PARSOW
WIRTSCHAFTSPRÜFER|STEUERBERATER

Compliance Monitoring durch automatisierte Interne Kontrollsysteme

Auswirkungen des Verbandssanktionsgesetz auf das CMS

Webinar 10.02.2021

Agenda

- Einordnung der Governance Elemente Risikomanagement, Compliance, Internes Kontrollsystem sowie Interne Revision
- Vom Compliance Management System zum „VerSanG“ Compliance Management System (vCMS)
- Risk Assessment im Lichte des vCMS
- Verknüpfung des IKS mit dem CMS sowie vCMS

PARSOW
WIRTSCHAFTSPRÜFER|STEUERBERATER

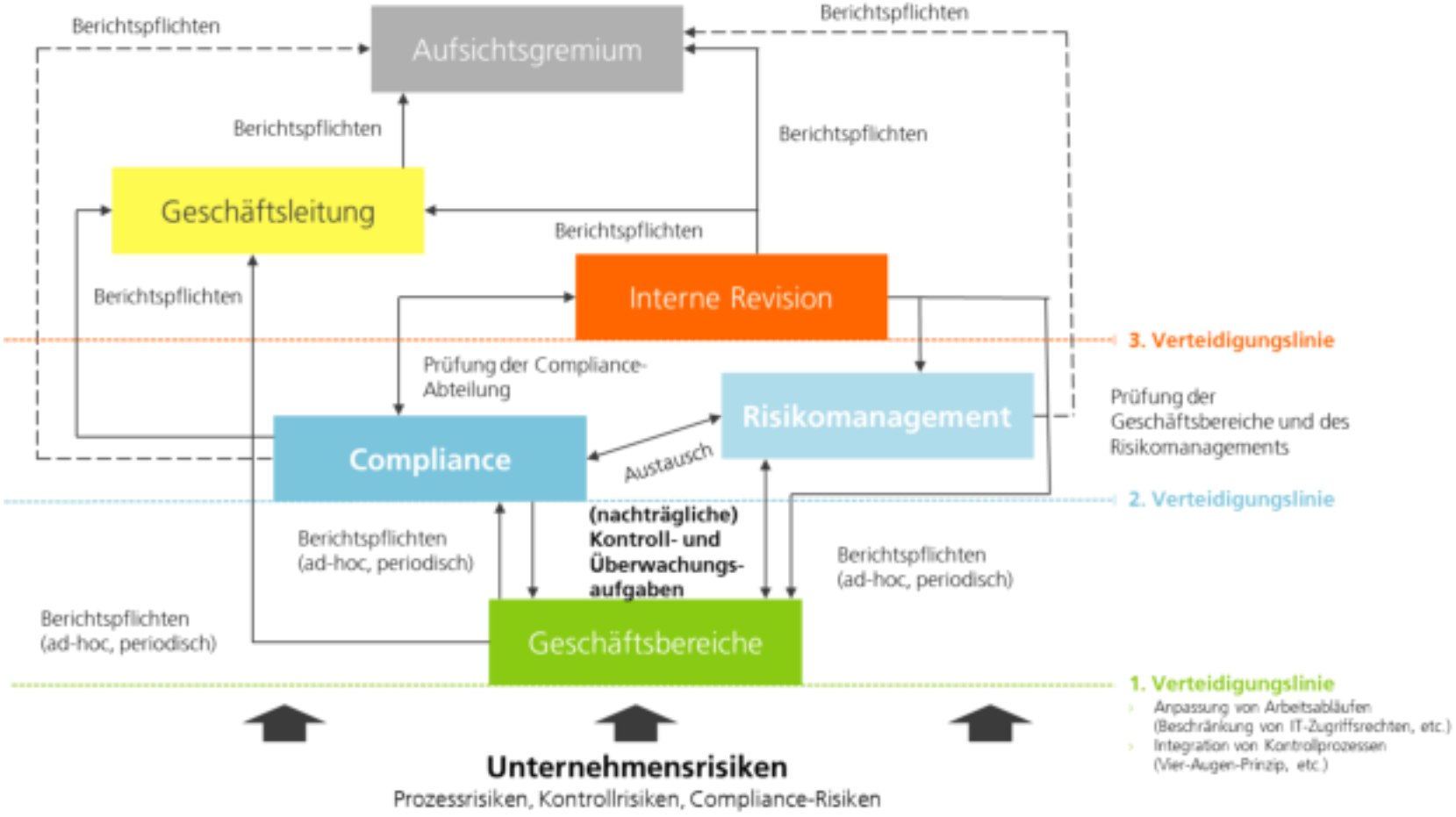
Einordnung der Governance Elemente Risikomanagement, Compliance, Internes Kontrollsystem sowie Interne Revision

