frühwarnsystems
- Flexibilität bei Erweiterungen
- Gutes Preis/Leistungsverhältnis
- Mehrsprachige Anwendung
- Einfach darzustellende Branchenspezifika

Zusätzlich zum Internen Kontrollsystem birgt auch das Risikomanagementsystem laut der befragten Unternehmen Verbesserungspotential. Eine Befragte sehen folgende Möglichkeiten zur Optimierung ihres Risikomanagements:

- Verbesserung der Reports bzw. Abbildung von Soll- vs. Ist-Risikoprofilen
- Laufenden Risikoüberwachung
- Umsetzung von Risikomaßnahmen
- Weiterentwicklung bestehender IT-Systeme

Ein aussagekräftiges und gut funktionierendes Risikomanagementsystem zeichnet sich laut Angabe der befragten Unternehmen durch folgende Merkmale aus:

- Geringe Komplexität
- Umfassende Unterstützung bei Erkennung, Analyse, Bewertung, Steuerung und Überwachung von Unternehmensrisiken
- Möglichst themen-, abteilungs- und länderübergreifende Vernetzung
- Simulationsmöglichkeiten
- Darstellungsmöglichkeit von Portfolios
- Frühwarnsystem
- Einfache und flexible Änderungsmöglichkeiten
- Wirtschaftlichkeit in Bezug auf Kosten/Nutzen Aspekte

Abschließend ist hervorzuheben, dass man anhand der Antworten der 60 Unternehmen, die an der Befragung teilnahmen eine repräsentative Stichprobe für die österreichischen Top 500 Unternehmen erhält. Damit kann man durchaus behaupten, dass die Wichtigkeit und Relevanz eines Internen Kontroll- und Risikomanagementsystems von den österreichischen Top 500 Unternehmen erkannt wurde und die Absicht zu einer laufenden Verbesserung besteht.

Trotz der guten Resonanz ist zu bemerken, dass das IKS von einigen Unternehmen nicht eingesetzt bzw. dokumentiert wird und dies eine Gesetzeswidrigkeit darstellt. Weiters existiert in vielen Unternehmen noch nicht das Bewusstsein, dass die letztendliche Verantwortung für ein funktionierendes Internes Kontrollsystem bei der Geschäftsleitung liegt.