

Whitepaper

Rating und Zertifizierung von Internen Kontrollsystemen (IKS)

Autor
Dr. Oliver Bungartz



Rating und Zertifizierung von Internen Kontrollsystemen (IKS)

Interne Kontrollsysteme (IKS) sind seit Jahrhunderten ein zentrales Element verantwortungsvoller Unternehmensführung sowie Ausprägung der Sorgfaltspflicht einerseits sowie der Legalitätspflicht und der Kontroll- und Überwachungspflicht eines jeden Kaufmanns andererseits.

Ursprünglich wurden sie häufig als Reaktion auf Unternehmenskrisen oder regulatorische Eingriffe etabliert – etwa nach dem Enron-Skandal und der daraus resultierenden Einführung des Sarbanes-Oxley Act (SOX) im Jahr 2002.

Seither hat sich die Perspektive deutlich gewandelt: Ein IKS wird heute nicht mehr als reine Compliance-Verpflichtung, sondern als strategisches Instrument zur Steuerung, Risikominimierung und Vertrauensbildung verstanden.

Angesichts wachsender Komplexität, globaler Lieferketten und zunehmender Cyber- und ESG-Risiken, kommt der regelmäßigen Bewertung und Zertifizierung von IKS eine immer größere Bedeutung zu. Unternehmen stehen unter steigendem Druck, ihr IKS nicht nur einzurichten, sondern deren Wirksamkeit nach internationalen Standards nachzuweisen – und zwar nachvollziehbar, vergleichbar und prüfbar.

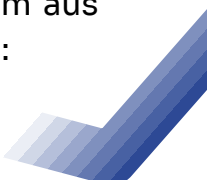
Aufgrund des gestiegenen öffentlichen Interesses an Steuerung und Kontrolle, ist auch die Demonstration dieses Nachweises in der Öffentlichkeit von hohem Interesse.

International anerkannte und global verbreitete Rahmenwerke im Bereich interner Kontrollen

Ein international anerkanntes Rahmenwerk wie das „Internal Control – Integrated Framework (ICIF) des Committee of Sponsoring Organizations of the Treadway Commission (COSO) bildet die theoretische und methodische Basis für den Aufbau, die Beurteilung und die Zertifizierung von IKS.

Das 1992 erstmals veröffentlichte und 2013 überarbeitete Rahmenwerk gilt weltweit als Referenzrahmen für angemessene und wirksame interne Kontrollen. Ein IKS nach COSO besteht aus fünf – aufeinander abgestimmte und integral operierende – Komponenten, welche die Wirksamkeit eines IKS bestimmen.

Bekannt wurde COSO insb. durch seine dreidimensionale Darstellung – den sog. COSO-Würfel – der die Verknüpfung zwischen Zielen, Komponenten und organisatorischen Ebenen verdeutlicht. Hiermit wird verdeutlicht, dass IKS immer ein integriertes System aus Kultur, Struktur und Prozessen ist:



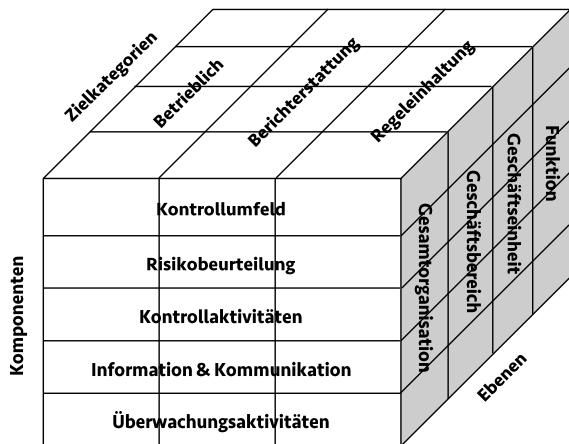


Abb. 1: COSO-Würfel – Struktur eines IKS nach international anerkannten Grundsätzen

