

Erfolgsfaktoren Risikomanagementsystem

1. Organisation des Risikomanagements im Unternehmen
2. Aufgaben des Risikomanagementsystems
3. Interne / externe Risikokommunikation
4. Revision / Auditierung des Risikomanagementsystems
5. IT-gestützte Risikomanagementsysteme (Client Server-Systeme)
6. Risikomanagement in der Unternehmensführung
7. Risikomanagement in der Internen Revision / im Controlling
8. Risikomanagement im Krisenmanagement
9. Normative Rahmenbedingungen

Die nachfolgende Checkliste erhebt keinen Anspruch auf Richtigkeit und Vollständigkeit. Diese Checkliste muss firmenspezifisch angepasst werden. Secricon GmbH übernimmt infolgedessen keine juristische Verantwortung und wird keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung der vorliegenden Checkliste oder Teilen davon entsteht.



1. Organisation des Risikomanagements im Unternehmen

Definition: Ein Risikomanagementsystem definiert organisatorische, finanzielle, methodische und technische Aspekte für ein wirksames und wirtschaftliches Risikomanagement im Unternehmen, im Vorhaben oder in der Organisation.

- Gibt es für die Risikomanagement-Organisation ein Pflichtenheft, welches die Verantwortlichkeiten, Kompetenzen und Aufgaben definiert?
- Ist ein Risikomanager benannt, welcher die Funktionsfähigkeit und die Weiterentwicklung des Risikomanagementsystems organisiert? Welche Kompetenzen hat er? Hat er Anordnungsrechte und unter welchen Bedingungen darf er sie ausüben?
- Ist das Risikomanagement konform zur Unternehmensstrategie? Werden die Grundsätze und die Vorgaben der Unternehmensführung in Bezug auf das Risikomanagement in einer Risikopolitik / Sicherheitspolitik dokumentiert und den Mitarbeitern kommuniziert?
- Wird die Konformität des Risikomanagements zur Geschäftsstrategie durch die Interne Revision regelmässig überprüft?
- Gibt es ein Risikosteuerungsausschuss, welcher die Aufsicht über das Risikomanagement wahrnimmt und unternehmenswichtige Risikomanagement-Entscheidungen in Abstimmung mit der Unternehmensstrategie / Geschäftsleitung fällt?
- Wird im Unternehmen der Grundsatz Prozess-Eigner = Risiko-Eigner gelebt? Wie werden die Prozess-Eigner in die Risikomanagement-Organisation eingebunden? Gibt es eine Risk Map, welche die Risikosituation der Geschäftsprozesse darstellt?
- Gibt es Anreizsysteme, welche die Akzeptanz und Wirkung des Risikomanagements im Unternehmen fördern und die Ertrags- / Risikoposition des Unternehmens steuern und lenken?
- Sind die Ziele und Erfolgsfaktoren des Risikomanagements und die Anforderungen an das Risikomanagement definiert? Werden die Risikomanagementziele den Mitarbeitern kommuniziert?
- Sind die Anspruchsgruppen des Risikomanagements identifiziert (Aufsichtsrat / Verwaltungsrat, Geschäftsleitung, Mitarbeiter, Finanzinstitute [Rating nach Basel II], Gesellschaft / Politik, Gesetzgeber [Gesetze, Corporate Governance])?
- Ist die Risikokommunikation (Top-down) und die Risikoberichterstattung (Bottom-up) organisiert und funktionsfähig?
- Gibt es im Unternehmen eine gelebte Risikomanagement-Kultur, eine Risikomanagement-Sprache, welche jedem Mitarbeiter zugänglich und verständlich ist?
- Werden die Risikoinformationen zielgruppenorientiert bereitgestellt?



2. Aufgaben des Risikomanagementsystems

• Risikoidentifikation

Die Identifikation von Risiken kann eine sehr komplexe Tätigkeit sein. Insbesondere bei der Identifikation / Wahrnehmung von Risiken, denen man sich im Unternehmen nicht bewusst ist (Blinde Flecke, Betriebsblindheit), hilft es, systematisch vorzugehen.

