

Risikomanagement und Risikocontrolling

Diederichs

5., vollständig überarbeitete und ergänzte Auflage 2023
ISBN 978-3-8006-6931-8
Vahlen

schnell und portofrei erhältlich bei
beck-shop.de

Die Online-Fachbuchhandlung beck-shop.de steht für Kompetenz aus Tradition. Sie gründet auf über 250 Jahre juristische Fachbuch-Erfahrung durch die Verlage C.H.BECK und Franz Vahlen.

beck-shop.de hält Fachinformationen in allen gängigen Medienformaten bereit: über 12 Millionen Bücher, eBooks, Loseblattwerke, Zeitschriften, DVDs, Online-Datenbanken und Seminare. Besonders geschätzt wird beck-shop.de für sein

umfassendes Spezialsortiment im Bereich Recht, Steuern und Wirtschaft mit rund 700.000 lieferbaren Fachbuchtiteln.

durchzuführen. Bei der Bewertung sind Wechselwirkungen zwischen Risiken zu berücksichtigen.³¹⁸

Unabhängig davon sollte das Management jederzeit sein Urteilsvermögen und Fachwissen einbringen. Zudem können Bewertungen auch unternehmensweit von verschiedenen Teams durchgeführt werden. Es ist dann ein Prozedere festzulegen, wie mit Unterschieden in den Bewertungsergebnissen umgegangen wird. Annahmen, die bei der Bewertung getroffen werden, sind nachvollziehbar zu dokumentieren.

Bruttorisiko sowie angestrebtes und realisiertes Restrisiko

Bei der Risikobewertung sind das Bruttorisiko sowie das angestrebte und das realisierte Restrisiko (Nettorisiko) zu betrachten.³¹⁹ Folglich ist bereits hier der Aspekt der Risikosteuerung/-bewältigung zu berücksichtigen.³²⁰ So kann z. B. bewertet werden, ob bestehende Maßnahmen nicht zu einer messbaren Änderung der Risikoauswirkung führen oder Maßnahmen redundant sind. Dementsprechend kann die Allokation von Ressourcen hinterfragt werden.

Bewertungsergebnisse darstellen

Die Ergebnisse der Risikobeurteilung sind grafisch darzustellen. Sollte ein Unternehmen hierzu ein Risikoportfolio verwenden, d. h. die Darstellung der Risiken anhand von Eintrittswahrscheinlichkeit und Auswirkung mit Blick auf ein (Unternehmens-/Bereichs-/Abteilungs-) Ziel bei gegebener Performance, kann das Portfolio – unter Berücksichtigung des jeweiligen Risikoappetits – um Toleranzbereiche zu einer „Heat Map“ erweitert werden.³²¹

Außerdem kann die Risikosituation für ein bestimmtes Performanceziel anhand eines Risikoprofils schematisch dargestellt werden (vgl. rekapitulierend Abb. 2-57, S. 154). Jeder Punkt auf der Risikoprofillinie stellt die Kombination von Eintrittswahrscheinlichkeit und Auswirkung der Risiken für das betrachtete Ziel schematisch dar. Sollte sich die Performance ändern, kann dies z. B. dazu führen, dass neue Risiken entstehen, Risiken wegfallen oder sich die Bewertung ändert.

Auslöser für Risikoneubewertungen

Es sind Auslöser zu definieren, die zu einer Neubewertung von Risiken führen. So können z. B. Änderungen im Unternehmensumfeld oder des Risikoappetits die der Bewertung zugrundeliegenden Annahmen hinfällig machen.

Zudem impliziert das Risiko selbst, wie oft eine Neubewertung durchzuführen ist. So sind z. B. Risiken aus sich ändernden Rohstoffpreisen potenziell täglich zu bewerten, Risiken aufgrund sich ändernder Demografien dagegen nur jährlich.

³¹⁸ Interdependenzen sind z. B. dann gegeben, wenn mehrere Risiken ein Unternehmensziel beeinflussen oder wenn ein Risiko ein anderes auslöst.

³¹⁹ Vgl. hierzu die Begriffserklärung in COSO (2017), S. 77

³²⁰ Der Aspekt wird im Rahmen der nächsten beiden Prinzipien näher beschrieben.

³²¹ Vgl. hierzu weiterführend COSO (2017), S. 77 f. sowie Kapitel 3.3.3, S. 302 ff.

