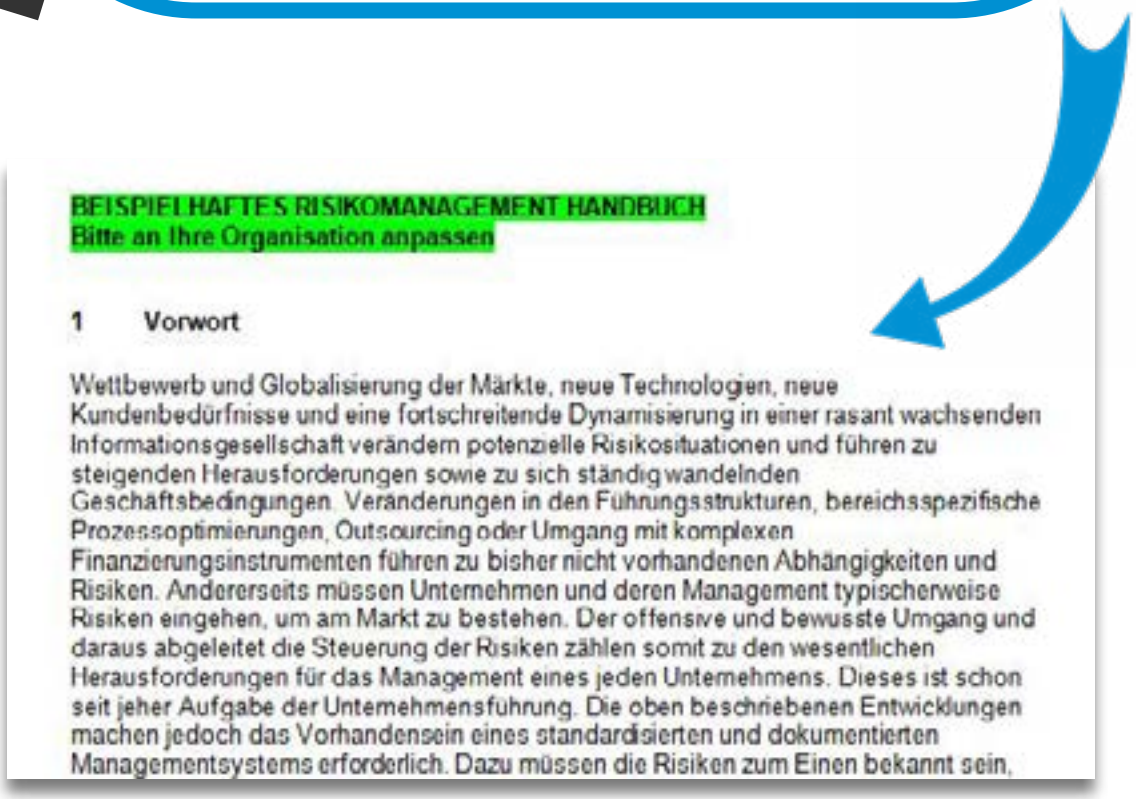
Risikomanagement Handbuch ISMS ISO 27001 & 27005

Word-Vorlage

Word-Vorschau

Hier werden nur Auszüge dargestellt!
Nach dem Erwerb steht Ihnen selbstverständlich die vollständige Version im offenen Dateiformat zur Verfügung.