- **Kontrollumfeld:** Werte, Integrität, Führungsverhalten und organisatorische Verantwortlichkeiten.
- **Risikobeurteilung:** Systematische Identifikation und Bewertung von Risiken
- **Kontrollaktivitäten:** Maßnahmen zur Risikosteuerung in Prozessen und Systemen
- **Information & Kommunikation:** Bereitstellung relevanter Informationen für Entscheidungen
- **Überwachungsaktivitäten:** Laufende und unabhängige Prüfung der Angemessenheit und Wirksamkeit

Diese Struktur bietet eine international einheitliche Grundlage für Prüfungen, Ratings und Zertifizierungen. Nationale Standards wie z.B. die Prüfungsstandards des Instituts der Wirtschaftsprüfer in Deutschland e.V.

(IDW) orientieren sich an COSO, während die Normen der International Organization for Standardization (ISO) als globale Referenzen dienen.

Zielsetzung und Charakter einer IKS-Zertifizierung

Eine Zertifizierung geht über die klassische Prüfung eines IKS hinaus. Die IKS-Zertifizierung dient nicht nur der Feststellung von Angemessenheit und Wirksamkeit, sondern auch der Bestandsaufnahme und Optimierung interner Kontrollen.

Das Rating im Rahmen einer Zertifizierung zeigt, wie gut das Unternehmen Risiken beherrscht und inwieweit es internationale Best Practices erfüllt. Darüber hinaus wird ein Benchmark-Vergleich in Bezug auf die Compliance mit anderen Organisationen ermöglicht.

Ein Zertifikat soll dabei als objektives Signal dienen, dass das Managementsystem den rechtlichen Anforderungen genügt, Best-Practice Vergleichen standhält und von der Unternehmensleitung aktiv getragen wird.

Nutzen einer IKS-Zertifizierung

Die Zertifizierung eines IKS bietet Organisationen einen doppelten Vorteil: Sie reduziert potenzielle Haftungsrisiken und stärkt gleichzeitig Wettbewerbsfähigkeit und Reputation.

Ein zertifiziertes IKS dokumentiert die Erfüllung regulatorischer Pflichten, betriebswirtschaftlicher Notwendigkeiten und signalisiert Stakeholdern, dass Risiken systematisch gesteuert werden.

Zu den zentralen Vorteilen einer IKS-Zertifizierung zählen:

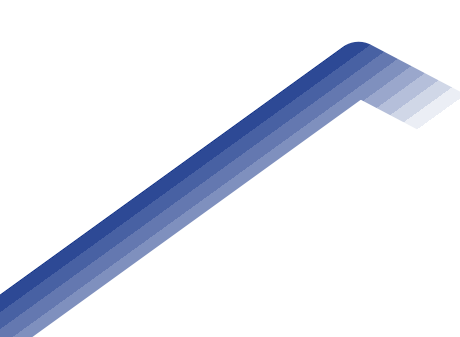
- Reduzierung zivil- und strafrechtlicher Haftungsrisiken durch Nachweis von Sorgfaltspflichten
- Verbesserung der Wettbewerbsfähigkeit und Glaubwürdigkeit im Markt
- Stärkung des Unternehmensimage bei Geschäftspartnern, Banken, Prüfern und Behörden
- Vermeidung potenzieller Vergabesperren und Ausschlüssen
- Orientierung für kontinuierliche Verbesserung und Effizienzsteigerung

Zertifizierung von Managementsystemen im internationalen Vergleich

Auch andere Managementsysteme im Bereich der Corporate Governance – etwa im Bereich Compliance (Compliance Management Systeme – CMS), Risikomanagement (Risikomanagementsysteme – RMS) oder Interne Revision (Interne Revisionsysteme – IRS) – unterliegen zunehmend internationalen Audit- und Zertifizierungsstandards.