- Haben Sie eine Risikodefinition im Unternehmen? Verstehen alle das Gleiche unter einem Risiko?
- Organisieren Sie interdisziplinäre Teams, welche im Rahmen von Risk Assessment Workshops die relevanten Risiken identifizieren und bewerten?
- Welche Methoden wenden Sie an, um eine ganzheitliche Sicht auf ihre Risikosituation zu erhalten? Klassifizieren Sie Ihre Risiken nach geeigneten Risikofeldern?
- Nutzen Sie regelmässig die Erfahrung und das Wissen von externen Spezialisten bei der Erstellung / Überprüfung des Risikoinventars?
- Organisieren Sie für den Erfahrungsaustausch Arbeitskreise mit Mitarbeitern von anderen Standorten oder mit Mitarbeitern von anderen Unternehmungen mit ähnlicher Risikoexposition?
- Kennen Sie die Unternehmenswerte, welche durch Risiken gefährdet sind? Kennen Sie die Verletzlichkeiten, so genannte neuralgische Punkte des Unternehmens? – Diese bilden besonders gute Angriffspunkte.
- Wenden Sie methodische Ansätze des Systems Engineerings, der System Dynamics an, um die Ursachen-, Wirkungsbeziehungen von Risiken und Chancen im Unternehmen und in der Interaktion mit seinem Umsystem zu analysieren und zu verstehen?
- Analysieren Sie den Markt? Kennen Sie die relevanten Marktteilnehmer?
- Kennen Sie die zukünftigen Techniken, die ihre Produkte / Dienstleistungen substituieren könnten? Entwickeln Sie Bilder von möglichen zukünftigen Markt-, Gesellschaftsentwicklungen? Führen Sie Trendanalysen durch?

• Risikobewertung

- Welche Risikobewertungsmetriken wenden Sie mit welcher Gewichtung an? Qualitative / quantitative? Wie aggregieren Sie die Risiken?
- Wie oft führen Sie Risikobewertungen durch? Wer bewertet die Risiken?
- Unterscheiden Sie zwischen Brutto-, / Netto- und Soll- / Ist-Risikobeurteilungen?
- Basiert Ihre Risikobewertung nur auf vergangenheitsbezogenen Informationen? Oder berücksichtigen Sie bei der Risikobewertung auch zukünftige Einflussfaktoren?
- Wird die Risikoanalyse durch eine Business Impact-Analyse ergänzt? Werden Informationen des Activity Based Costing verwendet, um Geschäftsprozessausfallkosten zu berechnen und damit das Schadensausmass der operationellen Risiken zu berechnen?
- Berücksichtigen Sie bei den Risikobewertungen Aspekte der Risikoperzeption, Risikoaversion, Risikowahrnehmung im Allgemeinen oder werden seltene, grosse Ereignisse stärker bewertet / wahrgenommen als öfters vorkommende Risiken mit kleinerem Schadensausmass, welche aber, über einen längeren Zeithorizont betrachtet, ein ähnlich grosses Schadenspotenzial aufweisen können?
- Berücksichtigen Sie, dass bei medienwirksamen Ereignissen die Risikowahrnehmung der Gesellschaft / Öffentlichkeit von der unternehmensinternen Risikobewertung massiv abweichen kann?



• Risikohandhabung

- Ist die Finanzierung der Risikohandhabung gewährleistet? Ist die Risikohandhabung konform zur Unternehmensstrategie?
- Ist das akzeptierbare Restrisiko definiert? Haben Sie die Grenzkosten / den Grenznutzen des Risikomanagements definiert?
- Berücksichtigen Sie, dass eine abgestimmte Kombination von organisatorischen, baulichen, technischen und versicherungstechnischen Massnahmen meist wirksamer und wirtschaftlicher wirkt als z.B. nur technische Massnahmen?
- Risikoreduzierende Massnahmen können Risiken vermeiden, vermindern, an Dritte überwälzen, überwachen sowie durch Förderung der Risikowahrnehmung identifizieren.
- Die Investitions- und Betriebsaufwände der Risikohandhabung können sehr kostenintensiv sein. Ist dafür gesorgt, dass die Risikohandhabung Added Value generiert?
- Die Wirksamkeit der Risikohandhabung definiert langfristig die Akzeptanz des Risikomanagements im Unternehmen und beantwortet die Frage „Was bringt das Risikomanagement?“