Die einzelnen GRC-Elemente

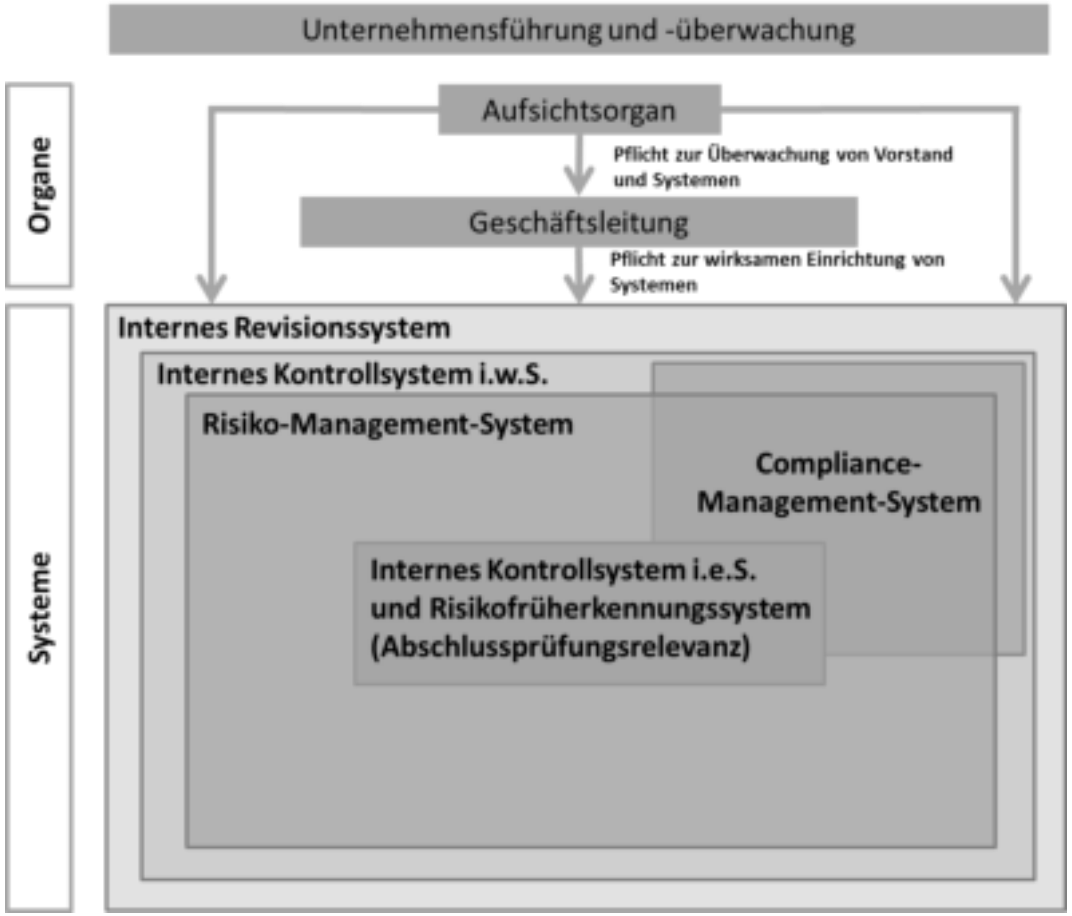
- **Internes Kontrollsystem**
  - Technische und organisatorische Maßnahmen und Kontrollen zur Einhaltung von Richtlinien
- **Compliance**
  - Systematisch-organisatorische Vermeidung und Behandlung von Regelverstößen
- **Risk Management**
  - Fokussiert auf Erkennen, Berichten und Bewerten von Risiken
- **Interne Revision**
  - Unabhängige Prüfungs- und Beratungsfunktion

Aufgabe der Elemente eines Compliance-Systems ist es, die Einhaltung von Recht und unternehmensinternen Richtlinien sicherzustellen.

Die Verteidigungslinien (TLOD)



Einordnung der Governance Elemente



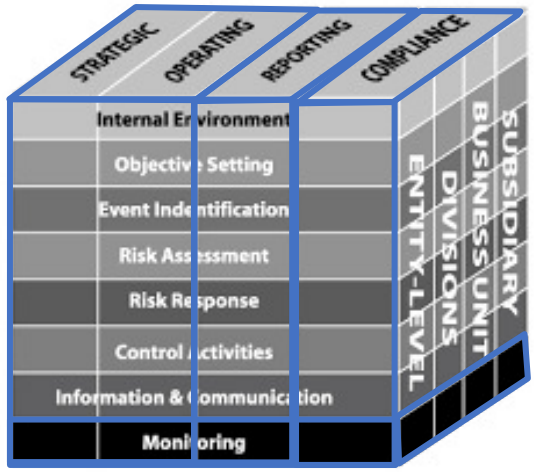
Governance Elemente und COSO

- Das COSO Referenzmodell ist Grundlage für das Risikomanagement in allen Elementen und den Risikodimensionen strategisch und operativ.

- Das Interne Kontrollsystem bezieht sich auf alle Elemente und die Dimension „Reporting“.

- Das Compliance Management System bezieht sich auf alle Elemente und die Dimension „Compliance“.