Voreingenommenheit, Vorurteile und Verzerrungen

Voreingenommenheit, Vorurteile und Verzerrungen sind zu vermeiden. Die Art und Weise, wie ein Risiko formuliert und dargestellt wird, haben einen signifikanten Einfluss darauf, wie es interpretiert und bewertet wird. Bei der Nutzung der Kennzahl „Schadenerwartungswert“ (d. h. der Multiplikation von Eintrittswahrscheinlichkeit und monetärer Auswirkung) könnte ein Risiko mit geringer Wahrscheinlichkeit aber hoher Auswirkung zu einem gleichen Ergebnis führen wie ein Risiko mit hoher Wahrscheinlichkeit aber geringer Auswirkung. Das eine Risiko kann jedoch für das Unternehmen akzeptabel sein, während das andere dies nicht ist.

Voreingenommenheit, Vorurteile und Verzerrungen haben auch eine Auswirkung auf die sich anschließende Risikosteuerung/-bewältigung. Werden z. B. Risiken unterschätzt, sind die eingesetzten Maßnahmen möglicherweise nicht ausreichend und das Unternehmen bewegt sich außerhalb des Risikoappetits. Umgekehrt besteht das Risiko, dass Ressourcen fehlallokiert werden. Zudem kann es vorkommen, dass durch „unnötige“ Maßnahmen die Performance beeinträchtigt wird, weil potenzielle Chancen unterdrückt werden.

2.4.1.4.3 Prinzip 12: Priorisierung von Risiken³²²

Festlegung der Kriterien/Voreingenommenheit bei der Priorisierung

Risiken sind zu priorisieren, um Entscheidungen bezüglich der optimalen Risikoreaktionen sowie der Zuweisung von Ressourcen treffen zu können. Die Priorisierung und Ressourcenallokation haben vorurteilsfrei zu erfolgen.

Die Priorisierung ist anhand von Kriterien festzumachen. So kann sie unter Berücksichtigung der Eintrittswahrscheinlichkeit und des Ausmaßes, der Bedeutung für die Unternehmensziele sowie des Risikoappetits erfolgen. Außerdem können folgende Aspekte beachtet werden:³²³

- Anpassungsfähigkeit: Die Fähigkeit eines Unternehmens, sich an Risiken anpassen und darauf reagieren zu können.
- Komplexität: Umfang und Art eines Risikos für den Unternehmenserfolg.³²⁴
- Geschwindigkeit: Die Geschwindigkeit, mit der ein Risiko auf ein Unternehmen einwirkt.
- Persistenz: Fortdauer/Beständigkeit des Risikos.
- Wiederherstellung: Die Fähigkeit eines Unternehmens, nach einem schwerwiegenden Ereignis wieder zum normalen Tagesgeschäft zurückzukehren.

Priorisierung von Risiken

Ähnlich bewertete Risiken (d. h. hinsichtlich Wahrscheinlichkeit und Auswirkung) können unterschiedlich priorisiert werden. Dies kann z. B. dann der Fall sein, wenn ein Risiko eine größere Geschwindigkeit und Beständigkeit aufweist. Außerdem ist Risiken Priorität einzuräumen, die ein Unternehmen

³²² Vgl. hierzu und ff. COSO (2017), S. 79 f.

³²³ Die Kriterien können auch bei der Risikobewertung berücksichtigt werden (vgl. Prinzip 11).

³²⁴ Gegenseitige Abhängigkeiten von Risiken erhöhen typischerweise die Komplexität.

als Ganzes betreffen. Letztlich beeinflusst die Priorisierung die Maßnahmen zur Risikobewältigung.

Verwendung des Risikoappetits

Risiken sind auch mit Blick auf den Risikoappetit oder andere Toleranzgrenzen zu priorisieren. Risiken, die dazu führen, dass sich das Unternehmen dem Risikoappetit stark annähert, ist meist eine höhere Priorität einzuräumen.

Zudem ist zu entscheiden, welche Risiken akzeptiert werden, d.h. für welche Risiken keine (weiteren) Maßnahmen in Erwägung gezogen werden.

Risikopriorisierung auf allen Ebenen

Die Risikopriorisierung hat auf allen hierarchischen Ebenen zu erfolgen. Dabei ist es zumeist sinnvoll, dass Risiken unternehmensweit konsistent priorisiert werden. Dies ist z. B. der Fall, wenn eine gemeinsame bzw. gleichartige Risiko-reaktion erforderlich ist. Im Ergebnis sollte sich infolgedessen eine konsequentere und effizientere Reaktion zeigen, als wenn jedes Risiko separat priorisiert worden wäre.