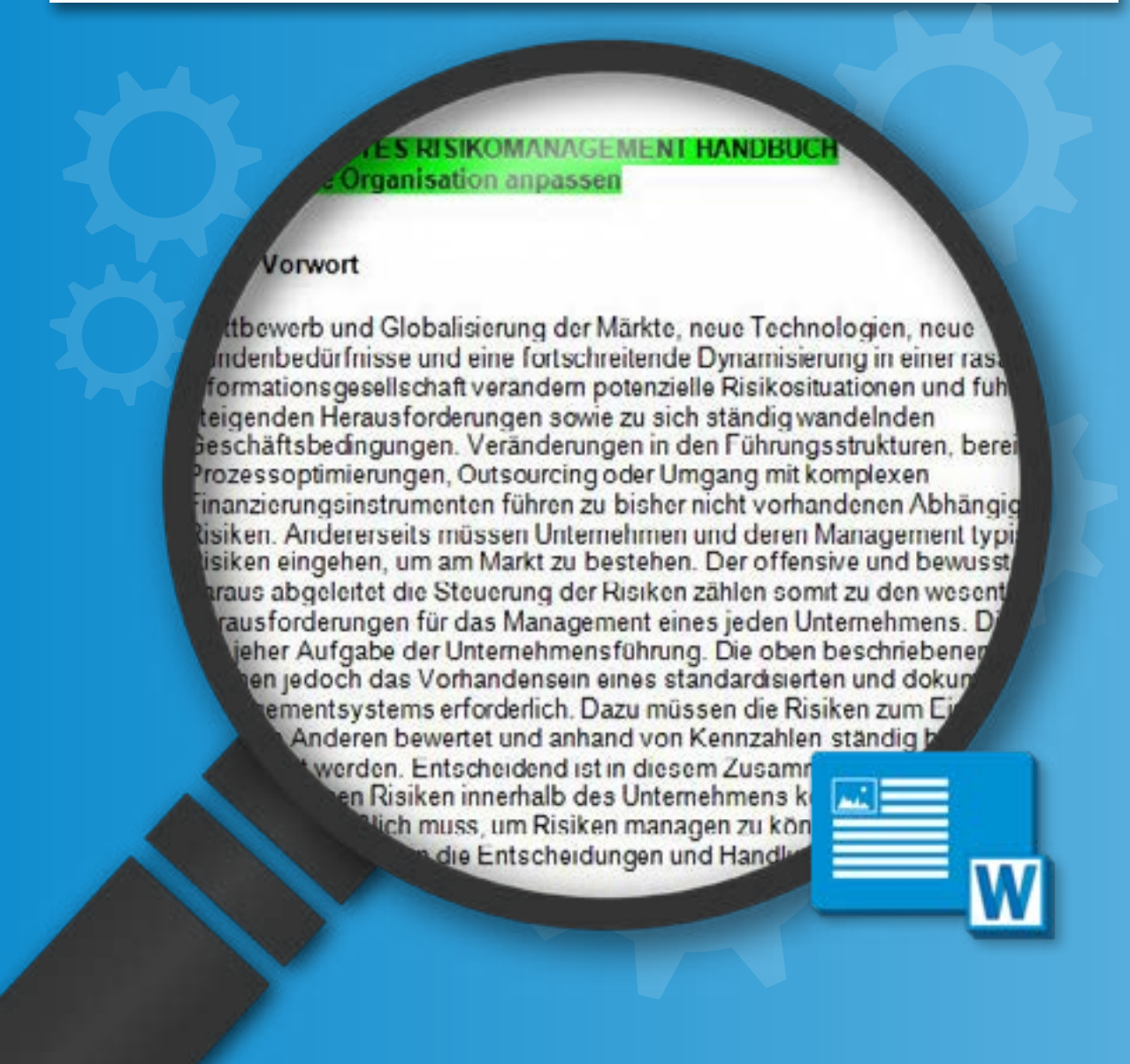
BEISPIELHAFTES RISIKOMANAGEMENT HANDBUCH
Bitte an Ihre Organisation anpassen

1 Vorwort

Wettbewerb und Globalisierung der Märkte, neue Technologien, neue Kundenbedürfnisse und eine fortschreitende Dynamisierung in einer rasant wachsenden Informationsgesellschaft verändern potenzielle Risikosituationen und führen zu steigenden Herausforderungen sowie zu sich ständig wandelnden Geschäftsbedingungen. Veränderungen in den Führungsstrukturen, bereichsspezifische Prozessoptimierungen, Outsourcing oder Umgang mit komplexen Finanzierungsinstrumenten führen zu bisher nicht vorhandenen Abhängigkeiten und Risiken. Andererseits müssen Unternehmen und deren Management typischerweise Risiken eingehen, um am Markt zu bestehen. Der offensive und bewusste Umgang und daraus abgeleitet die Steuerung der Risiken zählen somit zu den wesentlichen Herausforderungen für das Management eines jeden Unternehmens. Dieses ist schon seit jeher Aufgabe der Unternehmensführung. Die oben beschriebenen Entwicklungen machen jedoch das Vorhandensein eines standardisierten und dokumentierten Managementsystems erforderlich. Dazu müssen die Risiken zum Einen bekannt sein,