• Risikoüberwachung / Frühwarnung

Risiken definieren kritische Unternehmenssituationen, welche durch präventive Massnahmen möglichst vermieden werden sollten. Aus wirtschaftlichen Gründen kann es notwendig sein, nur eine bedingt ausreichende Risikoprävention zu realisieren, hohe Restrisiken in Kauf zu nehmen und durch geeignete Frühwarnmechanismen und Interventionsmassnahmen eine Risikovorsorge zu treffen, welche das Schadensvolumen im Ereignisfall beschränkt.

- Ist gewährleistet, dass Veränderungen der Risikoexposition / Risikosituation systematisch und regelmässig identifiziert und an die Entscheidungsträger kommuniziert werden?
- Ist ein internes Kontrollsystem vorhanden, welches die Risikosituation lenkt, steuert und transparent dokumentiert?
- Wie erfolgt die Überwachung der Risikoexposition? Welche Risikoindikatoren sind definiert? Gibt es Risikolimits und werden Verletzungen der Risikolimits erkannt und behoben?
- Werden kritische Ereignisse im Unternehmen rechtzeitig erkannt?
- Mit welcher Frequenz werden die Risikoindikatoren durch wen erfasst?
- Wurden Frühwarn- und Alarmschwellen definiert, welche eine Alarmierung auslösen?
- Ist das Risikoüberwachungssystem / Frühwarnsystem mit dem Alarmmanagement und dem Ereignis- / Notfall- / Krisenmanagement gekoppelt (vgl. Checkliste Erfolgsfaktoren Krisenmanagement)?

• Risikoberichterstattung / Risikokommunikation

- Vgl. nächster Erfolgsfaktor
- Wird das Risikomanagement in die Unternehmenssteuerung und -führung eingebunden?

• Prüfung des Risikomanagements

- Wird das Risikomanagementsystem regelmässig von der Internen Revision geprüft?
- Genügt das Risikomanagement den gesetzlichen Anforderungen?
- Unterliegt das Risikomanagementsystem einem kontinuierlichen Verbesserungsprozess?



3. Interne / externe Risikokommunikation

• Kommunikationsstrategie

- Wer ist im Unternehmen für die Risikokommunikation zuständig? Wer bestimmt, wer welche Risikoinformation wie an wen und wann kommunizieren darf?
- Wird eine moderne Fehlerkultur im Unternehmen gelebt? Werden Fehler als Chance für Verbesserungen wahrgenommen und akzeptiert?

• Interne Top-down-Kommunikation

- Sind die Kommunikationswege Top-down (Anordnung / Genehmigung von Risikomassnahmen, Instruktion / Anweisung / Information / Ausbildung der Mitarbeiter) definiert?
- Wie werden die Risikowahrnehmung und das Sicherheitsbewusstsein der Mitarbeiter gefördert?
- Werden die Mitarbeiter in Risiko- und Sicherheitsfragen ausgebildet?
- Wird das Verhalten der Mitarbeiter bezüglich Risikomanagement und Sicherheitsmanagement regelmässig geprüft?
- Gibt es Anweisungen für den Umgang mit Medien?
- Welche Medien, Channels werden für die Risikokommunikation verwendet?

• Interne Bottom-up-Kommunikation

- Sind die Kommunikationswege Bottom-up (Risikomeldung, Risikoberichterstattung etc.) definiert?
- Wie erfolgt die Schadensmeldung? Wie erfolgt die Frühwarnung?
- Ist die Risikosituation transparent?
- Welche Anreizsysteme gibt es für die Mitarbeiter, welche die Risikokommunikation fördern?
- Wurde die Risikoberichterstattung standardisiert und strukturiert? Kann die Risikoberichterstattung ausgewertet werden? Sind die Risikoinformationen unterschiedlicher Bereiche miteinander vergleichbar?
- Wird eine einheitliche Risikomanagement-Methodik unternehmensweit angewendet?