Grundsätzlich sollten die Mitarbeiter priorisieren, die das Risiko verantworten (Risk Owner). Sie sind dafür verantwortlich, entsprechend der Priorität angemessene Maßnahmen zur Risikobewältigung unter Berücksichtigung der Ziele auszuwählen und anzuwenden.

In den Fällen, in denen der Risk Owner und diejenigen, die für die Maßnahmen verantwortlich sind, unterschiedliche Personen, Abteilungen etc. sind, muss der Risk Owner über ausreichend Befugnisse verfügen, ein effektives Risikomanagement gemäß Priorisierung durchzusetzen.

2.4.1.4.4 Prinzip 13: Maßnahmen zur Risikobewältigung implementieren³²⁵

Auswahl und Einsatz von Maßnahmen

Für die identifizierten Risiken sind Maßnahmen zur Risikobewältigung auszuwählen und umzusetzen. Dabei sind Auswirkung, Eintrittswahrscheinlichkeit und Priorisierung der Risiken, der Risikoappetit, die Unternehmensziele, die Performance, der jeweilige Geschäftskontext, Kosten-Nutzen-Aspekte sowie Verpflichtungen gegenüber und Erwartungen von Stakeholdern zu berücksichtigen.

Folgende Ansätze stehen grundsätzlich zur Verfügung: akzeptieren, vermeiden, verfolgen, reduzieren und teilen.³²⁶ Zeigen Maßnahmen nicht die angestrebte Reaktion, kann es aufgrund der Tragweite eines Risikos sinnvoll sein, Ziele oder Strategien zu überprüfen und ggf. anzupassen.

Ein Unternehmen kann sich bei Bedarf auch dafür entscheiden, den Risikoappetit zu überschreiten, um Chancen wahrzunehmen. Sollte es im Rahmen seiner gewöhnlichen Geschäftstätigkeit allerdings wiederholt Risiken akzeptieren, die dem Risikoappetit nahekommen oder diesen überschreiten, ist möglicherweise eine Adjustierung des Risikoappetits erforderlich.

³²⁵ Vgl. hierzu und ff. COSO (2017), S. 81 ff.

³²⁶ Vgl. hierzu ausführlich COSO (2017), S. 81 sowie Kapitel 3.3.2, S. 294 ff.

Zumeist führt eine Kombination mehrerer Maßnahmen zum angestrebten Restrisiko. Die Maßnahmen zur Risikobewältigung sind zu kontrollieren und zu überwachen.³²⁷ Es ist sicherzustellen, dass sie wie vorgesehen greifen. Zudem ist zu prüfen, ob zusätzliche Maßnahmen erforderlich sind.

Achtung

Hier verweist das COSO-Rahmenwerk auf die Komponente „Control Activities“ des COSO I-Rahmenwerks „Internal Control – Integrated Framework“.

Vollständigkeitshalber führt das COSO-Rahmenwerk aus, dass Risiken nicht voll umfänglich eliminiert werden können bzw. sollen. Dies liegt einerseits an der zukünftigen Ungewissheit und andererseits an begrenzten Ressourcen bzw. der Sinnhaftigkeit, jedes Risiko steuern zu wollen.

Berücksichtigung von Kosten und Nutzen

Die Kosten risikobewältigender Maßnahmen umfassen direkte Kosten, indirekte Kosten (sofern messbar) und ggf. Opportunitätskosten (im Zusammenhang mit der Nutzung von Ressourcen). Die Kosten sind dem Nutzen gegenüberzustellen. Sie sollten in einem angemessenen Verhältnis zueinanderstehen. So kann z. B. ein mit „hoch“ priorisiertes Risiko und einer größeren Tragweite angesichts des erwarteten Nutzens der Maßnahmen höhere Ressourcen rechtfertigen.

Kosten-Nutzen-Erwägungen können meist nur unterschiedlich genau durchgeführt werden. So ist der Nutzen in manchen Fällen nur schwer oder subjektiv quantifizierbar. Allerdings kann der Nutzen i. d. R. im Zusammenhang mit der Erreichung von Strategien und Zielen bewertet werden. Es kann hierbei vorkommen, dass es keine optimale Risikobewältigung mit Blick auf die Kosten-Nutzen-Relation gibt und daher Strategien und Ziele (z. B. einer Unternehmens Einheit) kritisch zu reflektieren sind.