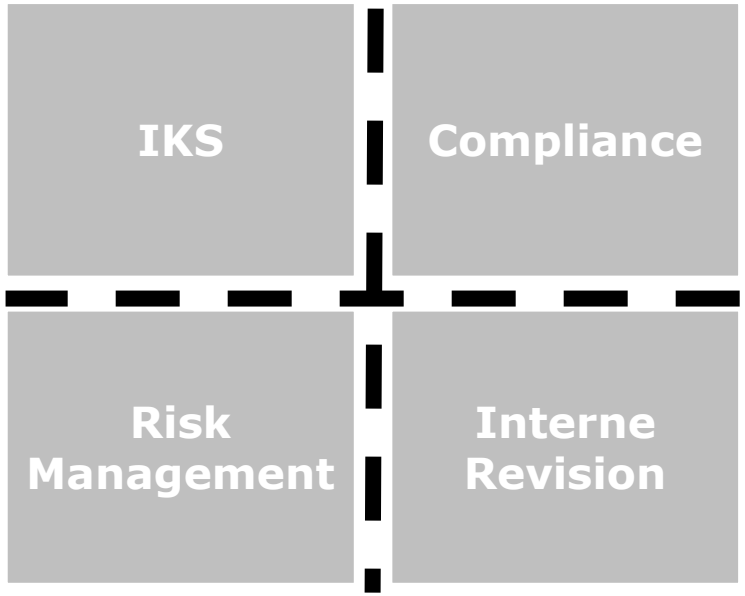
- Die Interne Revision bezieht sich über alle Dimensionen auf das Element „Monitoring“.



COSO Enterprise Risk Management - Integrated Framework (2004)

Integration der GRC-Elemente – Status Quo

- GRC-Strukturen häufig **heterogen**
- Funktionen **unabhängig** voneinander personell und organisatorisch **gewachsen**
- Ergebnis: Oft Ansammlung **unkoordinierter Strukturen**, interner Vorgaben, Gremien und Berichte
- Tendenz: Herstellen einer digitalen Verzahnung der unterschiedlichen Systeme



PARSOW
WIRTSCHAFTSPRÜFER|STEUERBERATER

Vom Compliance Management System zum vCMS

Verbandssanktionengesetz – Übersicht (1/3)

- Verband ist eine juristische Person des öffentlichen oder privaten Rechts, ein nicht rechtsfähiger Verein oder eine rechtsfähige Personengesellschaft. Ausrichtung auf einen wirtschaftlichen Geschäftsbetrieb.
- Verbandstat ist eine Straftat durch die die Pflichten des Verbandes verletzt oder der Verband bereichert wurde.
- Führt zur Haftung und Strafbarkeit von Unternehmen.
- Verbandsverantwortung liegt dann vor, wenn eine Leitungsperson oder eine andere Person bei der Wahrnehmung von Angelegenheiten des Verbandes eine Verbandstat begangen hat.
  - Voraussetzung: Verbandstat hätte durch angemessene Maßnahmen verhindert oder erschwert werden können (z.B. CMS).
- Auslandsstraftaten unterliegen ebenfalls VerSanG, wenn diese in Deutschland strafbar sind.
- Verbandstat unterliegt Legalitätsprinzip (Staatsanwaltschaft ist verpflichtet bei Bekanntwerden ein Ermittlungsverfahren einzuleiten).

Verbandssanktionengesetz – Übersicht (2/3)

- Verbandsgeldsanktion bis zu 10% des durchschnittlichen Konzernumsatzes der letzte 3 Geschäftsjahre.
- Bei Verbänden mit Umsatz von weniger als 100 Mio. EUR beträgt die Verbandsgeldsanktion max. 10 Mio. EUR bei vorsätzlichen und 5 Mio. EUR bei fahrlässigen Straftaten.
- Verwarnung mit Verbandsgeldsanktionsvorbehalt kann mit Auflagen, z.B. Verbesserter Elemente des CMS, verbunden sein; Gericht kann anordnen, dass die Umsetzung durch eine Sachkundige Stelle bescheinigt werden muss.
- Mögliche öffentliche Bekanntmachung der Verurteilung im Verbandssanktionsregister.
- Sanktionsmilderung durch Kooperation mit den Strafverfolgungsbehörden bis zu 50%
  - Wesentlicher Beitrag zur Aufklärung;
  - Trennung Verteidigung und Aufklärung;
  - Ununterbrochene und uneingeschränkte Zusammenarbeit mit den Verfolgungsbehörden;
  - Dokumente müssen nach Abschluß der Untersuchung an die Verfolgungsbehörde übergeben werden;
  - Untersuchung muss unter Beachtung der Grundsätze eines fairen Verfahrens durchgeführt werden (insb. Befragung der Mitarbeiter).

Verbandssanktionengesetz – Übersicht (3/3)

- Dokumente aus einer verbandsinternen Untersuchung können sichergestellt werden und sind nicht vor Beschlagnahme geschützt.
- Effektives CMS:
  - Kann sanktionsmildernd wirken;
  - Kann dazu führen, dass eine Mitarbeiterstraftat nicht dem Verband zugerechnet wird;
  - Ein nicht vorhandenes oder unzureichendes CMS kann straferhöhend wirken;
  - Ein nach der Verbandsstraftat verbessertes CMS kann sanktionsmildernd wirken.

  ➢ Keine Konkretisierung wie ein ausreichendes CMS ausgestaltet sein muss!