• Kommunikation nach aussen

- Soll die Risikoanalyse den Aufsichtsrat bei seiner Entscheidungsfindung unterstützen?
- Werden Risikoberichte für die Eigner / Aktionäre des Unternehmens erstellt?
- Wer kommuniziert das Risikomanagement nach aussen? Welche externen Anspruchsgruppen gibt es?
- Soll das Risikomanagement im Sinne eines Ratings nach Basel II das Unternehmen in Fragen der externen Finanzierung unterstützen?
- Soll die Risikoanalyse bei Verhandlungen mit Versicherungsgesellschaften unterstützen? Aushandlung der Versicherungs-Policen.
- Werden Risikoberichte den Medien zur Verfügung gestellt?



4. Revision / Auditierung des Risikomanagementsystems

• Interne Überprüfung

- Erfolgt eine regelmässige Überprüfung des Risikomanagementsystems durch eine unabhängige Stelle, z.B. Qualitätsmanagement, Interne Revision?
- Welche Aspekte werden überprüft? Ergebnisse, Verfahren, Vollständigkeit, Wirtschaftlichkeit, Konformität mit gesetzlichen und unternehmerischen Richtlinien?
- Wie oft erfolgt eine Überprüfung? Wird risikoorientiert überprüft, d.h. Bereiche mit hoher Risikoexposition öfters als solche mit geringer Risikoexposition?
- Wird die Auditierung des Risikomanagementsystems dokumentiert und der Geschäftsleitung zur Verfügung gestellt?
- Werden in Abstimmung mit der Geschäftsleitung dem Risikomanager und dem Risikosteuerungsausschuss Verbesserungsempfehlungen unterbreitet?
- Wird die kontinuierliche Verbesserung des Risikomanagementsystems geprüft und nachgewiesen?

• Externe Überprüfung

- Erfolgt eine regelmässige Überprüfung des Risikomanagementsystems durch einen Wirtschaftsprüfer oder Risikomanagement-Spezialisten?
- Werden Verbesserungsvorschläge der Internen Revision, der externen Wirtschaftsprüfung realisiert?

5. IT-gestützte Risikomanagementsysteme (Client Server-Systeme)

IT-gestützte Risikomanagementsysteme unterstützen die Risikotransparenz und steigern die Effizienz der Risikoberichterstattung und optimieren dadurch den Zeitaufwand und die Kosten des Risk Reporting.

- Kann das eingesetzte Risikomanagementsystem sämtliche Aufgaben, welche unter dem Erfolgsfaktor „Aufgaben des Risikomanagementsystems“ aufgelistet sind, abbilden?
- Verwendet das Risikomanagement-Tool ein Rollenkonzept, welches den geforderten Informationssicherheitsanforderungen genügt und die gegebene Risikomanagement-Organisation abbilden kann?
- Sind unternehmensspezifische Anpassungen an der Risikosoftware möglich, und ist der Anbieter des Systems in der Lage, unternehmensspezifische Anpassungen zu guten Konditionen durchzuführen und zu warten?
- Werden Aktionen der Systemanwender protokolliert?
- Gibt es Auswertungsmöglichkeiten und Exportfunktionen, so, dass eigene Auswertungen z.B. in MS Excel durchgeführt werden können?
- Verfügt das System über ein zielgruppenorientiertes Reporting?
- Ist das RM-System leicht anwendbar und selbsterklärend?
- Verfügt das System, falls notwendig, über eine Mehrsprachenfunktionalität?
- Kann das RM-System in die bestehende Applikationslandschaft integriert werden? Welche Datenbank-Systeme unterstützt das Tool?



6. Einbindung des Risikomanagements in die Unternehmensführung

Unternehmensziele und Unternehmenswerte gehören zu den risikobehaftetsten Elementen eines Unternehmens. Die Zielerreichung und Wertschöpfung ist durch vielfältige Risiken gefährdet.