Weitere Überlegungen

Die Maßnahmenauswahl kann neue Fragestellungen aufwerfen oder unbeabsichtigte Folgen haben (z. B. neue Risiken verursachen), die es zu berücksichtigen gilt.

Ferner können neue Risiken andere und innovative Wege bei der Risikobewältigung notwendig machen, die wiederum eine Revision des bestehenden Maßnahmenportfolios erfordern bzw. sinnvoll erscheinen lassen. Auch veränderte Optionen hinsichtlich der Maßnahmen (z. B. durch neue technologische Möglichkeiten) können eine kritische Überprüfung nach sich ziehen.

2.4.1.4.5 Prinzip 14: Portfoliosicht entwickeln³²⁸

Risikosituation ganzheitlich verstehen

Das Risikomanagement soll die potenziellen Auswirkungen der identifizierten Risiken aus einer ganzheitlichen Perspektive betrachten – das COSO-Rahmenwerk spricht hier von einer Portfoliosicht – und das Restrisiko im Verhältnis zu

³²⁷ Vgl. hierzu Kapitel 3.3.4, S. 304 ff.

³²⁸ Vgl. hierzu und ff. COSO (2017), S. 84 ff.

den jeweiligen Zielen und definierten Toleranzen beurteilen. Hierzu sind die Risiken zu betrachten, die sich auf jede Abteilung, Funktion, Einheit oder das Gesamtunternehmen beziehen, und anschließend in entsprechenden Portfoliosichten zusammenzutragen.

Achtung

Die Portfoliosicht aus Gesamtunternehmensperspektive soll es ermöglichen, die Art, Tragweite sowie gegenseitigen Abhängigkeiten von Risiken sowie die Auswirkung auf die Performance, Ziele und Strategien zu verstehen. Es ist festzustellen, ob das Restrisiko mit dem Risikoappetit übereinstimmt; ggf. ist korrigierend einzugreifen. Dies kann dann z.B. der Fall sein, wenn ein Risiko über verschiedene Einheiten hinweg für die operativen Einheiten akzeptabel, allerdings auf Unternehmensebene anders zu würdigen ist. In einem anderen Fall, in dem das Restrisiko deutlich unter dem Risikoappetit liegt, könnten höhere Risiken eingegangen werden, um den Unternehmenswert zu steigern.³²⁹

Entwicklung einer Portfoliosicht

Das COSO-Rahmenwerk stellt heraus, dass eine Portfoliosicht auf unterschiedliche (qualitative und quantitative) Weise entwickelt und grafisch veranschaulicht werden kann. Eine Methode besteht darin, sich auf die wichtigsten Risikokategorien der operativen Einheiten oder des Gesamtunternehmens zu konzentrieren. Sie ist dann anzuwenden, wenn Risiken anhand von Zielen bewertet werden. Dabei kann die Art und Höhe der übernommenen Risiken im Vergleich zum Risikoappetit (z. B. für jede Funktion, die Strategie oder jedes Ziel) dargestellt werden.

Bei der Entwicklung einer Portfoliosicht sollten Risiken hinsichtlich einer potenziellen Zunahme bzw. Abnahme ihrer Tragweite sowie potenzieller Kompensationen und Korrelationen analysiert werden, wenn sie sukzessive auf den unterschiedlichen Unternehmensebenen konsolidiert werden.

Letztlich soll laut COSO die Portfoliosicht eine risikobasierte Entscheidungsfindung unterstützen und bei der Festlegung und Änderung von Performancezielen sowie der Beeinflussung der unternehmerischen Risikosituation helfen. Im Zusammenhang mit der Strategie, den Zielen sowie dem Risikoappetit soll ein Verständnis für die Beziehung zwischen Performance und Risiken geschaffen werden.

Portfoliosicht analysieren

Um „Überraschungen“ und Verluste zu vermeiden oder besser darauf zu reagieren und um Änderungen der unternehmerischen Rahmenbedingungen mit Blick auf die Strategie und Ziele bewerten zu können, sind im Rahmen der Analyse qualitative Instrumente und/oder quantitative Instrumente anzuwenden. So kann z. B. anhand von Stresstests analysiert werden, wie das Portfolio reagiert. Dies soll es dem Unternehmen ermöglichen, seine Anpassungsfähigkeit und Resilienz zu beurteilen. Zudem kann die Analyse auch bei der Auswahl einer Strategie oder der Festlegung von Zielen nützlich sein.

³²⁹ COSO (2017), S. 84.