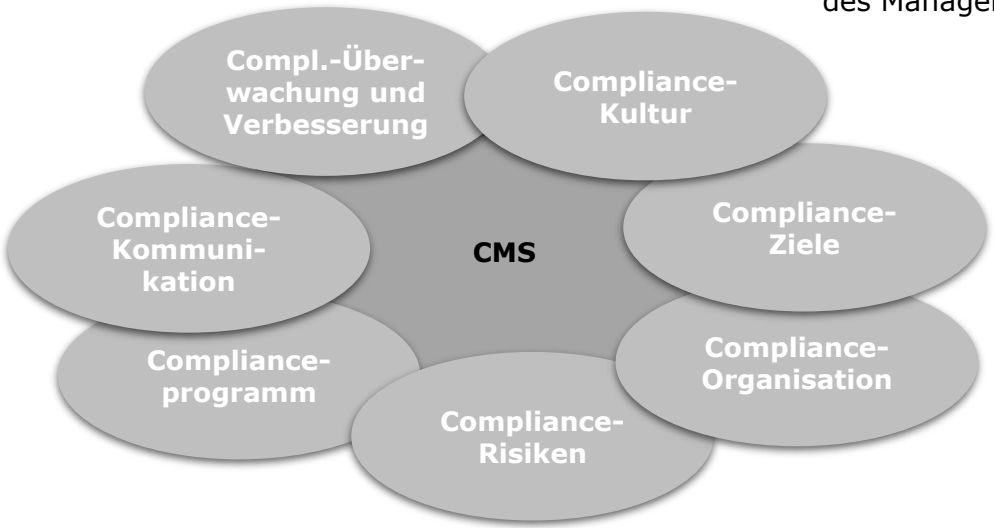
- Mögliche Leitlinien für ein ausreichendes CMS
  - PS 980
  - Kriterienkatalog des 2016 Federal Sentencing Guidelines Manuals
  - US Department of Justice „Evaluation of Corporate Compliance Programs“ Update June 2020
  - UK Bribery Act 2010

Überblick Grundelemente eines CMS nach PS 980

Compliance-Überwachung und Verbesserung
- Überwachung der Angemessenheit und Wirksamkeit
- Voraussetzung: ausreichende Dokumentation
- Berichterstattung von Schwachstellen und Verstößen
- Management trägt Verantwortung und sanktioniert Fehlverhalten

Compliance-Kultur
- Bewusstsein für die Bedeutung von Regeln als Grundlage für die Angemessenheit und Wirksamkeit des CMS
- Wesentlicher Einflussfaktor: Grundeinstellung und Verhaltensweisen des Managements („tone at the top")

Compliance-Kommunikation
- Information betroffener Mitarbeiter und ggf. Dritter über das Compliance-Programm sowie der Rollen/ Verantwortlichkeiten
- Festlegung der Berichtswege für Compliance-Risiken und für Hinweise auf Regelverstöße



Compliance-Ziele
- Festlegung wesentlicher zu erreichender CMS-Ziele auf Grundlage der allgemeinen Unternehmensziele
- Festlegung der relevanten Teilbereiche und der darin einzuhaltenden Regeln

Compliance-Programm
- Einführung von Grundsätzen und Maßnahmen zur Begrenzung von Risiken und Vermeidung von Verstößen
- Dokumentation

Compliance-Risiken
- Identifikation wesentlicher Compliance-Risiken
- Einführung systematischer Verfahren zur Risikoerkennung und -berichterstattung

Compliance-Organisation
- Bestimmung der Aufbau- und Ablauforganisation
- Festlegung von Rollen, Verantwortlichkeiten und Berichtswegen
- Festlegung und Bereitstellung notwendiger Ressourcen

DOJ „Evaluation of Corporate Compliance Programs“

- Faktoren für ein „gutes“ CMS nach dem DOJ
  - Is the Corporations Compliance Program Well Designed
    - Risk Assessment
    - Policies and Procedures (Gatekeepers)
    - Training and Communications
    - Reporting Structure and Investigations Process
    - Third Party Management (Appropriate Controls)
    - Mergers and Acquisitions
  - Is the Corporations Compliance Program Adequately Resourced and Empowered to Function Effectively
    - Commitment by Senior and Middle Management
    - Autonomy and Resources (Data Resources and Access)
    - Incentives and Disciplinary Measures
  - Does the Corporation’s Compliance Program Work in Practice
    - Continuous Improvement, Periodic Testing, and Review (control testing)
    - Investigation of Misconduct
    - Analysis and Remediation of Any Underlying Misconduct

Weitere Anforderungen an ein „gutes“ vCMS

- Individuelle Berücksichtigung der Größe des Unternehmens, Branche, geografische Präsenz, regulatorische Umfeld und sonstige interne und externe Faktoren
- Über die klassische Risiken hinaus, wie z.B. Korruption, Geldwäsche, Datenschutz sollten auch andere CMS Bereiche Berücksichtigung finden wie z.B.:
  - Tax Compliance (§153 AO, IKS)
  - Banking Compliance
  - Technische Compliance (Produkt Compliance)
  - IT Compliance
  - Food Compliance
  - HR Compliance
- Berücksichtigung aller für das Unternehmen relevanten Strafrechtsrisiken
- Einbettung des CMS in die relevanten Betriebsabläufe
- End to End Betrachtung und Dokumentation
  - ➢ Vom Risiko zur Kontrolle
- CMS Bereiche müssen zu einem holistischen CMS zusammengeführt werden