Übersicht

- Überblick über die Grundsätze eines Risikomanagementsystems
- Beispielhafte Darstellung eines Risikomanagement Handbuchs
- Grundlage für die Erstellung Ihres unternehmensspezifischen Risikomanagement Handbuchs



Inhalt

BEISPIELHAFTES RISIKOMANAGEMENT HANDBUCH
Bitte an Ihre Organisation anpassen

1 Vorwort

Wettbewerb und Globalisierung der Märkte, neue Technologien, neue Kundenbedürfnisse und eine fortschreitende Dynamisierung in einer rasant wachsenden Informationsgesellschaft verändern potenzielle Risikosituationen und führen zu steigenden Herausforderungen sowie zu sich ständig wandelnden Geschäftsbedingungen. Veränderungen in den Führungsstrukturen, bereichsspezifische Prozessoptimierungen, Outsourcing oder Umgang mit komplexen Finanzierungsinstrumenten führen zu bisher nicht vorhandenen Abhängigkeiten und Risiken. Andererseits müssen Unternehmen und deren Management typischerweise Risiken eingehen, um am Markt zu bestehen. Der offensive und bewusste Umgang und daraus abgeleitet die Steuerung der Risiken zählen somit zu den wesentlichen Herausforderungen für das Management eines jeden Unternehmens. Dieses ist schon seit jeher Aufgabe der Unternehmensführung. Die oben beschriebenen Entwicklungen machen jedoch das Vorhandensein eines standardisierten und dokumentierten Managementsystems erforderlich. Dazu müssen die Risiken zum Einen bekannt sein, und zum Anderen bewertet und anhand von Kennzahlen ständig beobachtet und kontrolliert werden. Entscheidend ist in diesem Zusammenhang, dass die eingegangenen Risiken innerhalb des Unternehmens kontrollierbar und kalkulierbar bleiben. Schließlich muss, um Risiken managen zu können, das Bewusstsein hierfür entwickelt sein und die Entscheidungen und Handlungen einfließen.

Wichtig für die dauerhafte Wirksamkeit eines Risikomanagement-Systems ist es, dass bei allen Mitarbeitern das Bewusstsein für eine Risiko- und Kontrollkultur geschaffen wird. Dies bedeutet, dass neben formellen Voraussetzungen, wie der Formulierung von risikopolitischen Grundsätzen auch die Etablierung eines in allen Funktionsbereichen funktionierenden Risikomanagement-System durchgesetzt werden muss. Um eine

Zunächst erhalten Sie einen Überblick über den Nutzen und die Funktion eines Risikomanagementsystems.

Inhalt

2 Risikostrategie

Die Risikostrategie konkretisiert die Umsetzung der risikopolitischen Grundsätze für die Organisationsbereiche. Abgeleitet aus der Strategie ergeben sich die Zielvorgaben, welche die Geschäftseinheiten zu berücksichtigen haben. Damit wird bestimmt, welche Risikoposition oder welches Risikovolumen als vertretbar angesehen werden kann. Die Einhaltung dieser Vorgaben wird durch das Risikocontrolling kontrolliert werden. Die so gewonnenen Risikoinformationen können dann wiederum zu einer Anpassung der Risikostrategie führen.

3 Risikobegriff

Unternehmensbestand gefährdende Entwicklungen die sich auf die Vermögens Finanz und Ertragslage des Konzerns auswirken können, sind zum Beispiel:

- risikobehaftete Geschäfte
- Unrichtigkeiten der Rechnungslegung
- Verstöße gegen gesetzliche Vorschriften
- Verletzung der Vertraulichkeit, Integrität und Verfügba keit von Informationen
- Möglichkeit, eine Schwachstelle an einem Objekt dur eine Bedrohung auszunutzen
- Eintrittswahrscheinlichkeit einer Bedrohung an einem bjekt

Unter den verschiedenen Oberpunkten „Risikostrategie“, „Risikobegriff“, „Risikoarten“, „Risikopolitische Leitsätze“, „Strategische Unternehmensführung und RM“, „Risikoberichterstattung“ und „Risikomanagement im Unternehmen“ erhalten Sie umfassende Informationen zur Thematik.