2.4.1.5 Review and Revision

Drei Prinzipien konkretisieren die Komponente „Review and Revision“ des COSO-Rahmenwerks (vgl. Abb. 2-60).³³⁰ Die wesentlichen Aspekte und Anforderungen werden fortfolgend umrissen.

Komponente und Grundsatz		Aspekte
Review & Revision	15. Assesses Substantial Change Die Organisation identifiziert und bewertet Änderungen, die sich erheblich auf die Strategie und Unternehmensziele auswirken können.	Integration von Reviews in die Geschäftspraktiken
		Interne und externe Veränderungen
	16. Reviews Risk and Performance Die Organisation überprüft die Performance und berücksichtigt Risiken.	Integration von Reviews in das Tagesgeschäft
		Berücksichtigung organisatorischer Fähigkeiten
	17. Pursues Improvement in Enterprise Risk Management Die Organisation strebt eine Verbesserung des Risikomanagements an.	Verbesserungen durchführen

Abb. 2-60: Komponente „Review & Revision“

2.4.1.5.1 Prinzip 15: Wesentliche Änderungen bewerten³³¹

Integration von Reviews in die Geschäftspraktiken

Bereits bei der Festlegung von Strategien und Zielen versuchen Unternehmen, zahlreiche potenzielle zukünftige Veränderungen zu berücksichtigen. Dennoch müssen sie sich bewusst sein, dass auch Änderungen mit ausgeprägteren Auswirkungen auftreten können. Diese können zu neuen oder veränderten Risiken führen und wichtige Annahmen beeinflussen.³³² Praktiken und Instrumente zur Identifikation derartiger Änderungen sind in das Tagesgeschäft zu integrieren und anzuwenden.

Interne und externe Veränderungen

Unternehmen haben zu analysieren, wie sich Veränderungen auf das Risikomanagement und das Erreichen von Strategien und Zielen auswirken können. Dies erfordert die Identifizierung interner und externer Umweltveränderungen sowie Veränderungen in der Kultur.³³³

Das Erkennen wesentlicher Änderungen, das Bewerten ihrer Auswirkungen und das Reagieren auf die Änderungen sind iterative Prozesse, die sich auf mehrere Risikomanagement-Komponenten auswirken können. Grundsätzlich ist es nach einem Risikoereignis sinnvoll, eine Ex-Post-Analyse durchzuführen. Hierbei ist zu überprüfen, wie das Unternehmen reagiert hat und welche Erkenntnisse sich auf zukünftige Ereignisse übertragen lassen.

³³⁰ Vgl. COSO (2017), S. 89 f.

³³¹ Vgl. hierzu und ff. COSO (2017), S. 90 f.

³³² Als Beispiele nennt COSO den Erwerb eines Unternehmens oder die Implementierung eines neuen IT-Systems. Vgl. COSO (2017), S. 90.

³³³ Als Beispiele nennt COSO: schnelles Unternehmenswachstum, Innovationen, Änderungen in der Führung und im Personal sowie Änderungen regulatorischer oder wirtschaftlicher Rahmenbedingungen.

2.4.1.5.2 Prinzip 16: Review der Risiken und Performance³³⁴

Integration von Reviews in das Tagesgeschäft

Im Laufe der Zeit führt ein Unternehmen seine Risikomanagement-Praktiken möglicherweise nicht so effizient wie beabsichtigt durch. Hierdurch können sich Risiken manifestieren und die Performance kann beeinträchtigt werden. Daher sind z. B. die Fähigkeiten, Praktiken sowie Kultur regelmäßig kritisch zu prüfen. Zudem kann die Performance auch aufgrund der inhärenten Natur des Risikos beeinträchtigt werden, die nicht exakt vorhergesagt werden kann. In diesem Kontext sind folgende Fragen zu beantworten:³³⁵

- Hat sich das Unternehmen wie erwartet entwickelt und sein Ziel erreicht? Aufgetretene Abweichungen sind zu identifizieren und die Gründe zu analysieren.
- Sind neue Risiken aufgetreten, die die Performance beeinträchtigen können? Es ist zu prüfen, ob Risiken zuvor identifiziert wurden oder ob neue Risiken aufgetreten sind. Es ist auch zu analysieren, ob die tatsächlichen Risikoniveaus innerhalb der Toleranzgrenzen liegen.
- Ist das Unternehmen genug Risiko eingegangen, um sein Ziel zu erreichen? Es ist zu analysieren, ob die Zielverfehlung auf Risiken zurückzuführen ist oder ob ein unzureichendes Risiko eingegangen wurde, um das Erreichen des Ziels zu unterstützen.
- Wurde die Höhe des Risikos richtig eingeschätzt? Es ist zu evaluieren, warum das Risiko nicht „richtig“ bewertet wurde bzw. werden konnte. Hierzu sind der Geschäftskontext und die Annahmen zu hinterfragen, die der ursprünglichen Bewertung zugrunde lagen. Zudem ist zu prüfen, ob neue Informationen verfügbar sind, die zu einer genaueren Bewertung beitragen würden.