PARSOW
WIRTSCHAFTSPRÜFER|STEUERBERATER

Risk Assessment im Lichte des vCMS

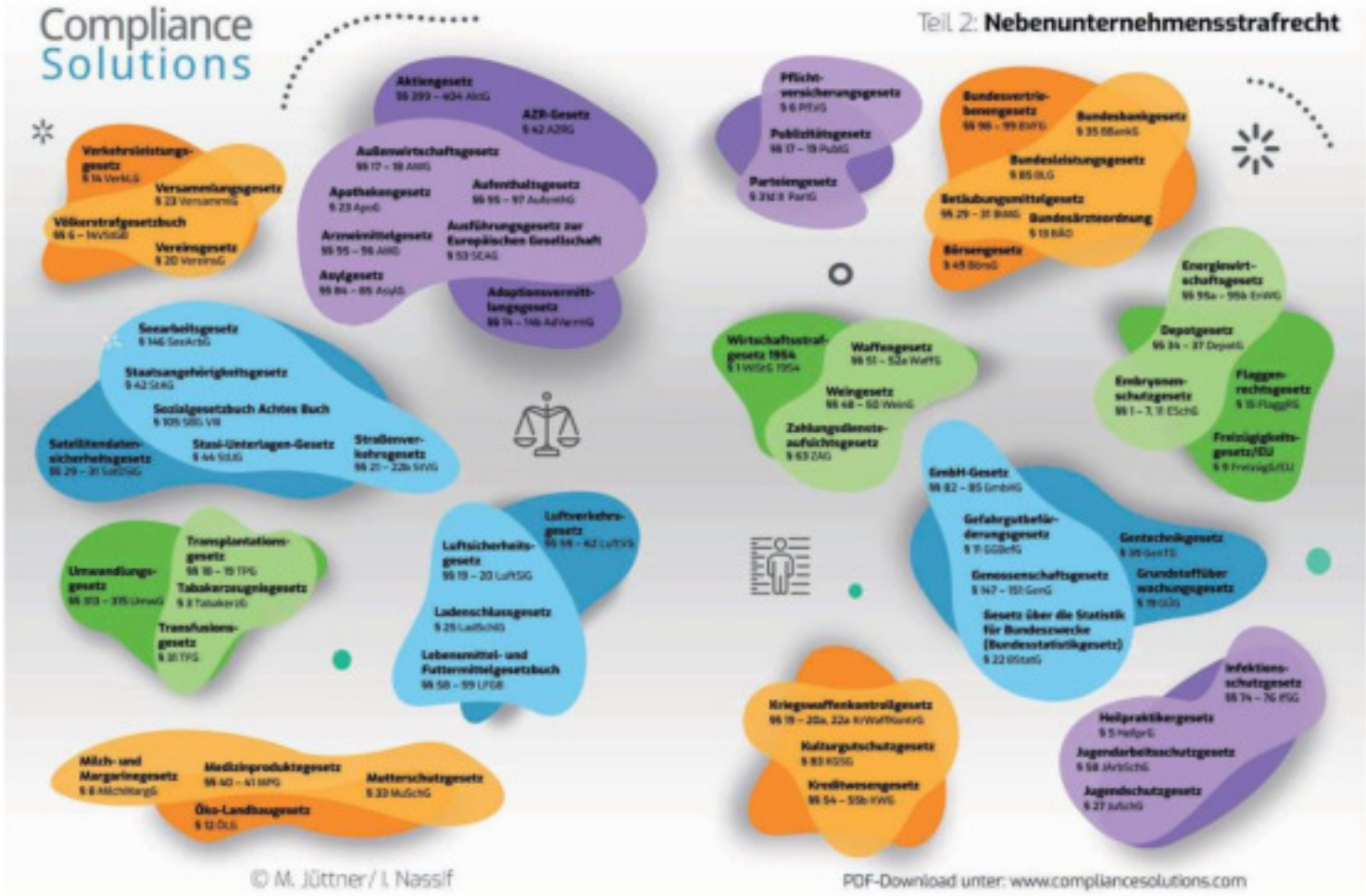
PARSOW
WIRTSCHAFTSPRÜFER|STEUERBERATER

Compliance Risiko Katalog

DICO Risikokatalog

vCMS-Universum

vCMS-Universum



Ansatz und vorgehen

Zielsetzung: **Reduktion der Unternehmensrisiken** durch Einführung eines wirksamen VerSanG Compliance-Management-Systems (vCMS)

Aufnahme des Status Quo

- In der ersten Phase wird das Compliance-Risiko für das Unternehmen evaluiert. Dabei wurde die Risikoeinschätzung in Form von Workshops mit der Geschäftsführung und einzelnen Mitarbeitern durchgeführt.

Ergebnis

- Das Unternehmen hat Kenntnis über sein Compliance-Umfeld inklusive zu mitigierender Risiken und vorhandenen Maßnahmen zur Risikoreduzierung.

Analyse des Risikos

- In einer zweiten Phase wurden die gesammelten Risiken und Informationen ausgewertet. Dabei wurden die identifizierten Risiken den bereits vorhandenen sowie notwendigen Internen Kontrollen gegenübergestellt

Ergebnis

- Das Unternehmen entscheidet sich für Interne Kontrollen, die die wesentlichen Compliance-Risiken mitigieren.

Umsetzung von Maßnahmen

- In der letzten Phase werden die mitgierenden Maßnahmen umgesetzt bzw. vorhandene Maßnahmen angepasst. Dabei sollten Maßnahmen auch durch IT-Einsatz unterstützt werden.