Inhalt

- Darstellung der Sicherheitsnsiken und der damit verbundenen Kosten
- Auswirkungen von IT-Sicherheitsvorfällen auf die kritischen Geschäftsprozesse
- Gesetzliche und vertragliche Sicherheitsanforderungen
- Übersicht über Standard-Vorgehensweisen zur IT-Sicherheit für die Branche

8 Das Risikomanagement bei dem Musterunternehmen

8.1 Bewertung der Werte

Der Prozessinhaber definiert den Wert des bedrohten Wertes hinsichtlich der Auswirkung auf seinen oder ihren Prozess oder die Auswirkung auf Musterunternehmen im allgemeinen oder die Auswirkung auf den Kunden im Falle des Verlustes, des Diebstahles, der Unverfügbarkeit, der Veränderung oder anderen Sicherheitsverletzungen. Der zugehörige Wert wird wie folgt bewertet:

sehr hoch	(>500.001,00 €)
hoch	(5.001 € - 500.000 €)
normal	(501 € - 5.000 €)
niedrig	(0 – 500 €)

Anmerkung:
Die Bewertung ist Organisationsspezifisch anzupassen

Die Werte, die im Rahmen einer bestimmten Analyse ermittelt wurden, werd einem gemeinsamen Dokument zusammengefasst (Ermittelte Werte aus Analyse Information dieser Listen wird in das Werteverzeichnis aufgenommen.

8.2 Risikoanalyse und Risikobewertung

Ein Risiko ist die Möglichkeit, dass eine Bedrohung unter Ausnutzung Schwachstelle Schaden an einem Objekt oder den Verlust eines Obje damit direkt oder indirekt einen Schaden verursacht.

Die Vorlage lässt sich selbstverständlich an Ihre unternehmensspezifischen Gegebenheiten anpassen, sodass Sie letzten Endes eine individualisierte Vorlage zur Hand haben.

Inhalt

Maßnahmen oder Verfahren einzuführen, wird diese Entscheidung als Teil der Sitzung des IT Sicherheitsforums dokumentiert und zur Sicherstellung, dass die Entscheidung angemessen war und Bestand hat, regelmäßig überprüft.

Ausgehend von den in der Risikoanalyse ermittelten Sicherheitsanforderungen wird ein Sicherheitskonzept erstellt. Dies erfolgt durch die Auswahl geeigneter Maßnahmen, die die Risiken auf ein akzeptables Maß reduzieren und unter dem Gesichtspunkt von Kosten und Nutzen eine optimale Lösung darstellen.

8.6 Risikomonitoring

Das Risikomonitoring ist Aufgabe des dezentralen und des zentralen Risikomanagements. Dazu werden für die kritischen Erfolgsfaktoren Frühwarnindikatoren vom dezentralen Risikomanager definiert. Aufgabe des zentralen Risikomanagements ist die Überwachung der definierten Frühwarnindikatoren. Sobald die definierten Schwellenwerte erreicht werden, wird ein Risikoreporting vom dezentralen Risikomanager erstellt, d.h. eine Prognose der zu erwartenden Auswirkungen des Risikoeintritts für das Musterunternehmen. Diese Prognosen werden idealerweise durch Szenarioanalysen ergänzt, die unterschiedliche Datenkonstellationen berücksichtigen. Das Risikomonitoring dient so als eine Art Wissensverstärker für Managemententscheidungen, da versucht wird, die Unsicherheit bezüglich der zukünftigen Unternehmens- bzw. Risikosituation zu reduzieren. Anhand dieser Informationen und der Maßnahmenvorschläge der dezentralen Risiko-Manager sowie des Zentralen Risikomanagements, entscheidet die Geschäftsführung, ob und in welchem Umfang Maßnahmen zur Risikobewältigung zu ergreifen sind oder ob sogar eine Anpassung der Unternehmensziele erforderlich ist. Sowohl die Verfolgung der Frühwarnindikatoren, die Überwachung der zugehörigen Schwellenwerte als auch die Durchführung der Szenarioanalysen obliegt dem dezentralen Risikomanagement.