Während in Deutschland die IDW-Standards orientierende Prüfungsgrundlagen darstellen, haben sich international ISO-Normen etabliert, z.B.:

- IDW PS 980 als CMS-Prüfungsstandard und ISO 37301 zur Zertifizierung eines CMS
- IDW PS 981 als RMS-Prüfungsstandard und ISO 31000 als allgemeiner Referenzrahmen zur Zertifizierung eines RMS
- IDW PS 982 als IKS-Prüfungsstandard und Certinova als Rating und Zertifizierung eines IKS
- IDW PS 983 – als IRS-Prüfungsstandard und Qualitätsbeurteilungen nach IIA-Standards zur Reifegradbestimmung und Beurteilung eines IRS



Hervorzuheben ist, dass die als Beispiel angeführten IDW-Prüfungsstandards allesamt auf den globalen Rahmenwerken von COSO basieren. Die Beispiele zur Prüfung, Rating und Zertifizierungen von Managementsystemen verdeutlichen, dass die Zertifizierung über rein nationale Anforderungen hinausgehen und ein international vergleichbares Vertrauen in Managementsysteme erschaffen werden muss.

Die Prüfung von IKS als Managementsystem im Bereich der internen Kontrollen, ist eine Beurteilung der Angemessenheit und/oder Wirksamkeit und zeigt Schwachstellen auf.

Hierbei ist keine Einschätzung /Bewertung des IKS auf einer Skala mit Benchmark-Vergleich verbunden. Die Ergebnisse in Form eines Prüfungsberichts sind in der Regel ausschließlich für die interne Verwendung bestimmt. Eine Weitergabe an Dritte ist nur mit entsprechender Genehmigung des Prüfers zulässig.

Im Gegensatz dazu beinhaltet ein IKS-Zertifikat ein Rating, das eine Einordnung in ein Reifegradmodell ermöglicht. Es kann als Benchmark gegenüber Geschäftspartnern, Prüfern und Wettbewerbern dienen und

öffentlich belegen, dass Risiken systematisch analysiert sowie angemessene Kontroll- und Steuerungsmaßnahmen definiert sind.

Reifegradmodelle als Rating-Instrument

Reifegradmodelle sind in der IKS-Zertifizierung ein wesentliches Werkzeug zur Bestandsaufnahme und Orientierung, indem sie verdeutlichen, auf welcher Entwicklungsstufe sich ein IKS befindet. Hierdurch wird deutlich welche Schritte zur Optimierung notwendig sind. Dadurch entsteht ein skalierbares und international vergleichbares Rating.

In der Praxis wird häufig auf das Capability Maturity Model Integration (CMMI) zurückgegriffen, um den Reifegrad eines IKS zu bestimmen. Das IKS kann in Anlehnung an dieses Modell in fünf verschiedene Reifegrade unterteilt werden:



Die Reifegrade bauen bei diesem Modell aufeinander auf, d.h. jeder höhere Reifegrad beinhaltet alle Eigenschaften seines Vorgängers. In der Literatur wird gefordert, dass ein IKS im Unternehmen nach diesem Modell mindestens den Reifegrad der „Stufe 3: Definiert“ erreichen sollte. Im Hinblick auf die Anforderungen, dass die Wirksamkeit des IKS kontinuierlich überwacht werden muss, ist jedoch ein Reifegrad der „Stufe 4: Überwacht“ zu fordern.

Ausblick: Digitale IKS-Zertifizierung mit Certinova

Während COSO den theoretischen

Rahmen liefert, zeigt die Praxis, dass Organisationen effiziente, standardisierte und digital unterstützte Verfahren benötigen. Die Methodik der IKS-Zertifizierung nach Certinova bietet hierfür eine Innovative Lösung:

Die Plattform ermöglicht die Zertifizierung von IKS auf Basis internationaler und nationaler Standards (COSO und IDW PS 982) und kombiniert interne Kontrollen mit digitaler Effizienz und globaler Vergleichbarkeit:

IKS-Reifegrad	Merkmale der einzelnen IKS-Reifegrade
Stufe 5: Optimiert	<ul style="list-style-type: none"> - Ausgeprägtes Kontrollbewusstsein im ganzen Unternehmen - Weitgehende Automatisierung der Kontrollaktivitäten - Hohe Reaktionsfähigkeit auf Veränderungen durch Tools - Integriertes IKS, Revisions- und Risikomanagementsystem
Stufe 4: Überwacht	<ul style="list-style-type: none"> - IKS-Grundsätze und Richtlinien sind detailliert dokumentiert - Regelmäßige Überwachung der Kontrollen - Laufende Aktualisierung der Kontrollen - Regelmäßige IKS-Berichterstattung
Stufe 3: Definiert	<ul style="list-style-type: none"> - IKS-Grundsätze und Richtlinien sind dokumentiert - Kontrollen sind in den Prozessen integriert und dokumentiert - Nachvollziehbarkeit der Kontrollen ist gegeben - Information, Kommunikation und Schulung existieren
Stufe 2: Wiederholbar	<ul style="list-style-type: none"> - Interne Kontrollen sind vorhanden, aber nicht standardisiert - Fehlende Nachvollziehbarkeit der Kontrollen - Kontrollen sind personenabhängig und nicht dokumentiert - Fehlende Information, Kommunikation und Schulung
Stufe 1: Initial	<ul style="list-style-type: none"> - Unstrukturiertes Kontrollumfeld im Unternehmen - Interne Kontrollen sind kaum oder nicht vorhanden - Vorhandene Kontrollaktivitäten werden fallweise ausgeführt - Vorhandene Kontrollen sind nicht verlässlich

Abb. 2: IKS-Reifegrade auf Basis des CMMI

- Digitale und ressourcenschonende Durchführung nach modernstem Stand der Technik
- Kompatibilität mit internationalen und nationalen Prüfungsstandards
- Skalierbare Reifegradmodelle mit Benchmark-Vergleichen zugeschnitten auf die individuellen Bedürfnisse und Ausgestaltung des IKS in Organisationen
- Hohe Reputation durch anerkannte, praxiserprobte und unabhängige Bewertung basierend auf jahrzehntelanger Erfahrung
- Sichtbare Stärkung des Vertrauens in Governance & Compliance und wettbewerbswirksame Außendarstellung durch transportierbare Gütesiegel

Damit verbindet die Zertifizierungsmethode von Certinova rechtliche Sicherheit mit wirtschaftlicher Effizienz und stärkt zugleich die Reputations- und Wettbewerbsfähigkeit zertifizierter Organisationen.

Die Zertifizierung von IKS gewinnt weltweit an strategischer Bedeutung. Sie schafft Vertrauen, reduziert Risiken und stärkt die Wettbewerbsposition von Organisationen. Ein nach internationalen Standards zertifiziertes IKS signalisiert Verantwortungs-

bewusstsein, Transparenz sowie nachhaltige Führung und Steuerung von Organisationen.

Angesichts zunehmender Regulierungsdichte und globaler Erwartungen wird die Zertifizierung künftig zu einem zentralen Bestandteil moderner Corporate Governance.





Certinova

Your compliance benchmark



+49 / (0)40 35006-400



info@certinova.com



www.certinova.com



Caffamacherreihe 16
20355 Hamburg

Certinova ist ein Service der BRL Risk Consulting GmbH & Co. KG. Dieses Whitepaper dient ausschließlich zu Informationszwecken. Es stellt weder eine rechtliche, steuerliche, finanzielle oder sonstige professionelle Beratung dar, noch sollte es als solche ausgelegt werden. Die hierin enthaltenen Informationen, Daten und Analysen wurden nach bestem Wissen und Gewissen erstellt, erheben jedoch keinen Anspruch auf Vollständigkeit oder Richtigkeit. Weder BRL Risk Consulting GmbH & Co. KG noch die Autoren übernehmen eine Haftung für Verluste oder Schäden, die direkt oder indirekt aus der Nutzung oder dem Vertrauen auf die in diesem Dokument enthaltenen Informationen entstehen. Dieses Dokument kann zukunftsgerichtete Aussagen enthalten, die Risiken und Unsicherheiten unterliegen. Tatsächliche Ergebnisse können erheblich von den in solchen Aussagen ausgedrückten oder implizierten abweichen.