Ergebnis

- Das Unternehmen bindet die Unternehmens-Einheiten in sein Compliance-Management-System ein.

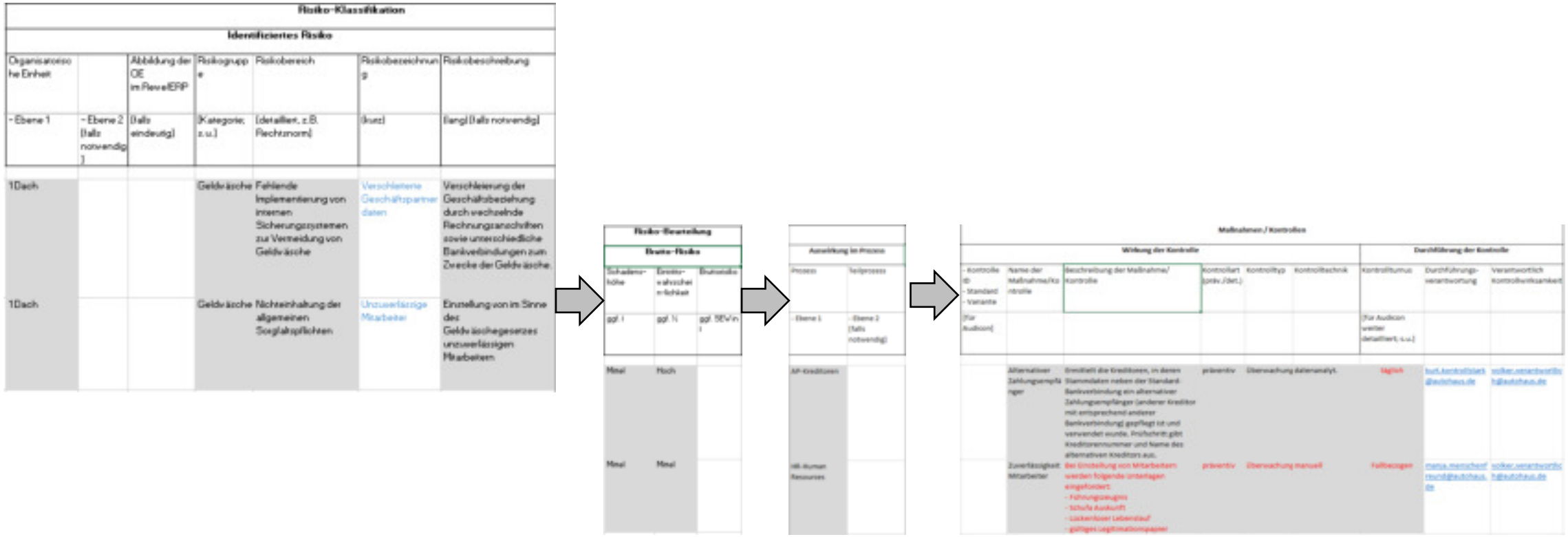
vCMS

Risiko Assessment und Durchführung (1/2)

Mögliche Arbeitsergebnisse

- Dokumentation der Risikobewertung (Fragebögen, Workshop-Unterlagen)
- Compliance-Risiko-Kontroll-Matrizen
- Richtlinien, Prozessbeschreibungen, Schulungskonzepte inkl. Inhalte, Tool-Beschreibungen
- vCMS-Dokumentation (Ist-Zustand und sich fortentwickelnd)

Risiko Assessment und Durchführung (2/2)



Risiko-Klassifikation						
Identifiziertes Risiko						
Organisatorische Einheit		Abbildung der OE im ReveERP	Risikogruppe	Risikobereich	Risikobezeichnung	Risikobeschreibung
- Ebene 1	- Ebene 2 (falls notwendig)	(falls eindeutig)	(Kategorie; z.u.)	(detailliert, z.B. Rechtsnorm)	(kurz)	(lang) (falls notwendig)
1Dach			Geldwäsche	Fehlende Implementierung von internen Sicherungssystemen zur Vermeidung von Geldwäsche	Verschleierte Geschäftspartner daten	Verschleierung der Geschäftsbeziehung durch wechselnde Rechnungsanschriften sowie unterschiedliche Bankverbindungen zum Zwecke der Geldwäsche.
1Dach			Geldwäsche	Nichteinhaltung der allgemeinen Sorgfaltspflichten	Unzuverlässige Mitarbeiter	Einstellung von im Sinne des Geldwäschegesetzes unzuverlässigen Mitarbeitern

Risiko-Beurteilung		
Brutto-Risiko		
Schadenshöhe	Eintrittswahrscheinlichkeit	Bruttorisiko
ggf. 1	ggf. ½	ggf. 5EVin 1
Mmal	Hoch	
Mmal	Mmal	

Auswirkung im Prozess	
Prozess	Teilprozess
- Ebene 1	- Ebene 2 (falls notwendig)
AP-Kreditoren	
HR-Human Ressources	