- Werden Risiken, welche die Strategieumsetzung gefährden, in das Risikomanagement integriert und im Rahmen der Risikohandhabung entschärft?
- Gibt es eine Risk Map, die Auskunft gibt, welches Risiko welche Ziele und Erfolgsfaktoren des Unternehmens wie stark gefährdet? Wird eine Risiko-Ziel-Wirkungsanalyse durchgeführt?
- Ist der strategische Fit der Ressourcenbereitstellung für die Risikohandhabung gewährleistet?
- Werden die Risikohandhabungsmassnahmen in das Programm- / Projektmanagement des Unternehmens integriert?
- Wie wird die Risikofinanzierung organisiert?
- Wird das Risikomanagement durch ein Chancenmanagement für die Zielfindung ergänzt?
- Welche Risikokonstellationen sollen den Aufsichtsrat zu einer Anpassung der Unternehmensstrategie und damit einer Anpassung des Zielsystems bewegen?
- Wann darf eine Risikokonstellation die Umsetzung eines Geschäftsziels stoppen, um weitere Abklärungen zu treffen?
- Wie soll mit Zielen umgegangen werden, welche einerseits hohe Chancen und andererseits hohe Risiken beinhalten?
- Wie hoch ist das akzeptierbare Restrisiko, welcher Sicherheitsstandard soll minimal eingehalten werden?

7. Einbindung des Risikomanagements in die Interne Revision / das Controlling

• Risikoorientierte Interne Kontroll-Systeme IKS

- Ist dafür gesorgt, dass risikobehaftete Unternehmensbereiche stärker kontrolliert werden? Werden die Frequenz und der Aufwand für interne Kontrollen risikoorientiert bestimmt?
- Wird der Prozess der Risikobewertung, welche regelmässig durch den Risiko-Eigner durchzuführen ist, im Rahmen des internen Kontrollsystems geprüft?
- Ist das IKS in das Frühwarnsystem des Unternehmens eingebunden?

• Risikoorientierte Prüfung der Internen Revision

- Erfolgen die Revisionen auf der Basis der Risikoexposition des Unternehmens? Verwendet die Interne Revision die Ergebnisse / Berichte der Internen Kontrollsysteme für die Erstellung ihres Prüfprogramms?
- Wird zwischen fixen und variablen Kontrollbereichen unterschieden? – Fixe Kontrollbereiche müssen unabhängig von der Risikosituation aufgrund von gesetzlichen oder unternehmerischen Auflagen immer kontrolliert werden. Variable Kontrollbereiche sollten in erster Linie dann, wenn sie risikobehaftet sind, kontrolliert werden.
- Ist dafür gesorgt, dass eine unabhängige Interne Revision zusätzliche eigene Risikoeinschätzungen und -hypothesen durchführt und diese Ergebnisse mit der Risikoanalyse des Unternehmens vergleicht?
- Sorgt die Interne Revision dafür, dass sie, trotz Verwendung der Ergebnisse des Internen Kontrollsystems und des Risikomanagements, unabhängig bleibt?



- Werden im Sinne einer Stichprobenkontrolle auch variable risikounkritische Unternehmensbereiche im Rahmen der Mehrjahresplanung berücksichtigt?

8. Krisenmanagement / Notfallmanagement

Im Rahmen der Risikoanalyse sind Risiken mit Notfall- / Krisenpotenzial zu kennzeichnen. Für solche Risiken / Szenarien sind Massnahmenpläne auszuarbeiten, welche im Ernstfall eine Eskalation des Ereignisses zu einem Notfall, zu einer Krise verhindern sollen.

→ **Vgl. Checkliste Erfolgsfaktoren Krisenmanagement**

9. Normative Regelwerke

- ONR49000 Risikomanagement Norm des Österreichischen Normungsinstituts; <http://www.on-norm.at/>
- AIRMIC Risk Management Standard; <http://www.armic.com>
- ASIS Risk Management Guideline; <http://www.asisonline.org/guidelines>
- COSO Enterprise Risk Management Framework; <http://www.coso.org>
- AS/NZS 4360:2004 Risk Management Standards Australia; <http://www.standards.com.au>