8.9 Zentrales Risikomanagement (ZRM)

Eine wichtige Rolle im Risikomanagement- und Steuerungsprozess kommt dem Zentralen Risikomanagement zu. Im Rahmen der Verantwortung für die Risikosituation eines Unternehmens überträgt die Geschäftsleitung die Aufgabe der Durchführung der

Inhalt

Das Risikomanagement Handbuch ist ein Dokument, das die Grundsätze eines Systems zur Erkennung und Überwachung von geschäftsspezifischen Risiken in einer Organisation beschreibt.

Bei der Erstellung eines unternehmensspezifischen Risiko-Handbuches sollten folgende Informationen mit einfließen:

- Beschreibung der vorhandenen Systeme zur Risikofrüherkennung und zur Handhabung von Risiken
- relevante Risikofelder, die einer besonderen systematischen Überwachung hinsichtlich immanenter Risiken unterliegen
- Darstellung und Systematisierung der betrieblich relevanten Risiken
- Definition der effizienten und zieladaquaten Risikomaße einschließlich Darstellung des Wertebereiches
- Eine Beschreibung des Berichtswesens, über diese Risikofelder mit den Berichtswesen.
- Informationen über die Darstellung der Risikomaße im Berichtswesen und ihrer zulässigen Wertebereiche

Das Risikomanagement Handbuch wird von der Unternehmensführung verabschiedet.

Hilfreiche Hinweise zur Nutzung des Dokuments runden diese Vorlage ab.

VOREST AG
Bausteine Ihres Erfolgs

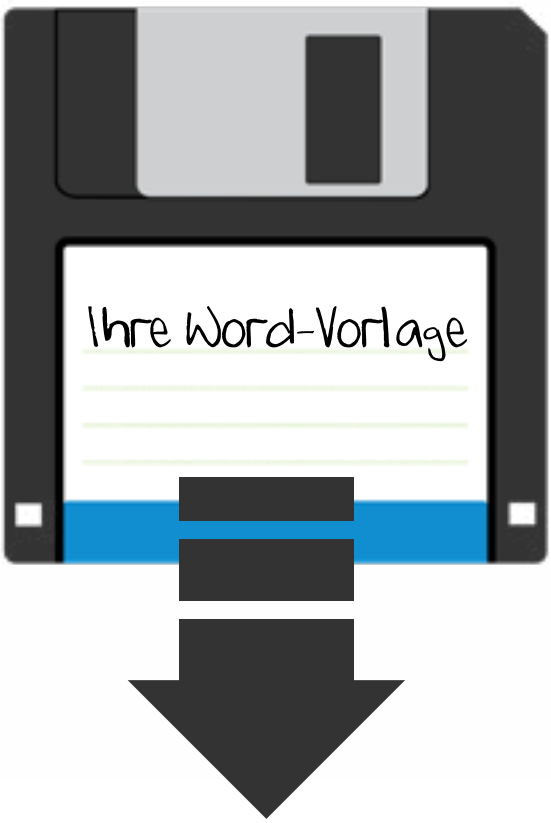
Kostenloser Update-Service

Bei ISO-Revisionsänderungen **binnen 1 Jahres**
nach Kauf dieser Vorlage wird Ihnen
das Dokument inklusive aktueller Normrevision
kostenfrei zur Verfügung gestellt.

VOREST AG
Bausteine Ihres Erfolgs

Sofortdownload

Ihre Vorlage steht Ihnen nach
dem Kauf als Download zur Verfügung.



VOREST AG
Bausteine Ihres Erfolgs

Zufriedenheitsgarantie

Ihre Autoren - mit **Erfahrung für Sie!**

Aus der **Praxis für Ihre Praxis**. Unsere Vorlagen, Checklisten, Formblätter und Schulungsunterlagen stammen alle von **erfahrenen Beratern**, die diese Musterdokumente mit ihrem ganzen **Erfahrungsschatz** für Sie erstellt haben.