Maßnahmen / Kontrollen									
Wirkung der Kontrolle						Durchführung der Kontrolle			
- Kontrolle ID - Standard - Variante	Name der Maßnahme/Kontrolle	Beschreibung der Maßnahme/ Kontrolle	Kontrollart (präv./det.):	Kontrolltyp	Kontrolltechnik	Kontrollturnus	Durchführungs-verantwortung	Verantwortlich Kontrollwirksamkeit	
(für Audicon)						(für Audicon weiter detailliert; z.u.)			
	Alternativer Zahlungsempfänger	Ermittelt die Kreditoren, in denen Stammdaten neben der Standard-Bankverbindung ein alternativer Zahlungsempfänger (anderer Kreditor mit entsprechend anderer Bankverbindung) gepflegt ist und verwendet wurde. Prüfschritt gibt Kreditorennummer und Name des alternativen Kreditors aus.	präventiv	Überwachung datenanalyt.	täglich	kurt.kontrollstark@autohaus.de	volker.verantwortlich@autohaus.de		
	Zuverlässigkeit Mitarbeiter	Bei Einstellung von Mitarbeitern werden folgende Unterlagen eingefordert: - Führungszeugnis - Schufa Auskunft - Lückenloser Lebenslauf - gültiges Legitimationspapier	präventiv	Überwachung manuell	Fallbezogen	maria.menschenrecht@autohaus.de	volker.verantwortlich@autohaus.de		

Wesentliche Erfolgsfaktoren für ein vCMS Risk Assessment

- Implementierung eines Legal Change Monitoring Prozesses
- Fokussierung auf die das Unternehmen spezifisch betreffenden „High-Risk-Areas“; Hauptunternehmensstrafrecht vs. Nebenunternehmensstrafrecht
- Interdisziplinäres Denken
- Kontinuierliches Risk Assessment (Produktlebenszyclus)
- Etablierung eines lernenden Systems (Monitoring and Improvement)
- Zusammenführen der CMS Risk Assessments (z.B. Tax Compliance, Technical Compliance) zu einem integrierten CMS Risk Assessment
- Self Monitoring durch die Interne Revision
- Permanentes Control Testing
- Identifizierung von Gate Keepern
- Eindeutige Festlegung von Kontrollverantwortlichen

Verknüpfung des IKS mit dem CMS sowie vCMS durch Automatisierte Interne Kontrollen

Grundlagen – Was ist ein IKS?

Was ist ein IKS?

- Systematisch gestaltete organisatorische Maßnahmen und Kontrollen im Unternehmen zur Einhaltung von Richtlinien und zur Abwehr von Schäden, die durch das eigene Personal oder Dritte verursacht werden können.

Ziele eines IKS

- Effektivität und Effizienz von Geschäftsprozessen
- Zuverlässigkeit der Finanzberichterstattung
- Einhaltung von Gesetzen, Verordnungen und Verträgen

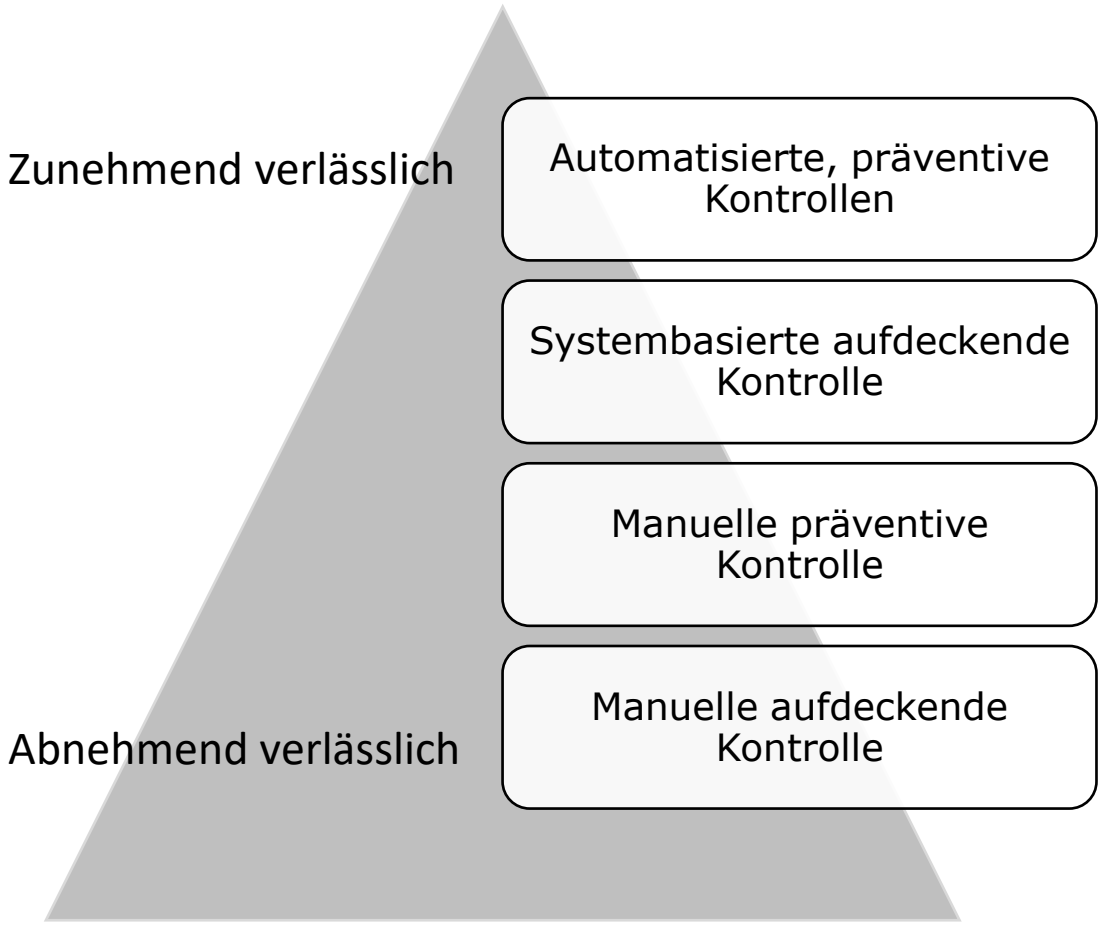
- Die konkrete Ausgestaltung ist dabei abhängig von:
- Größe und Gestalt des Unternehmens
- Unternehmensspezifische Anforderungen
- Präferenzen der Unternehmensführung