Berücksichtigung organisatorischer Fähigkeiten

Wenn ein Unternehmen feststellt, dass die Performance (signifikant) außerhalb der Toleranz liegt oder dass das Performanceziel zu einem anderen Risikoprofil als erwartet führt, muss es möglicherweise:

- die Geschäftsziele oder Strategie(n) nachschärfen,
- die Kultur und den Risikoappetit überprüfen und ggf. korrigieren,
- die Fähigkeiten der Organisation und deren Auswirkung auf die Performance überprüfen,
- das Performance-Ziel überarbeiten,
- die Auswirkung von Risikoergebnissen neu bewerten,
- die Risikopriorisierung überprüfen sowie Risikoreaktionen und Ressourcenzuweisungen überarbeiten und/oder
- die Überwachungsaktivitäten neugestalten.³³⁶

³³⁴ Principle 16: Reviews Risk and Performance; vgl. hierzu und ff. COSO (2017), S. 92 ff.

³³⁵ Vgl. COSO (2017), S. 92.

³³⁶ Hier verweist das COSO-Rahmenwerk auf die Komponente „Control Activities“ des COSO I-Rahmenwerks „Internal Control – Integrated Framework“. Vgl. COSO I (2013).

Achtung

Das COSO-Rahmenwerk stellt vollständigkeithalber heraus, dass der Umfang der Korrekturmaßnahmen dem Ausmaß der Performance-Abweichung, der Bedeutung des Ziels und den Kosten und Vorteilen im Zusammenhang mit der Änderung von Risikoreaktionen entsprechen muss.

Wenn bei der Überprüfung der Performance wiederholt neue Risiken identifiziert werden oder wenn das Risiko als deutlich gravierender einzuschätzen ist, hat die Unternehmensführung zu bestimmen, ob eine Überprüfung der unternehmensweiten Risikomanagementpraktiken zu rechtfertigen ist.³³⁷

2.4.1.5.3 Prinzip 17: Verbesserung des Risikomanagements³³⁸**Verbesserungen durchführen**

Auch Unternehmen mit einem geeigneten Risikomanagement-System können „besser“ werden. Durch Einbettung von Reviews und Bewertungen in das Tagesgeschäft können Verbesserungspotenziale systematisch identifiziert werden. Auch separate Prüfungen können hilfreich sein.³³⁹

Die Verfolgung von Verbesserungen hinsichtlich des Risikomanagement-Systems sollte sich auf das gesamte Unternehmen erstrecken. Dabei können folgende Bereiche bzw. Aspekte von Interesse sein:

- Änderungsrate/Dynamik des Geschäftskontextes,
- Neue Technologien (wie z. B. Data-Mining),
- Governance/organisatorische Einbindung des Risikomanagements (z. B. der Risikomanagement-Funktion),
- Analyse der Kommunikations- und Berichtsprozesse,
- Peer-Vergleich(e),
- Analyse historischer Mängel (z. B. zurückliegende Fehleinschätzungen von Risiken),
- Überprüfung des Risikoappetits,
- Review/Ergänzungen von Risikokategorien.

2.4.1.6 Information, Communication and Reporting

Drei Prinzipien konkretisieren die Komponente „Information, Communication and Reporting“ des COSO-Rahmenwerks (vgl. Abb.2-61).³⁴⁰ Die wesentlichen Aspekte und Anforderungen werden fortfolgend umrissen.

³³⁷ Die Überprüfung der Risikobewertungspraktiken wird noch einmal bei Prinzip 17 aufgegriffen. Vgl. COSO (2017), S. 95 f.

³³⁸ Vgl. hierzu und ff. COSO (2017), S. 95 f.

³³⁹ Auch hier wird auf das COSO I-Rahmenwerk verwiesen.

³⁴⁰ Vgl. COSO (2017), S. 97 ff.