Prinzipien eines IKS

- **Transparenz-Prinzip** – für Prozesse sind Sollkonzepte etabliert, die es einem Außenstehenden ermöglichen die Konformität zu beurteilen
- **Vier-Augen-Prinzip** – wichtige Entscheidungen bzw. kritische Tätigkeiten werden nicht von einer einzelnen Person getroffen/ durchgeführt
- **Prinzip der Funktionstrennung** – vollziehende, verbuchende und verwaltende Tätigkeiten, die innerhalb eines Prozesses vorgenommen werden, werden nicht durch eine einzelne Person durchgeführt
- Das **Prinzip der Mindestinformation** – nur diejenigen Informationen sind für Mitarbeiter verfügbar, die sie für ihre Arbeit brauchen

Arten von Kontrollen

- Primäre vs. Sekundäre
- Routine vs. Nicht-Routineprozesse
- Unternehmens vs. Prozessebene



Typen von Kontrollaktivitäten

- Abstimmung / Nachvollzug
- Analytische Prüfung
- Verifizierung
- Genehmigung
- Funktionstrennung
- Bestätigung
- Checklisten
- Durchsicht
- Physische Kontrollen
- Kontinuierliche Kontrollen

Dokumentation des IKS

Formen

- Verbale Prozessbeschreibungen (sog. Narratives)
- Flussdiagramme (Flowcharts oder Swimlanes)
- Risiko-Kontroll-Matrizen
- Testblätter
- Funktionstrennungsmatrizen
- Fragebögen
- Organisationshandbücher
- Organisationsdiagramme
- Rollen- und Stellenbeschreibungen
- Richtlinien und Anweisungen
- Protokollierungen
- Key-Performance-Indikatoren (KPI)

Anforderungen

- Die Dokumentation muss vollständig und aktuell sein – alle notwendigen Informationen
- Die Dokumentation muss fehlerfrei und eindeutig sein – zutreffende und widerspruchsfreie Informationen
- Die Dokumentation muss für den Anwender verständlich sein – ausreichender Detailierungsgrad mit Fokus auf Anwenderhorizont
- Die Dokumentation muss übersichtlich sein – erkennbare Zusammenhänge zwischen einzelnen Arbeitsbereichen
- Die Dokumentation muss auf Verlangen in angemessener Zeit zugänglich gemacht werden

Verknüpfung vCMS mit IKS

	Einfaches IKS	Integriertes IKS	Umfassendes IKS
Internes Umfeld	• Keine Abstimmung mit anderen Elementen der Corporate Governance	• Enge Vernetzung mit weiteren Elementen der Corporate Governance	• IKS als integriertes Steuerungssystem der Unternehmensführung
Risikobeurteilung	• Risikoidentifikation auf Basis standardisierter, generischer Risikokataloge	• Systematische Risikoidentifikation mit Fokus auf die wesentlichen Risiken	• Integrative und fortlaufende Risikoidentifikation („one view of risk“)
Kontrollaktivität	• Kontrollportfolio zeichnet sich durch unregelmäßige und nicht risiko-basierte Kontrolldurchführung aus	• Ausgewogenes Kontrollportfolio hinsichtlich Automatisierungsgrad & Kontrollart (präventiv vs. detektiv)	• Kontrollportfolio charakterisiert durch präventive, automatische und Managementkontrollen
Information und Kommunikation	• Manuelle und dezentrale Berichterstellung auf Basis der Bestätigungen des Managements	• Systemgestützte Berichterstellung auf Basis von aggregierten CSA*-Ergebnissen	• Systemgestützte Berichtserstellung auf Basis der Prüfungsergebnisse der Internen Revision
Überwachung	• Unsystematische Prüfung mittels standardisierter Fragebögen und Kontrollchecklisten	• Prüfung wesentlicher Kontrollen durch Prozess und Kontroll-Verantwortliche (CSA)*	• CSA-Evaluierung flankiert durch integrierte Continuous Assurance-Methodiken
Dokumentation	• Verwendung generischer Kontrollanforderungen, welche durch das Management abzudecken sind	• Systemgestützte, prozessspezifische Dokumentation der wesentlichen (Management-) Kontrollen	• Toolbasierte Dokumentation und Aktualisierung des unternehmens-weiten Kontrollportfolios • Integration des CMS in das IKS